Le droit de la preuve à l'aune de la blockchain

Alice Barbet-Massin

Université de Lille
École Doctorale n°74 des Sciences juridiques, Politiques et de Gestion

Thèse :

LE DROIT DE LA PREUVE À L'AUNE DE LA BLOCKCHAIN

Pour l'obtention du grade de Docteur en droit
Présentée et soutenue publiquement
Le 14 septembre 2020 par :
Alice Barbet-Massin

Sous la direction de :
Monsieur Marcel Moritz
Maître de Conférences, HDR
Université de Lille

Membres du jury de thèse :

- **Florence G'sell**, Professeure agrégée de droit, Université de Lorraine (rapporteure)
- **Mustapha Mekki**, Professeur agrégé de droit, Université Sorbonne Paris Cité (rapporteur)
- **Pierre Berlioz**, Professeur agregé de droit, Université Paris Descartes (président)
- **Primavera de Filippi**, Chargée de recherche au CNRS/CERSA, Université Pantheon-Assas et chercheuse associée au Berkman Center for Internet & Society, Université de Harvard
- **Jean-Paul Delahaye**, Professeur émérite d'informatique, Université de Lille

L'Université n'entend donner ni approbation, ni improbation aux opinions émises dans la présente thèse. Ces opinions doivent être considérées comme propres à leur auteur.

REMERCIEMENTS

Ce travail de recherche n'aurait pu être mené à bien sans certaines personnes avec qui j'ai eu la chance de travailler, ou plus largement d'interagir, que je souhaite remercier.

Je tiens avant tout à adresser mes remerciements à Marcel Moritz qui a dirigé cette thèse. En m'incitant à exprimer librement ma pensée, il m'a permis d'œuvrer avec indépendance et satisfaction intellectuelle tout au long de ces années de recherche. Son suivi régulier, attentif et bienveillant de mes travaux ont participé à l'accomplissement ce travail.

Je remercie aussi vivement les membres du jury qui - après avoir largement nourri ma pensée - me font l'honneur de me lire et de siéger à ma soutenance de thèse.

Également, je remercie les membres du CERAPS et les doctorants en droit du numérique pour leurs relectures et nos discussions enrichissantes.

J'exprime ensuite une grande reconnaissance aux membres du cabinet d'avocats August Debouzy, particulièrement Mahasti Razzavi et Florence Chafiol. Je les remercie d'avoir cru en mon projet de recherche, accepté de le financer, et permis à ces travaux de voir le jour. En plus d'avoir pu mettre en perspective concrètement ces recherches, j'ai eu plaisir à travailler avec eux (notamment Abdelaziz Khatab, Cen Zhang, Eden Gall pour les débats idéologiques sur les *Cypherpunks*).

Ma profonde gratitude est de toute évidence adressée à mes proches pour l'attention qu'ils m'ont portée durant cette épreuve, leur patience et encouragements sans cesse renouvelés.

Enfin, cette thèse est dédiée à la riche communauté de la *blockchain* et des crypto-actifs, un secteur stimulant et singulier.

SOMMAIRE

PARTIE 2 : L'APPRÉHENSION JURIDICTIONNELLE INSUFFISANTE DE LA « *VÉRITÉ CRYPTOGRAPHIQUE* » DES DONNÉES ENREGISTRÉES DANS LA *BLOCKCHAIN*

TITRE 1 : L'INTERVENTION JURIDICTIONNELLE PRUDENTE DANS LA RECONNAISSANCE DES PREUVES DE DONNÉES ENREGISTRÉES DANS LA *BLOCKCHAIN*

CHAPITRE 1 : LE RÔLE CARDINAL DES JURIDICTIONS TRADITIONNELLES EN MATIÈRE DE PREUVE DES DONNÉES ENREGISTRÉES DANS LA *BLOCKCHAIN*

CHAPITRE 2 : LE DÉPASSEMENT ATTENDU DES JURIDICTIONS TRADITIONNELLES EN MATIÈRE DE PREUVE DES DONNÉES ENREGISTRÉES DANS LA *BLOCKCHAIN*

TITRE 2 : L'INTERVENTION EXTRA-JURIDICTIONNELLE DÉMESURÉE DANS LA RECONNAISSANCE DES PREUVES DE DONNÉES ENREGISTRÉES DANS LA *BLOCKCHAIN*

CHAPITRE 1 : LES ATTENTES EXCESSIVES DU JUGE ET DES PARTIES ENVERS LES HUISSIERS ET EXPERTS DE JUSTICE EN MATIÈRE DE PREUVE DE DONNÉES ENREGISTRÉES DANS LA *BLOCKCHAIN*

CHAPITRE 2 : LES PALLIATIFS AUX RISQUES D'ATTEINTES A L'INDÉPENDANCE DE LA JUSTICE EN MATIÈRE DE PREUVE DE DONNÉES ENREGISTRÉES DANS LA *BLOCKCHAIN*

TABLE DES ABREVIATIONS

AFNOR	Association française de normalisation
AGRASC	Agence de gestion et de recouvrement des avoir saisis et confisqués
AJDA	Actualité Juridique Droit Administratif
AJ Contract	Actualité Juridique Contrat
AMF	Autorité des marchés financiers
ANSSI	Agence nationale de la sécurité des systèmes d'information
Art.	Article d'un texte
BaaS	*Blockchain as a Service*
BCE	Banque centrale européenne
BEPAB	*Blockchain Expert Policy Advisory Board*
BJB	Bulletin Joly Bourse
BJS	Bulletin Joly Sociétés
Bull. civ	Bulletin des arrêts de la Cour de cassation (chambres civiles)
Bull. crim	Bulletin des arrêts de la Cour de cassation (chambre criminelle)
BTA	*Blockchain Technology Act*
C. civ.	Code civil
C. com.	Code de commerce
C. conso.	Code de la consommation
C. mon. fin.	Code monétaire et financier
C. pén.	Code pénal
C. pr. civ.	Code de procédure civile
C. pr. pén.	Code de procédure pénal
Cass.	Cour de cassation
Cass. ass. plen.	Cour de cassation assemblée plénière
Cass. ch. mixte	Cour de cassation chambre mixte
Cass. civ.	Cour de cassation chambre civile
Cass. com.	Cour de cassation chambre commerciale
CE	Conseil d'État
CEN	*European Committee for Standardization*
CEDH	Cour européenne des droits de l'homme
CESDH	Convention de sauvegarde des droits de l'homme et des libertés fondamentales
CESTI	Centre d'Evaluation de la Sécurité des Technologies de l'Information
CJUE	Cour de justice de l'Union européenne
CNUDCI	Commission des Nations unies pour le droit commercial international
CNIL	Commission nationale de l'informatique et des libertés
CMII	Complexe mondial Interpol pour l'innovation
CNRS	Centre national de la recherche scientifique
COFRAC	Comité français d'accréditation
Coll.	Collection
Com.	Commentaire
CPI	Code de la propriété intellectuelle
CSPLA	Conseil supérieur de la propriété littéraire et artistique
Dalloz IP/IT	Dalloz revue droit de la propriété intellectuelle et du numérique
DEEP	Dispositif d'enregistrement électronique partagé

DLT	*Distributed ledger technologies*
E-evidence	Projet de règlement relatif à l'accès transfrontière aux preuves numériques
E-Sign Act	*Electronic Signatures in Global National Commerce Act*
ECE	Equipes communes d'enquête
Ed.	Edition
ERC	*Ethereum Request for Comment*
FRE	*Federal Rules of Evidence*
GMT	*Greenwich Mean Time*
eIDAS	Règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur
Gaz. Pal.	Gazette du Palais
Ibid.	*Ibidem*
JCl	Jurisclasseur
JCP	Semaine Juridique
JCP E	Semaine Juridique – Edition Entreprise et Affaires
JCP G	Semaine Juridique – Edition Générale
JCP N	Semaine Juridique Edition Notariale
JO	Journal officiel
JOCE	Journal officiel de la Communauté européenne
JOUE	Journal officiel de l'Union européenne
JORF	Journal officiel de la République française
JUB	Juridiction unifiée du brevet
ICO	*Initial coin offering*
ISO	*International Organization for Standardization*
Op.cit.	*Opus citatum*
Infra	Ci-dessous
KYC	*Know your customer*
LCB-FT	Lutte contre le blanchiment de capitaux et le financement du terrorisme
LGDJ	Librairie Générale de Droit et de Jurisprudence
LPA	Revue Les Petites Affiches
LCEN	Loi pour la confiance dans l'économie numérique
MDBC	Monnaie digitale de Banque centrale
Obs.	Observation
OCDE	Organisation de coopération et de développement économique
OPESCT	Office parlementaire d'évaluation des choix scientifiques et technologiques
PACTE	Loi relative à la croissance et la transformation des entreprises
PSC	Prestataire de services de confiance
PSCQ	Prestataire de services de confiance qualifié
PSAN	Prestataire de services sur actifs numériques
Puf	Presses Universitaires de France
RB	Revue Banque
Règl.	Règlement européen
RDBF	Revue droit bancaire et financier
RLDA	Revue Lamy Droit des Affaires
RLDC	Revue Lamy Droit Civil
RLDI	Revue Lamy Droit de l'Immatériel
RTD Civ.	Revue Trimestrielle de Droit Civil
RTD Com.	Revue Trimestrielle de Droit Commercial

SEC	*Securities and Exchange Commission*
STAD	Système de traitement automatisé de données
Supra	Ci-dessus
T. Com.	Tribunal de Commerce
TA	Tribunal Administratif
TGI	Tribunal de Grande Instance
Tracfin	Traitement du renseignement et action contre les circuits financiers clandestins
TRD	Technologie des registres distribués
UETA Act	*Uniform Electronic Transactions Act*
UTC	*Universal Time Coordinated*

« *Les isolants cryptographiques produisent une* “*flèche du temps*” *qui rend l'écriture irréversible. Or cette flèche du temps est bien ce qui fait qu'il y a du réel : c'est parce qu'il n'est pas possible de revenir sur ces pas que les choses existent* »[1].

Mark Alizart

[1] M. Alizart, *Cryptocommunisme*, Perspectives critiques, Puf, fevr. 2019, p.73.

INTRODUCTION

1. C'est à l'orée d'une ère technologique neuve que l'apparition de la technologie *blockchain* et de son schéma de preuve distribuée est le présage d'un modèle probatoire en mutation[2]. Saluée par certains auteurs comme une décentralisation d'ampleur égale à Internet[3], la *blockchain* opère un glissement de l'échange décentralisé de l'information à celui de la valeur. Mais davantage encore, elle sécurise ces échanges de valeurs à l'appui d'une combinaison de procédés techniques constituant un ensemble de preuves nouvelles inaltérables. Satoshi Nakamoto, l'inventeur anonyme du premier protocole de *blockchain* (Bitcoin)[4], faisait

[2] Les rapports pléthoriques publiés ces dernières années par différentes institutions françaises, européennes et étrangères témoignent la portée innovante de cette technologie : Government Office for Science, Distributed Ledger Technology: Beyond Block Chain, A Report by the UK Government Chief Scientific Adviser, 2016, https://www.gov.uk/government/news/distributed-ledger-technology-beyond-block-chain (consulté le 31/05/2020), p.3-4 : « *In distributed ledger technology, we may be witnessing one of those potential explosions of creative potential that catalyse exceptional levels of innovation. The technology could prove to have the capacity to deliver a new kind of trust to a wide range of services…so may the visibility in these technologies reform our financial markets, supply chains, consumer and business-to-business services, and publicly-held registers* » and « *Algorithms that enable the creation of distributed ledgers are powerful, disruptive innovations that could transform the delivery of public and private services and enhance productivity through a wide range of applications* » ; France Stratégie, Rapport, Les enjeux des *blockchains*, Présidente du groupe de travail Joëlle Toledano, juin 2018, p.5 : « *(…) la blockchain est aujourd'hui à l'agenda de tous les décideurs (…) Certains y voient l'innovation disruptive qui va bouleverser la plupart des secteurs économiques, les plus optimistes allant jusqu'à annoncer l'entrée dans une ère de l'efficacité et de la confiance partagée* » ; EU Blockchain Observatory and Forum, Blockchain innovation in Europe, 27 juill. 2018, p.4 : « *Blockchain is one of the major breakthroughs of the past decade* » ; Assemblée Nationale, Rapport d'information n°1501, par la mission d'information commune sur les chaînes de blocs (*blockchains*), présenté par L. De La Raudière et J.-M. Mis, avant-propos de Julien Aubert, 12 déc. 2018, p.7 : « *La réflexion sur le potentiel des technologies de chaînes de blocs s'inscrit dans la révolution numérique que nous traversons* » ; Assemblée Nationale, Rapport d'information, par la commission des finances, de l'économie générale et du contrôle budgétaire en conclusion des travaux d'une mission d'information relative aux monnaies virtuelle, présenté par Eric Woerth et Pierre Person, avant-propos du Président, 30 janv. 2019, p.3 et 119 : « *(…) Notons que l'opacité qui entoure les crypto-actifs repose sur un paradoxe : en effet, l'immense avantage de la blockchain, cette technologie innovante de stockage et de diffusion d'informations, qui permet à de nombreux crypto-actifs de fonctionner, c'est justement qu'elle permet une transparence et une certification autonome des opérations, sans recours à un tiers de confiance* » et « *la blockchain et les crypto-actifs préfigurent ainsi une révolution technologique majeure. Du fait de la désintermédiation, de nombreuses activités économiques commencent à être transformées (banque, assurance, transports,…) et de nouveaux outils de financement de l'économie voient le jour (ICO, security token)* ». Voir aussi en ce sens la résolution du Parlement européen : Parlement européen, Résolution du 3 oct. 2018 sur les technologies des registres distribués et les chaînes de blocs : renforcer la confiance par la désintermédiation (2017/2772(RSP)), P8_TA(2018)0373, point M : « *Considérant que les applications de la TRD ont le potentiel de devenir rapidement systématiques, de la même manière que les innovations numériques ont radicalement transformé les services dans d'autres secteurs comme les télécommunications* ».

[3] J. Ito, La couche secondaire du protocole Bitcoin, Conférence Scaling bitcoin, Université de Stanford, 15 janv. 2018, https://bitconseil.fr/scaling-bitcoin-5-couche-secondaire/ (consulté le 31/05/2020) ; A. Wright, P.de Filippi, « Decentralized Blockchain Technology and the Rise of Lex Cryptographia », Librairie SSRN, 12 mars 2015, https://ssrn.com/abstract=2580664 (consulté le 31/05/2020).

[4] Voir *infra* n°25 et s. la notion de protocole.

référence à la nécessité de sécuriser les échanges par la preuve cryptographique en première page de son livre blanc en ces termes : « *ce qu'il faut, c'est un système de paiement électronique basé sur la preuve cryptographique plutôt que sur la confiance, (…) sans avoir besoin d'un tiers de confiance* ». Ce dernier mettait en exergue une solution « *utilisant un serveur d'horodatage distribué en pair-a-pair »* permettant alors de *« générer des preuves de l'ordre chronologique des transactions* »[5].

Cet outil à prouver qu'est la *blockchain* - dont les usages protéiformes reflètent l'effervescence de son développement - souffre de concepts aux contours imprécis en droit de la preuve. Il s'agira donc d'introduire l'étude du droit de la preuve à l'aune de la *blockchain* par la délimitation de son objet (I), pour développer ses intérêts (II) et enfin expliciter sa construction (III).

I. L'objet de l'étude

2. **Définition de *blockchain*.** La « *blockchain* », terme apparu en 2010[6], est une notion sibylline et incertaine au vocable plurivoque difficilement définie à ce jour[7]. Plusieurs sens peuvent être retenus pour sa définition, lesquels sont variables en fonction de l'angle - strict ou large et technique ou juridique - abordé. Les définitions large et stricte de *blockchain* tendent à distinguer les sens des termes employés entre « *la* » *blockchain* en tant que technologie et « *les* » *blockchains* considérant leurs diversités. Alors que les définitions techniques et juridiques expriment une distinction inhérente à des spécificités disciplinaires.

[5] S. Nakamoto, « Bitcoin : A Peer-to-Peer Electronic Cash System », 2008, p.1. Ce dernier n'emploie pas formellement le terme « *blockchain* » dans son livre blanc mais rapidement l'architecture bitcoin est directement associée à la technologie *blockchain* en tant que première application (A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, et P.Wuille, « Enabling *blockchain* innovations through pegged sidechains », 2014, p.3, https://blockstream.com/sidechains.pdf (consulté le 31/05/2020)).

[6] Même s'il semblerait que des traces du terme « *block chain* » ait été trouvées dès la fin des années 1990 sur des *mailing lists* de discussions entre cryptographes, l'usage dudit terme en lien avec les crypto-monnaies serait apparu - après l'invention du protocole Bitcoin en 2008 - avec son emploi par Hal Finney le premier développeur ayant travaillé avec Satoshi Nakamoto, en 2010 : https://satoshi.nakamotoinstitute.org/emails/cryptography/6/ (consulté le 31/05/2020). Voir à ce sujet : Institut Sapiens, Y. de Monbynes et G. Grandval, Rapport Bitcoin totem et tabou. Que présage l'essor des crypto-monnaies ?, févr. 2018, p.25.

[7] Selon le Professeur Mustapha Mekki, la *blockchain* fait l'objet de « *mystères* » car des questions juridiques de qualification et de sécurité des sujets de droit sont soulevées et restent en suspens. (Cour de cassation, Cycle de conférences « Entre mystère et fantasme : quel avenir pour les *blockchains* ? », ss. dir. scientifique de M. Mekki, N. Blanc, B. Haftel, conférence n°1 « Introduction générale. De la technologie des algorithmes à la technique juridique », propos introductifs de M. Mekki, le 7 févr. 2019).

3. **Définition large de « *la* » *blockchain*.** Il est courant de retenir la définition de la société Blockchain France pour la technologie *blockchain* qui séduit par sa clarté. Elle est définie simplement comme « *une technologie de stockage et de transmission d'informations, transparente, sécurisée et fonctionnant sans organe central de contrôle* »[8]. De manière plus prosaïque, la *blockchain* est représentée comme un grand livre numérique enregistrant l'ensemble des transactions chronologiquement réalisées entre individus. Le Professeur de mathématiques informatique et chercheur Jean-Paul Delahaye explique la *blockchain* en utilisant la métaphore de la place de la Concorde. Au côté de l'obélisque, serait installé un grand livre librement accessible à l'écriture et la lecture par tous les passants de la place sans que ce dernier ne puisse être détruit ou modifiable[9].

4. Avec la *blockchain*, les individus réalisent des transactions entre eux, ce qui lui vaut la qualification de technologie « *pair-à-pair* ». La *blockchain* Bitcoin en est l'illustration constituant une clé de voûte du pair-à-pair[10]. Le réseau *pair-à-pair* - déjà utilisé par d'autres technologies comme Internet - est un « *mode d'utilisation d'un réseau dans lequel chacun des participants connectés dispose des mêmes droits et qui permet un échange direct de services sans recourir à un serveur central* »[11]. Ce type de réseau pair-à-pair s'est développé depuis la fin des années 1970, au moyen de l'essor d'Internet, en vue de permettre le partage d'informations et de fichiers sur l'ensemble d'un réseau. Chaque utilisateur du réseau qui récupère un fichier devient lui-même à son tour hébergeur pour les autres participants au réseau. Ces réseaux ont été largement acceptés et popularisés au début des années 2000[12].

5. Dans le réseau *blockchain* de base, chacun des participants disposant des mêmes droits, l'intervention d'un serveur qui centralise et d'un organe qui valide n'est pas requise[13]. L'aboutissement du réseau pair-à-pair passe par la suppression des intermédiaires, qualifiés par

[8] https://blockcha*infra*nce.net/decouvrir-la-*blockchain*/c-est-quoi-la-*blockchain*/ (consulté le 31/05/2020).
[9] J. P.Delahaye, « Les *blockchains*, clefs d'un nouveau monde », Logique et calcul, Pour la Science n°449, mars 2015, p.80.
[10] Conférence Paris P2P Festival, intervention de A. Takkal Bataille, J. Favier, « Bitcoin, clé privée et clé de voûte du P2P », le 9 janv. 2020, https://bitcoin.fr/video-bitcoin-cle-privee-et-cle-de-voute-du-p2p/ (consulté le 31/05/2020).
[11] Vocabulaire de l'informatique (liste de termes, expressions et définitions adoptés), publié au JORF n°0121 du 23 mai 2017 texte n°20.
[12] A. Oram, *Peer-to-peer: harnessing the benefits of a disruptive technology 4-5*, 2001.
[13] Voir : P.de Filippi, « What Blockchain Means for the Sharing Economy », Harvard Business Review, 15 mars 2017, https://hbr.org/2017/03/what-*blockchain*-means-for-the-sharing-economy (consulté le 31/05/2020). *A contrario* des modèles centralisés des acteurs de l'économie numérique, la *blockchain* suit une architecture de type décentralisée, où certains acteurs sont chargés valider les transactions partout dans le monde et chacun conserve une copie du registre.

Satoshi Nakamoto de « *tiers de confiance* » (les États, les banques ou encore les professionnels réglementés)[14]. La *blockchain* jouerait technologiquement ce rôle par la substitution en lieu et place de ceux-ci et pourrait être regardée comme l'accomplissement d'un processus de désintermédiation[15]. Par exemple, le registre des comptes dans un système de paiement afin de connaître la balance financière de clients est tenu par une banque centralisée[16]. Au moyen de la *blockchain* publique Bitcoin, la balance financière des participants à cette *blockchain* est gérée par tout validateur souhaitant participer à l'approbation des transactions. La technologie est dite « *acéphale* »[17], ou encore « *trustless* »[18] en ce que le réseau endosse, lui-même, la surveillance et non un organe[19]. Or, l'évolution et la multiplication des *blockchains* se caractérisent par l'intervention de nouveaux tiers ou l'expérimentation d'applications diverses par certains tiers de confiance traditionnels, comme les banques, les notaires ou encore les greffiers[20]. Dans ces cas, la désintermédiation n'est pas totale mais la *blockchain* et le tiers de confiance sont complémentaires, garantissant une sécurité supplémentaire dans leurs activités.

6. En conséquence, la *blockchain* est - selon une conception large - avant tout, une technologie. Elle pourrait se voir définie comme une technologie de registre numérique distribué permettant l'échange et le stockage de valeur et plus largement de données, en pair-à-pair (sans organe central de contrôle et réduisant les intermédiaires à la transaction), de manière immuable et sécurisée, par un ensemble de techniques cryptographiques[21].

---

[14] Pour l'auteur Hervé Causse, le « *tiers de confiance* » serait une invention « *naïve* » de l'écosystème de la *blockchain* (H. Causse, Perspective colloque AFDIT, CRED « Qualification et état de la blockchain », le 24 avr. 2019).

[15] Conseil d'État, Étude annuelle 2017, Puissance publique et plateformes numériques : accompagner l' « ubérisation », le 13 juill. 2017.

[16] G. Marin-Dagannaud, « Le fonctionnement de la blockchain », Annales des Mine, 3 août 2017, p.42.

[17] Par référence à l'intitulé de l'ouvrage de Jacques Favier et Adli Takkal Bataille selon lequel la crypto-monnaie bitcoin est qualifiée d'acéphale (A. Takkal Bataille, J. Favier, Bitcoin. *La monnaie acéphale*, CNRS Editions, 2017, 280 p.).

[18] T. I. Kiviat, « Beyond bitcoin: issues in regulating blockchain transactions », Duke Law Journal, Vol. 65:569, 2015, p.574.

[19] « The trust machine », The Economist, 31 oct. 2015, https://www.economist.com/leaders/2015/10/31/the-trust-machine (consulté le 31/10/2015).

[20] Voir un article de cet avis : T. Douville et T. Verbiest, « Blockchain et tiers de confiance », Planet-Fintech, mai 2018, https://www.planet-fintech.com/Blockchain-et-tiers-de-confiance%C2%A0_a819.html (consulté le 31/05/2020).

[21] A ce jour, les codes cryptographiques sont considérés comme des codes surs par la communauté cryptologue (Conférence « Les mardis de l'espace des sciences », organisée avec l'Université de Rennes 2- CREA, intervention de J.-P.Delayahe « Les mathématiques et la cryptographie réinventent la monnaie : le bitcoin », le 14/10/2014, https://www.espace-sciences.org/conferences/mardis-de-l-espace-des-sciences/les-mathematiques-et-la-cryptographie-reinventent-la-monnaie-le-bitcoin (consulté le 31/05/2020)).

7. **Acteurs principaux.** Deux grandes catégories d'acteurs sont représentées dans une *blockchain*. D'une part, trois acteurs internes à la *blockchain* sont identifiés[22]. Ces acteurs sont différenciés mais ne s'excluent pas de manière étanche, un individu peut endosser différents rôles. Les « *participants* » à la *blockchain* réalisent des transactions. Ce sont des émetteurs et destinataires de transactions au sein d'un réseau. Ils font référence à un émetteur et un destinataire traditionnel à la différence que l'émetteur dispose d'un droit d'écriture dans le registre de la *blockchain*. L'émetteur peut être, par exemple, un débiteur qui paie une somme *via* une crypto-monnaie, une Université qui ancre un diplôme dans la *blockchain*, ou encore un assureur qui indemnise automatiquement un sinistre grâce à un *smart contract*[23]. Le destinataire de la transaction peut-être un créancier qui reçoit une somme en crypto-monnaie, un employeur qui vérifie l'authenticité d'un diplôme, ou encore un assuré qui perçoit automatiquement un dédommagement en cas de sinistre. Les « *accédants* » ou « *nœuds du réseau* », ont eux, un droit d'accès au registre des transactions, autrement dit, ils peuvent les lire et en obtenir une copie. En enregistrant l'ensemble de l'historique de ces transactions, l'accédant conserve une copie à jour du registre et héberge donc l'ensemble de son contenu. Enfin, les « *validateurs* », ou « *nœuds complets* » ou autrement appelés « *mineurs* » dans certaines *blockchains*[24], vérifient, valident et créent des blocs de transactions[25]. Dans la *blockchain* de Bitcoin, par exemple, c'est l'activité de « *minage* » qui permet de vérifier et valider les transactions. Les mineurs doivent mettre à la disposition du réseau une grande puissance de calcul informatique pour résoudre un problème mathématique complexe. Le premier mineur qui obtient la solution à ce problème reçoit une contrepartie en bitcoins, lesquels sont créés à l'occasion de chaque validation de bloc[26]. La chance de valider un bloc et de recevoir ces bitcoins est donc proportionnelle à la puissance de calcul apportée par le mineur[27]. Une fois la vérification réalisée par le mineur sélectionné, les autres mineurs n'ont plus qu'à approuver la solution pour l'ajout du nouveau

[22] Selon l'approche de la CNIL, il peut être distingué trois protagonistes dans la *blockchain* : les « *accédants* », les « *participants* » et les « *mineurs* » (CNIL, Premiers éléments d'analyse de la CNIL. Blockchain, 24 sept. 2018, https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf (consulté le 31/05/2020)).

[23] Voir les développements *infra* n°16, 17 sur l'usage du smart contract.

[24] Notons que seuls les mineurs en tant que validateurs techniques de transaction dans la *blockchain* seront évoqués dans cette thèse, ce qui exclut toute mention des mineurs par référence à l'âge légal de la majorité.

[25] La seule condition pour devenir validateur sur bitcoin « *est d'installer sur sa machine un logiciel qui allouera de la puissance de calcul pour contribuer à la validation des transactions* » (R. Pérez Marco, « Blockchain : l'autre révolution venue du bitcoin », CNRS Le Journal, mai 2016, https://lejournal.cnrs.fr/billets/blockchain-lautre-revolution-venue-du-bitcoin (consulté le 31/05/2020).

[26] Pour être incités à valider honnêtement les blocs, les validateurs sont rémunérés en bitcoin. Lorsqu'il valide un bloc de transactions, un validateur est actuellement rémunéré 12,5 bitcoins. Avec cette *blockchain*, la rémunération est décroissante, en 2021 un validateur pourra être rémunéré à hauteur de 6,75 bitcoins (jusqu'à l'émission totale de bitcoins de 21 000 millions) (A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder, *Bitcoin and Cryptocurrency Technologies*, Princeton University Press, 2016, p.61-68).

[27] R. Pérez Marco, « Blockchain : l'autre révolution venue du bitcoin », *op.cit.*

bloc ou la rejeter (en fonction de sa validité)[28]. Généralement, les validateurs ont une copie du registre, et cumulent ainsi le statut d'accédant. Toutefois, les participants à la *blockchain* ne font pas tous nécessairement de la vérification, validation et création de blocs de transactions[29].

8. D'autre part, des acteurs externes existent en complémentarité aux acteurs internes, et d'autres ont prospéré depuis le succès des *blockchains* et leurs accès aux non-initiés. Les développeurs de protocole jouent en effet un rôle déterminant dans le déploiement et la progression des *blockchains*. Externes à la *blockchain* elle-même, ils sont souvent aussi participants, accédants ou validateurs dans la *blockchain*. Cette communauté est puissante puisque les développeurs de codes spécialisés dans ce secteur sont rares, parfois formés par les acteurs économiques eux-mêmes. Des fondations comme les Fondations Ethereum, Bitcoin ou Hyperledger organisent ces communautés de développeurs et coordonnent les évolutions de la *blockchain*[30]. Ces sont traditionnellement des organismes à but non-lucratif financés par des cotisations, des dons ou encore des levées de fonds.

9. Divers autres tiers gravitent autour de la *blockchain*, incluant les prestataires de services sur actifs numériques (PSAN) visés limitativement par la loi n°2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises dite « *PACTE* »[31], tels que les plateformes d'achat et vente d'actifs numériques en monnaie ayant cours légal, les plateformes d'échange d'actifs numériques, les services de conservation pour le compte de tiers d'actifs numériques ou d'accès à des actifs numériques (services de portefeuille numérique), les plateformes de négociation d'actifs numériques, les prestataires de gestion de portefeuille d'actifs numériques pour le compte de tiers, de prix ferme d'actifs numériques, de placement garanti et non garanti d'actifs numériques, de réception et transmission d'ordres sur actifs numériques pour le compte de tiers, les conseillers aux souscripteurs d'actifs numériques. Des acteurs non visés par cette loi sont aussi présents sur ce marché, comme l'ensemble des

[28] R. Baron, « Introduction aux technologies blockchain supports des crypto-monnaies », Dossier « Monnaies », RDBF n°4, juill. 2019, p.40.
[29] https://bitcoin.fr/vocabulaire/ (consulté le 31/05/2020) : voir la définition du minage : « (…) *Le minage est un marché compétitif où les revenus sont divisés en fonction du nombre de calculs effectués. Ce ne sont pas tous les utilisateurs du Bitcoin qui font du minage et il ne s'agit pas d'un moyen facile de gagner de l'argent* ».
[30] Pour la fondation Ethereum par exemple voir : https://ethereum.org/foundation/ (consulté le 31/05/2020).
[31] C. mon. fin., art. L54-10-2. Voir à ce sujet les commentaires : H. de Vauplane, « Les prestataires de services sur actifs numériques de la loi PACTE », RTDF n°4, oct. 2018, p.78-80 ; D. Stucki, S. Clavé, « Le nouveau statut du prestataire de services en crypto-actifs », RB n°830, mars 2009, p.48-51 ; D. Legeais, « Loi PACTE : les dispositions relatives aux actifs numériques et aux prestataires de services numériques », Dossier spécial sur la loi relative à la croissance et la transformation des entreprises, JCP E n°26, 27 juin 2019, p.1333-1338 ; T. Bonneau, A.-C. Rouaud, P. Pailler, R. Vabres, A. Tehrani, *Droit financier*, Précis Domat coll. droit privé, LGDJ, 2e ed., oct. 2019, n°447-504.

prestataires techniques et stratégiques accompagnant l'usage de la technologie *blockchain*[32]. L'équilibre des *blockchains* réside donc en un jaugeage subtil entre ces acteurs. Enfin, inévitablement, l'intervention d'un fournisseur d'accès à Internet dans un réseau accessible en ligne est requise.

10. **Usages schématiques de la technologie *blockchain*.** Cette technologie est souvent associée à trois grandes catégories d'usages schématiques. Si ces usages sont traditionnellement distingués, ils se combinent en pratique[33]. Le premier usage sommaire et emblématique de la *blockchain* est le transfert de valeur, autrement dit, l'échange de crypto-monnaies. D'autres usages plus sophistiqués se sont développés progressivement, comme celui du contrat intelligent (ou « *smart contract* »), de la « *tokenisation* », ou du registre de données. Ces différents usages seront mobilisés pour la compréhension des enjeux pratiques de cette étude et leurs illustrations.

11. **Usage par l'échange de crypto-actifs.** Il est difficile et rare de séparer une solution basée sur la technologie *blockchain*, d'un actif numérique (crypto-monnaie ou jeton utilitaire), ou plus largement d'un crypto-actif[34]. Même si certains usages n'ont pas comme objectif principal d'être employés pour le transfert de crypto-actifs, ils en incluent cependant souvent un[35]. Chaque transaction dans une *blockchain* suppose l'échange d'un crypto-actif quelconque, en particulier celui d'une crypto-monnaie[36].

12. **La crypto-monnaie.** L'échange de crypto-monnaies est la première branche de la catégorie des actifs numériques[37]. Sa représentation la plus aboutie est l'échange de bitcoins

[32] Par exemple, ConsenSys, IBM, Microsoft qui déploient des solutions techniques liées à la *blockchain*.
[33] Voir *infra* n°19 et s. les développements selon lesquels chaque usage sera différent en pratique.
[34] OPECST, rapport (par V. Faure-Muntian, C. de Ganay, R. Le Gleut), Les enjeux technologiques des *blockchains* (chaînes de blocs), 20 juin 2018, p.66 et Rapport France stratégie (présidé par J. Toledano), Les enjeux des *blockchains*, *op.cit.*, p.11. Voir l'opinion contraire qui tend à distinguer la technologie des crypto-monnaies : T. I. Kiviat, « Beyond bitcoin: issues in regulating blockchain transactions », Duke Law Journal, Vol. 65:569, 2015, p.569-608.
[35] A. M. Antonopoulos, *Mastering Bitcoin : Unlocking Digital Cryptocurrencies*, O'Reilly Media, Inc., 3 dec. 2014, p.230.
[36] Institut Sapiens, Y. de Monbynes et G. Grandval, Rapport Bitcoin totem et tabou. Que présage l'essor des crypto-monnaies ?, *op.cit.*, p.9, 10, 17 : « *En nous focalisant sur la fameuse "technologie blockchain", nouveau totem moderne, et sur les travers des crypto-monnaies, jusqu'à transformer Bitcoin en quasi-tabou, nous commettons deux erreurs préoccupantes (…) d'une part (…), d'autre part, nous négligeons le fait que la monnaie est la première "killer app" de ce que l'on appelle vaguement la "technologie blockchain", tout en étant également un rouage essentiel de son fonctionnement* ». Les arguments avancés que « *"ce qui compte, ce n'est pas le bitcoin, c'est la technologie derrière lui" a permis d'évacuer un peu trop rapidement le fait que, sans crypto-monnaie, les blockchains contemporaines n'existent pas. En négligeant Bitcoin, on se prive d'éléments précieux pour comprendre le phénomène plus global de la "blockchain"* ».
[37] C. mon. fin., art. L54-10-1, 2°.

mais il existe à l'heure actuelle 5 500 crypto-monnaies recensées[38]. En droit français, une crypto-monnaie n'est pas considérée comme équivalente à une monnaie légale[39]. Elle échappe à la qualification de monnaie à cours légal étant donné que seul l'euro est l'unité de compte officielle et permet le paiement d'une obligation de somme d'argent[40]. Elle n'entre pas non plus, généralement, dans le champ de la monnaie électronique puisqu'elle n'est pas émise contre la remise de fonds aux fins d'opérations de paiement[41]. Pourra être retenue, la qualification de monnaie conventionnelle permettant l'usage des crypto-monnaies comme un moyen de paiement[42]. Les parties sont, en effet, libres de payer des obligations issues d'un contrat international dans la devise qu'ils souhaitent[43]. Cette position est d'ailleurs accréditée par la Cour de justice de l'Union européenne (CJUE) précisant dans son arrêt dit « *bitcoin* » du 22 octobre 2015 que « *la devise virtuelle "bitcoin" étant un moyen de paiement contractuel elle ne saurait, d'une part, être regardée ni comme un compte courant ni comme un dépôt de fonds, un paiement ou un virement (…)* »[44]. Hormis la définition en creux de « *représentation numérique d'une valeur qui n'est pas émise ou garantie par une banque centrale ou par une autorité publique, qui n'est pas nécessairement attachée à une monnaie ayant cours légal et qui ne possède pas le statut juridique d'une monnaie, mais qui est acceptée par des personnes physiques ou morales comme un moyen d'échange et qui peut être transférée, stockée ou échangée électroniquement* » visée par la loi PACTE et son appartenance au régime juridique des actifs numériques, la crypto-monnaie ne dispose pas à ce jour de définition positive et de qualification juridique certaine[45].

[38] Ce chiffre est variable en fonction des périodes. Voir : https://coinmarketcap.com/ (consulté le 31/05/2020).
[39] Cette position est partagée unanimement par la doctrine : L. Corbion-Condé, « De la défiance à l'égard des monnaies nationales au miroir du bitcoin», RDBF n°2, dossier 13, mars 2014 ; J. Lasserre-Capdeville, « Le Bitcoin », JCP E, 2014, act. 25 ; M. Roussille, « le bitcoin : objet juridique non identifié », Rev. Banque et droit n°159, 2015, p.27 ; T. Bonneau, « Le bitcoin, une monnaie ? », Rev. Banque et droit, 2015, p.8 ; D. Legeais, « Aspects juridiques », Dossier n°30 « Les monnaies », actes de conférence, RDBF n°4, juill.-août 2019, p.35.
[40] C. mon. fin., art. L111-1. et C. civ., art. 1343-3, al. 1.
[41] C. mon. fin., art. L315-1.
[42] Les auteurs soutenant cet avis : J. Huet, « Le bitcoin, dont la légalité paraît admise, est une sorte de monnaie contractuelle », RDC 2017, n°113, le 01/03/2017 ; G. Marain, « Le bitcoin à l'épreuve de la monnaie », AJ Contrat, dec. 2017 p.525.
[43] C. civ., art. 1343-3, al. 2.
[44] CJUE 22 octobre 2015, aff. C-264/14 Skatteverket c. David Hedqvist : note J. Huet, RDC 2017, n°113, p.54 ; note R. Vabres RISF 2016 n°1, p.170 ; adde : Th. Bonneau, « Analyse critique de la contribution de la CJUE à l'ascension juridique du bitcoin », *in* Liber amicorum Blanche Sousi, L'Europe bancaire, financière et monétaire, Rev. Banque 2016.
[45] Voir n°38 et D. Legeais, « Loi PACTE : les dispositions relatives aux actifs numériques et aux prestataires de services numériques », JCP E n°26, 27 Juin 2019, p.1324, n°10. Notons cependant qu'un arrêt est venu préciser la nature juridique du bitcoin : un actif incorporel fongible (T. com. Nanterre, 26 févr. 2020, n°2018F00466, BitSpread c/ Paymium : com. G. Marraud des Grottes, RLDI n°168, p.49-51 ; com. L. Costes, RLDI n°168, p.40 ; com. M. Julienne, JCP E n°19, p.41-44 ; N. Mathey, LEDB avr. 2020, p.1).

13. **Le jeton.** L'usage des jetons (ou *tokens*) est couramment baptisé opération de « *tokenisation* ». C'est une « *représentation digitale de valeur fongible et divisible* »[46] qui ouvre la possibilité de créer un jeton personnalisé pour représenter un titre financier ou un droit d'usage afin de l'introduire dans la *blockchain*. La *tokenisation* est dès lors une opération par laquelle un émetteur peut représenter, *via* un jeton, un actif ou un droit qui sera par la suite inscrit dans la *blockchain*. L'émetteur peut décider d'émettre une ou plusieurs catégories de jetons de manière automatisée en contrepartie du versement de fonds en crypto-monnaies ou en monnaies ayant cours légal par le souscripteur. Sur le plan juridique, une qualification souple des jetons est retenue selon leurs caractéristiques : droits d'usage, titres financiers, ou encore biens divers[47]. Plusieurs qualifications du jeton pourront ainsi être choisies par l'émetteur corrélativement à la fonction économique dudit jeton[48].

14. Dans un premier temps, le jeton utilitaire (ou *utility token*) offre un droit d'usage à son détenteur sur la technologie ou sur les services développés puis distribués par l'émetteur. Il correspond à une vente anticipée du droit d'utiliser un service ou d'acheter un produit. Par exemple, Telegram a réalisé une levée de fonds par la *blockchain* sous forme d'*initial coin offering* (ICO) d'un montant s'élevant à 1,7 milliard de dollars en février et mars 2017 en contrepartie de jetons utilitaires souscrits par des investisseurs[49]. Ceux-ci donneront droit à des services ou des avantages relatifs à la *blockchain* intitulée « *Ton* »[50]. Seuls ces jetons utilitaires

[46] La définition intégrale du rapport dit « *Landau* » précise que le jeton est une « *représentation digitale de valeur fongible et divisible pouvant circuler sur Internet et être échangée de pair-à-pair (peer-to-peer) sans preuve obligatoire d'identité et avec une finalité de paiement* » (Ministère de l'Économie et des Finances, Rapport J.-P.Landau avec la collaboration d'A. Genais, Les crypto-monnaies, 4 juill. 2018, p.4).

[47] A ce sujet, le Programme d'étude de l'Autorité des Marchés Financiers (AMF) « *Universal Node to ICO's Research & Network* » (UNICORN) a considéré que le token peut être qualifié de token d'usage ou token droit politique ou financier. La doctrine est plus divisée, selon Th. Bonneau : les tokens ne sont jamais des titres financiers et appel le législateur à adopter une réglementation *sui generis* nouvelle pour ces opérations (Th. Bonneau, Tokens, titres financiers ou biens divers, RD banc. Fin, 2018) ; pour A-S. Grimaldi : « *si le token offre un droit aux dividendes, un droit sur le boni de liquidation et des droits politiques, ou un droit à obtenir remboursement des sommes prêtées, la qualification qui s'impose est celle de titre de capital (action) ou de titre de créance (obligation) et le régime à appliquer est celui des titres financiers* » (A-S. Grimaldi, « Les contraintes du droit des obligations sur les opérations d'ICO », D. n°21, le 7 juin 2018, p.1171). En revanche, aux États-Unis, le jeton est considéré comme un titre financier (SEC, 25 july 2017, release no. 81207).

[48] Voir plus en détails l'analyse de la « token economy » (A. Barbet-Massin, P. Lorentz, A. Bensoussan, « La mise en œuvre d'une ICO : les étapes en pratique », Etude n°1, RDBF n°1, janv.-févr. 2019, p.20).

[49] https://www.capital.fr/entreprises-marches/gram-la-crypto-monnaie-de-telegram-prete-a-inonder-le-monde-1328811 (consulté le 31/05/2020). Notons toutefois, que la *Securities and Exchange Commission* (SEC) bloquerait actuellement les fonds pour défaut d'enregistrement notamment (https://www.lemonde.fr/economie/article/2019/10/12/le-gendarme-americain-des-marches-bloque-la-levee-de-fonds-de-telegram-aux-États-unis_6015218_3234.html (consulté le 31/05/2020)).

[50] https://ico-telegram.org/tech-wp-ico-telegram-org.pdf (consulté le 31/05/2020).

intègrent la seconde branche des actifs numériques contrairement aux jetons financiers qui en sont exclus[51].

15. Le jeton financier (ou *security token*), dans un second temps, offre des droit financiers à son détenteur et est qualifié d'instrument financier, le soumettant aux législations sur les valeurs mobilières. Par exemple, il est possible d'émettre des instruments financiers, comme des actions ou obligations sur la *blockchain* afin de réaliser une opération intégralement numérique nommée « *security token offering* » (STO). À titre d'illustration, une filiale de la Société Générale a émis des obligations s'élevant à un montant de 100 millions d'euros sous forme de jetons inscrits dans la *blockchain* Ethereum en avril 2019[52]. Notons que le régime applicable au jeton est, par conséquent, celui applicable au droit qu'il représente *via* cette opération de qualification préalable.

16. **Usage du *smart contract*.** Les *smart contracts* sont des programmes informatiques intégrés dans une transaction de la *blockchain* qui auto-exécutent tout ou partie d'un contrat. Concrètement, si une condition préalablement déterminée est vérifiée, la conséquence prévue sera automatiquement exécutée (fonctionnement sur le modèle « *if…, then…* »). Le *smart contract* est souvent déployé dans la *blockchain* pour conditionner une remise de fonds à venir. Mis en place tout d'abord au cœur des crypto-monnaies, dans le cadre du réseau Ethereum, les *smart contracts* sont utilisés pour divers applications comme les ICOs, les STOs, les paris en ligne, les assurances etc.

17. Les contrats intelligents ont été élaborés à l'origine par Nick Szabo - informaticien, cryptographe et juriste - comme des contrats numériques[53]. Ils sont perçus par les développeurs technophiles comme ayant des implications d'autant plus larges que celui du simple langage contractuel : celles de « *boîtes cryptographiques qui contiennent de la valeur et ne la déverrouillent que si certaines conditions sont remplies* »[54]. Au contraire, pour la doctrine française, ils ne sont « *ni des contrats, ni intelligents* » mais de simples logiciels[55].

---

[51] Branche visée par la loi PACTE : C. mon. fin., art. L54-10-1, 1°.

[52] https://www.societegenerale.com/fr/newsroom/premiere-obligation-securisee-sous-forme-de-security-tokens-sur-une-blockchain-publique (consulté le 31/05/2020).

[53] N. Szabo, « Smart contracts : building blocks for digital markets », 1996 ; N. Szabo, « Formalizing and securing relationships on public networks », 2 sept. 1997 ; N. Szabo, « The Idea of Smart contracts », 1997.

[54] V. Buterin, « Ethereum White Paper. A Next Generation Smart contract & Decentralized Application Platform », http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf (consulté le 31/05/2020).

[55] Voir *infra* n°416.

18. **Usage du registre distribué de données.** Les registres certifiant de données distribués entre différents acteurs font partie intégrante de l'innovation technologique projetée à l'origine (registre de transactions en bitcoins distribué entre participants). Cet usage permet de certifier des données en quantité variable (souvent restreinte), chiffrées ou en clair, grâce à leurs inscriptions dans une transaction de la *blockchain*. Le stockage de ces données dans le registre distribué garantit également leur date d'existence et leur intégrité. Par exemple, cette forme d'usage est pertinente pour la certification d'un processus créatif d'une œuvre de l'esprit de bout en bout ou encore des étapes successives de la chaîne de distribution d'un produit. Elle offre les avantages d'auto-certifier des données de manière sécurisée par les procédés cryptographiques, d'offrir une traçabilité de ces données grâce au registre immuable et transparent de la *blockchain*, ainsi que de rationaliser et numériser ces processus de certification induisant davantage de fluidité et des baisses de coûts[56]. Manuel Aráoz et Esteban Ordanoun, des développeurs, pionniers de la « *preuve d'existence* » décentralisée de données dans la *blockchain*, ont commercialisé en 2013 un service en ligne open source « *Proof of existence* » basé sur le protocole Bitcoin[57]. Cet usage se retrouve en droit français sous la notion de « *dispositif d'enregistrement électronique partagé* » (DEEP) pour certains titres financiers[58].

19. **Définition stricte : « *les* » *blockchains*.** Le champ des possibles dans l'utilisation des *blockchains* étant pléthorique, chaque *blockchain* désigne un cas particulier changeant en fonction de la typologie de *blockchain* (publique ou privée et non-permissionnée ou permissionnée) et de la nature d'un protocole informatique précis[59]. Par exemple, la *blockchain* développée par les greffiers des tribunaux de commerce a pour but de mettre à jour les documents du registre du commerce et des sociétés. Cet usage d'espèce qui met en œuvre une *blockchain* de type privée permissionnée se base sur le protocole Hyperledger sous-jacent déterminant les règles de fonctionnement de cette *blockchain*[60].

[56] Parlement européen, Résolution du 3 oct. 2018 sur les technologies des registres distribués et les chaînes de blocs: renforcer la confiance par la désintermédiation (2017/2772(RSP)), P8_TA(2018)0373, point B.
[57] https://proofofexistence.com/ (consulté le 31/05/2020).
[58] Voir *infra* n°37.
[59] Voir les développements sur les protocoles types (Bitcoin, Ethereum, Hyperledger, Corda) dans la partie préliminaire.
[60] Communiqué de presse, « Le Conseil national des greffiers des tribunaux de commerce annonce le déploiement d'un réseau *blockchain* développé par IBM permettant de fluidifier et de sécuriser la gestion du registre du commerce et des sociétés », 14 mars 2019, https://www.cngtc.fr/myfiles/files/Communique%20*Blockchain*%20Version%20finale.pdf (consulté le 31/05/2020).

20. **Typologie des *blockchains*.** Variablement à sa finalité, une *blockchain* déployée pourrait être de deux types très distincts en fonction de sa nature (publique ou privée) et en fonction des droits qu'elle accorde (non-permissionnée ou permissionnée).

21. ***Blockchain* publique.** Lorsqu'elle est publique, la *blockchain* est ouverte à tous en lecture, en écriture, comme à la validation des transactions. Par exemple, Bitcoin est une *blockchain* publique dédiée à la transmission de la crypto-monnaie bitcoin[61]. Pour la lecture, il est possible à chacun de télécharger le registre des transactions répertoriées depuis la création de cette *blockchain*[62]. Pour obtenir une copie du registre des transactions en bitcoins, le téléchargement peut durer plusieurs jours et il convient de disposer de 200 gigaoctets d'espace disponible sur son disque[63]. À l'écriture, chaque individu souhaitant se créer un compte peut réaliser une transaction en envoyant des bitcoins à un autre individu. Concernant la validation, n'importe quelle personne peut décider de devenir validateur[64].

22. ***Blockchain* privée.** À l'inverse, avec une *blockchain* privée, une ou plusieurs personnes physiques ou morales participent au contrôle direct ou indirect de cette *blockchain*. Seuls certains participants se voient alors octroyer des droits sur le réseau, comme celui d'écriture permettant d'effectuer des transactions, de validation desdites transactions, et souvent de modification, de lecture ou encore d'audit du protocole et du registre. Pour des raisons de gouvernance, la validation et la correction *a posteriori* d'une erreur peut être en pratique le fait d'un nœud central. Par exemple, la Banque de France s'est équipée d'une *blockchain* privée pour gérer les identifiants des créanciers émettant des prélèvements afin d'assurer une diffusion immédiate de l'information au sein des établissements bancaires participants[65]. En tant que

---

[61] A l'origine, le protocole Bitcoin est conçu exclusivement pour l'échange de crypto-monnaies mais progressivement, ce protocole est utilisé comme base pour des applications diverses, notamment la certification de données.

[62] K. Wüst, A. Gervais, « Do you need a Blockchain ? », actes de colloque *in* Crypto Valley Conférence sur la Technologie Blockchain Technology 2018 (CVCBT), le 20-22 juin 2018, p.2 : ces chercheurs en sciences de l'informatique parlent de « *vérifiabilité publique* » puisque « *tout observateur peut vérifier que l'état du registre a été modifié conformément au protocole et aura éventuellement la même vue du registre, au moins jusqu'à une certaine longueur* » alors que « *dans un système centralisé, les différents observateurs peuvent avoir des points de vue totalement différents sur l'état d'un registre. Par conséquent, il se peut qu'ils ne soient pas en mesure de vérifier tous les états par lesquels transitent le registre et leurs correctes exécutions. Les observateurs doivent plutôt faire confiance à l'entité centrale pour leur fournir l'état correct d'un registre* ».

[63] https://bitcoin.org/en/full-node#secure-your-wallet (consulté le 31/05/2020).

[64] A. M. Antonopoulos, *mastering bitcoin : unlocking digital cryptocurrencies*, *op.cit.*, p.19. Pour les explications sur le rôle du validateur : voir *supra* n°7.

[65] Cette *blockchain* aurait pour avantages essentiels d'accélérer les processus opérationnels et d'alerter des fraudes (voir : Audition France Stratégie, La technologie blockchain : le point de vue banque centrale, le 26/04/2017, https://www.strategie.gouv.fr/sites/strategie.gouv.fr/files/atoms/files/audition_france_strategie_banque_de_france-blockchain-crypto-monnaies_lecture_seule.pdf (consulté le 31/05/2020)).

personne morale, elle désigne les établissements bancaires autorisés à utiliser cette *blockchain*. Ou encore Carrefour introduit une *blockchain* privée pour garantir la traçabilité alimentaire de divers produits. L'entreprise Carrefour en tant que personne morale est gérante de la *blockchain* assurant le contrôle de l'historique des échanges effectués entre les producteurs, transformateurs et distributeurs[66].

23. Dans ces *blockchains* privées, une sous-catégorie vise les *blockchains* de consortium. Elles permettent le déploiement d'un registre distribué entre différents membres participants (nœuds) souvent représentés par des personnes morales, des acteurs économiques ou des institutions ayant un intérêt à partager de données ensemble. Ce registre est alors hébergé par ces membres (nœuds)[67]. La gouvernance de ce type de *blockchain* est majoritairement organisée par l'intermédiaire d'une personne morale dédiée et un ensemble d'engagements contractuels permettant de prévoir les droits et obligations des membres. Par exemple, Libra le consortium prévu pour le lancement de la crypto-monnaie « *libra* » de Facebook serait déployé sur cent nœuds partenaires du projet et la gouvernance s'organise autour d'une association de droit Suisse[68].

24. ***Blockchain* Permissionnée/non-permissionnée.** Il arrive qu'en plus de leur nature, certains droits soient ajustés à la *blockchain*. La *blockchain* est dite non-permissionnée quand tous les participants disposent des mêmes droits (lecture, écriture, validation pour l'essentiel) accordés dans une *blockchain*. La *blockchain* est dite permissionnée quand il existe des droits différents et spécifiques (lecture, écriture, validation, modification, contrôle ou audit par exemple) à certains utilisateurs. Généralement, une *blockchain* publique est non-permissionnée et inversement une *blockchain* privée est permissionnée. Toutefois, la *blockchain* Ethereum est l'exemple illustrant l'intérêt de ce critère des droits accordés : c'est une *blockchain* non-permissionnée de base mais certains projets sont permissionnés.

25. **Nature des protocoles de *blockchain*.** Le protocole, véritable ADN de la *blockchain*, établit des règles de fonctionnement destinées à permettre l'échange de valeurs et, plus

[66] Communiqué de presse, « Carrefour lance la première *blockchain* alimentaire d'Europe et étendra cette technologie à 8 autres filières d'ici fin 2018 », 6 mars 2018, https://www.carrefour.com/fr/newsroom/carrefour-lance-la-premiere-blockchain-alimentaire-deurope (consulté le 31/05/2020).
[67] S. de Thésut Dufournaud, « La blockchain de consortium », RLDA n°129, sept. 2017.
[68] https://libra.org/en-US/association/ (consulté le 31/05/2020).

largement de données, entre deux ordinateurs[69]. Les protocoles Bitcoin[70], Ethereum[71], Tezos[72], Hyperledger[73], Corda[74], Quorum[75] sont à titre d'exemple développées comme bases protocolaires à certaines *blockchains*. En toute hypothèse, seront étudiés - restrictivement -, au long de cette recherche, les protocoles majoritairement utilisés par les entités publiques et privées : Bitcoin, Ethereum, Corda, Hyperledger[76].

26. Pour faire évoluer ces protocoles, des modifications sont possibles dans l'hypothèse de « *fork* » (ou « *bifurcation* »). C'est une modification des codes sources du protocole après un accord des mineurs de la *blockchain*. Il existe deux types de *fork*. Le « *soft fork* » qui est une amélioration du protocole compatible avec la version précédente. Le registre des transactions originel est alors naturellement poursuivi. Par exemple, un *soft fork* peut être voté pour une mise à jour du logiciel. À l'inverse, le « *hard fork* » rend la nouvelle version incompatible avec l'ancienne, les transactions à venir ne s'inscriront donc plus dans le registre initial. Un nouveau registre est donc créé. L'ancien et le nouveau registre co-existent et des transactions peuvent être opérées dans chacun d'eux. Par exemple, un *hard fork* peut être voté pour incorporer une nouvelle fonctionnalité ou inverser les effets d'une action malintentionnée d'un développeur, comme le premier *hard fork* voté pour le protocole Ethereum suite au détournement de fonds du projet « *the DAO* »[77]. Désormais, il existe deux registres Ethereum et Ethereum classic ainsi que deux crypto-monnaies associées l'ether et l'ether classic.

27. À titre de comparaison, Internet est basé sur un protocole IP (*Internet Protocol*), spécifié par l'Internet Society[78]. Destiné à l'échange de messages électroniques, d'informations multimédias et de fichiers, ce protocole permet à des ordinateurs de communiquer entre eux au sein d'un réseau mondial[79]. Ce protocole commun achemine de proche en proche des messages

[69] Un protocole informatique est un « *ensemble de règles définissant le mode de communication entre deux ordinateurs* » (https://www.larousse.fr/encyclopedie/divers/protocole/83819 (consulté le 31/05/2020)).
[70] https://bitcoin.org/fr/ (consulté le 31/05/2020).
[71] https://www.ethereum.org/ (consulté le 31/05/2020).
[72] https://tezos.com/ (consulté le 31/05/2020).
[73] https://www.hyperledger.org/community/basics (consulté le 31/05/2020).
[74] https://www.r3.com/history/ (consulté le 31/05/2020).
[75] https://www.goquorum.com/ (consulté le 31/05/2020).
[76] Voir leurs intérêts respectifs dans le domaine de la preuve au sein de la partie préliminaire.
[77] Voir la question : « "*Hard fork*", "*soft fork*", qu'est-ce que c'est ? », https://bitcoin.fr/faq/ (consulté le 31/05/2020).
[78] Vocabulaire de l'informatique et de l'internet : liste des termes, expressions et définitions adoptés, Commission générale de terminologie et de néologie, NOR : CTNX9903444K, publié au JO le 16 mars 1999, p.3905-3910.
[79] A l'origine d'Internet dans les années 1960, il s'agissait de développer un réseau de communication entre divers ordinateurs de laboratoire universitaires sous le pilotage de l'Advanced Research Projects Agency (ARPA), l'agence de recherche du ministère américain de la Défense. C'est en 1974 que Robert Kahn et Vinton Cerf concevaient le protocole TCP/IP qui permettait de faciliter ces échanges. Le réseau Arpanet adoptait ensuite, en

découpés en paquets indépendants. Il est considéré comme le protocole originel et symbolique de la gestion décentralisée en réseaux interconnectés[80]. À ensuite suivi, le protocole SMTP (*Simple Mail Transfer Protocol*) basé technologiquement sur un standard ouvert et développé dans le domaine de la communication des courriers électroniques. Ce protocole décentralisé SMTP permet à toutes personnes d'exploiter son propre serveur de messagerie.

28. **Couches protocolaires.** Plusieurs couches protocolaires peuvent coexister dans une *blockchain* et ses services développés autour. La couche basse du protocole constitue le noyau de la *blockchain*, c'est-à-dire la base des règles de la *blockchain* et du registre distribué. Par ailleurs, peuvent se superposer au protocole initial, une ou différentes couches de solution, comme des applications qui seront construites sur le protocole[81]. Généralement, ces applications sont centralisées et permettent d'identifier un ou des gérants, contrairement aux protocoles *blockchains* décentralisés (pour les *blockchains* publiques à tout le moins). Par exemple, certains services créent des applications de signature et d'horodatage basées sur la *blockchain* en utilisant le protocole Bitcoin.

29. Un parallèle peut encore être réalisé avec Internet. L'application - désormais devenue incontournable - baptisée WWW (*World Wide Web)* ou autrement appelée « *Web* » développée grâce au protocole HTTP (*Hypertext Transfer Protocol*) fonctionnant sur la base du protocole TCP/IP (*Transmission Control Protocol/Internet Protocol*) offre la possibilité de consulter à distance des pages multimédias[82].

30. Par ailleurs, l'implémentation de ces protocoles au sein d'entreprises ou d'institutions publiques, sont établis, configurés et déployés par des fournisseurs de services. Dans ces cas, le client se charge généralement de la gestion des fonctionnalités de sa *blockchain* et le

1983, officiellement cette norme de protocole et Internet pris réellement essor en conséquence avec un millier de postes utilisateurs (P.Mounier-Kuhn, « Développement du réseau internet », Encyclopédie Universalis, https://www.universalis.fr/encyclopedie/protocole-informatique/ (consulté le 31/05/2020)).

[80] Vocabulaire de l'informatique et de l'internet : liste des termes, expressions et définitions adoptés**,** Commission générale de terminologie et de néologie - NOR : CTNX9903444K, publié au JO le 16 mars 1999, p.3905-3910.

[81] A. Barbet-Massin, W. O'Rorke, Fiche pratique n°4317 - Blockchain et données personnelles, Lexis Nexis, juill. 2019 : « *il est important de distinguer la différence entre la couche protocolaire – la blockchain sous-jacente – et ses applications fonctionnant « au-dessus », à l'instar de Facebook s'appuyant sur le protocole Internet* » ; Pour le Cambridge Centre for Alternative Finance, il existe une couche de protocole, une couche de réseau et une couche d'application (Cambridge Centre for Alternative Finance, University of Cambridge Judge Business School, Global blockchain benchmarking study, ss. dir. G. Hileman, M. Rauchs, 2017, p.12).

[82] D. Dromard, D Seret, « Internet, les applications », Encyclopedie Universalis, https://www.universalis.fr/encyclopedie/internet-les-applications/ (consulte le 31/05/2020).

prestataire a, lui, la tâche de la performance de l'infrastructure initiale. Les solutions de « *Blockchain as a Service* » (BaaS) sont de nouvelles prestations de services proposées par ces fournisseurs. En substance, ce sont des applications basées sur la technologie *blockchain* proposées par des prestataires avec un système d'hébergement de celles-ci dans le cloud, en dehors de la *blockchain*[83].

31. **Droits attachés aux protocoles.** Les protocoles *blockchains* sont mis en œuvre au moyen de logiciels appelés logiciels clients. Par exemple, le protocole Bitcoin fonctionne grâce au logiciel client Bitcoin Core[84]. Les codes sources de ces logiciels sont généralement publiés sous licences libres ou open source. Ces logiciels s'ancrent dans le « *mouvement du libre* » selon lequel l'accès au code source, qui est la version lisible d'un logiciel par un homme de l'art, est un moyen de comprendre, de modifier et faire évoluer le logiciel. En d'autres termes simples, le code source du logiciel est libre. Afin de mettre en place cet accès libre au code, les licences de logiciels peuvent organiser des régimes particuliers.

32. Le logiciel client de Bitcoin a été publié et diffusé sous le régime de la licence open source du MIT dès l'annonce de la création de Bitcoin le 17 juillet 2009 par Satoshi Nakamoto sur le site de la « *P2P Foundation* »[85]. Cette licence permet d'utiliser, copier, modifier, fusionner, publier, distribuer, sous-licencier et/ou vendre des copies du logiciel, sous réserve d'insérer une notice de copyright dans toutes les copies ou parties substantielles du logiciel. Dans l'hypothèse de modification ou distribution du logiciel, elle ne contraint toutefois pas à conserver la même licence et des termes analogues à cette licence (non copyleft)[86]. Les licences Apache 2.0 et GNU/GPL 2 ont ensuite été choisies respectivement pour les logiciels des protocoles Hyperledger[87] et Ethereum[88]. Qui plus est, les sources utilisées pour développer les protocoles et des applications autour de ces logiciels clients sont aussi issues la plupart du temps de logiciels libres et open source[89]. Les entreprises et institutionnels qui décident d'ouvrir leur

[83] X. Biseul, « Blockchain as a Service : quelle solution choisir pour se lancer ? », JDN, 14 mars 2018, https://www.journaldunet.com/solutions/cloud-computing/1206955-*blockchain*-as-a-service-quelle-solution-choisir/ (consulté le 31/05/2020) ; M.-A. Ledieu, « La Baas démocratise la blockchain », Expertises des systèmes d'information n°440, nov. 2018, p.365-369.
[84] A. M. Antonopoulos, *Mastering Bitcoin : Unlocking Digital Cryptocurrencies*, *op.cit.*, p.31-32.
[85] https://fr.wikipedia.org/wiki/Bitcoin_Core (consulté le 31/05/2020).
[86] https://opensource.org/licenses/MIT (consulté le 31/05/2020).
[87] https://wiki.hyperledger.org/display/HYP/FAQ (consulté le 31/05/2020).
[88] https://github.com/ethereum/wiki/wiki/Licensing (consulté le 31/05/2020).
[89] *Ibid.*

base de codes liée à des applications sur la base de protocoles *blockchains* les publie majoritairement sous les licences Apache 2 et MIT[90].

33. Ces protocoles *blockchains* doivent, dans ce contexte, être qualifiés de « *communs* »[91], et plus précisément de « *communs numériques* »[92], c'est-à-dire des biens immatériels inappropriables, accessibles et ouverts à tous. Le commun au sens large est ce qui concerne tous les membres d'un groupe, par opposition à l'individuel[93]. Cette notion doctrinale polysémique de commun fait référence à des biens ni publics, ni privés mais davantage à une ressource dirigée par une communauté autonome qui s'organise pour la placer, gérer ses conditions d'accès et la protéger contre les menaces[94]. Cette notion englobe donc les dimensions de ressource, régime collectif et gouvernance et insiste sur la dynamique collective[95]. La communauté autonome de développeurs des protocoles de *blockchain* et les fondations afférentes assurent la gouvernance et l'évolution de ces protocoles[96]. Mais les menaces d'appropriation ne sont pas des moindres.

[90] 35% de licence Apache 2 et 31% de MIT sont utilisées (Cambridge Centre for Alternative Finance, University of Cambridge Judge Business School, Global blockchain benchmarking study, *op.cit.*, p.35, 42, 43).

[91] Voir la théorie développée par l'économiste E. Ostrom qui redonne un sens la notion de communs. Ses travaux relatifs aux communs fonciers sont à l'initiative du mouvement de réflexion sur des formes institutionnelles et juridiques nouvelles concernant les communs de façon large (E. Ostrom, *La gouvernance des biens communs : pour une nouvelle approche des ressources naturelles*, Editions de Boeck, 2010).

[92] Ce sont dans les années 1990 que nait au sein d'un réseau d'institutions universitaires, la rencontre entre le commun et le numérique. Notamment, le Berkman Center de l'Université de Harvard a mis en relation des acteurs et des idées liées au partage de l'information sur Internet. Lawrence Lessig développe une conception de la culture en tant que commun numérique en appliquant l'idée du libre à la culture (voir : L. Lessig, *the future of ideas, the fate of the commons in a connected world*, 2001, 384 p.). Ces communs numériques seraient donc des « *nouveaux modes d'administration d'une ressource informationnelle par une communauté, qui sont permis par les technologies de l'information et de la communication. Ils constituent un mode de partage de ressources socialement valorisées* » (H. Verdier et C. Murciano, « Les communs numériques : éléments d'économie politique », *Le cahier de la Chaire*, n°69, 2016, p.1), à l'instar des protocoles Internet et des logiciels libres (H. Le Crosnier, « Leçons d'émancipation : l'exemple du mouvement des logiciels libres », in *Libres Savoirs*, C&F éditions, 2011, p.176 et s.). Or, les protocoles *blockchains* semblent - par nature - être les derniers venus de ces communs numériques.

[93] G. Cornu, *Vocabulaire juridique*, Puf, 2014, p.206.

[94] Cette notion de commun aborde la ressource selon une approche différente. Elle dépasse l'opposition entre l'appropriation privée, l'absence d'appropriation et l'appropriation collective car elle ne s'intéresse pas à l'appropriation (J. Rochfeld, « Quel modèle pour construire des « communs » ? », in B. Parance, J. de Saint Victor (dir.), *Repenser les biens communs*, CNRS Editions, 2014, p.119). Les communs ne se réduisent à des schémas théoriques sans existences concrètes en témoignent les exemples puisés dans la pratique juridique contemporaine (Séminaire international « Propriété et Communs. Les nouveaux enjeux de l'accès et de l'innovation partagés », intervention de J. Rochfeld, « Quel(s) modèle(s) pour construire des « communs » ? Entre élargissement du cercle des propriétaires et dépassement de la propriété », le 25 et 26 avril 2013).

[95] V. Peugeot, *les communs. Une brèche politique à l'heure du numérique*, Presses des mines, 2013, p.6.

[96] Voir *supra* n°8.

34. Dans une logique antagoniste aux développements des protocoles *blockchains*, les monopoles se sont progressivement multipliés sur cette technologie (logiciels propriétaires[97] et brevets[98]). Par exemple, de nature permissive, la licence MIT offre une « *liberté fragile* »[99] au protocole Bitcoin et à ses concepteurs. Il est possible de redistribuer un logiciel sous une licence propriétaire (le nouveau programme pourrait passer de la catégorie des logiciels libres à celle des logiciels non libres)[100] et il expose la technologie *blockchain* aux différents monopoles des brevets[101]. Mais force est de constater que dans ces hypothèses, 60 % des fournisseurs d'infrastructures décident d'ouvrir les codes du protocole pour monétiser leur plateforme, alors que 44 % des éditeurs de logiciels propriétaires sont toujours indécis quant au choix de l'ouverture des codes ou d'en conserver la propriété, essentiellement pour des raisons de modèle d'affaires[102].

---

[97] Du reste, précisons que la monétisation de l'*infra*structure des protocoles se produit essentiellement au niveau du conseil et du développement d'applications (Cambridge Centre for Alternative Finance, University of Cambridge Judge Business School, Global blockchain benchmarking study, *op.cit.*, p.35).

[98] En 2018, le nombre total de dépôts de brevets concernant la *blockchain* s'élevait à 2220 aux États unis, en Europe, en Chine, au Japon et en Corée du Sud (OEB, Compte-rendu de conference « Patenting *blockchain* », Y. Ménière « the emerging blockchain patent landscape », 4 dec. 2018, https://www.epo.org/news-issues/news/2019/20190314.html (consulté le 31/05/2020)), alors que ces derniers étaient respectivement, entre 2013 et 2017, de 27, 98, 258, 594 et 1 248 (https://www.coindesk.com/global-*blockchain*-patent-filings-spiked-in-2017-koreas-ip-office-says/ (consulté le 31/05/2020)).

[99] Voir la classification des logiciels libres par le critère de la « *liberté* » permettant d'identifier les types de licences par rapport à leurs effets : M. Clément Fontaine, *Les œuvres libres*, thèse ss dir. M. Vivant, Montpellier, 2006 reprise par le CSPLA (CSPLA, avis 2007-1, La mise à disposition ouverte des œuvres de l'esprit, 26 juin 2007) et le Syntec et la FNILL (Guide open source – Réflexions sur la construction et le pilotage d'un projet open source).

[100] Notons, en revanche, que ces modèles libres et propriétaires de logiciels attachés aux protocoles *blockchains* peuvent coexister selon Lerner et Tirole. Ces auteurs sont les premiers à avancer que développer que les modèles propriétaires et Open Source des logiciels sont plus convergents que divergents. Autrement dit, des articulations sont finalement possibles entre des codes propriétaires et des codes ouverts. Les premiers exemples à ce sujet sont les licences open source qui déterminent des conditions de cette articulation en n'empêchant pas une captation ultérieure (J. Lerner et J. Tirole, « The scope of open source licensing », Journal of Law, Economics, and Organization, Oxford University Press, 2005).

[101] A. Barbet-Massin, A. Khatab, « Les "brevets blockchain" : état des lieux et perspectives », Expertises des systèmes d'informations, mai 2018, n°435, p.176 : « *Aucun terme de cette licence n'interdit en effet sa conjugaison avec les brevets d'invention. En pratique, cette licence est simple d'utilisation et s'applique particulièrement aux petits programmes. Un programme devenu aussi important que bitcoin n'est plus approprié à ce format de licence. Il n'est dès lors pas certain que le choix de cette licence par Satoshi Nakamoto soit de nature à préserver complètement le protocole bitcoin de toutes réservations monopolistiques. Les licences Apache 2.0 ou encore GNU/GPL 2 sembleraient plus adaptées. La première, utilisée par la blockchain privée Hyperledger, oblige les « contributeurs » à donner leurs brevets en licence dès lors qu'une de leurs innovations incorporerait le code source de cette blockchain. En outre, elle conditionne la licence à une renonciation à toute action en contrefaçon dont la blockchain en cause serait l'objet[101]. La seconde utilisée par la blockchain publique Ethereum, est une licence contaminante qui contraint tous logiciels sous les termes GNU/GPL à être distribués sous le même régime GNU/GPL (copyleft)* ».

[102] Cambridge Centre for Alternative Finance, University of Cambridge Judge Business School, Global blockchain benchmarking study, *op.cit.*, p.35. Aussi, un tiers (1/3) des fournisseurs d'*infra*structures de *blockchain* en cours de développement sur une base de protocoles propriétaires prévoient de les ouvrir dans un avenir proche (Cambridge Centre for Alternative Finance, University of Cambridge Judge Business School, Global blockchain benchmarking study, *op.cit.*, p.42).

35. Par ailleurs, le fait qu'un logiciel soit libre n'est pas de nature à l'exonérer, pour autant, des protections prévues par le droit d'auteur[103]. En principe, le choix du logiciel libre ou propriétaire n'a pas d'influence sur les éléments composant la *blockchain* qui sont protégeables au bénéfice des auteurs (développeurs et graphistes). La *blockchain* est mise en œuvre par une série de logiciels dont les codes sources (langage utilisé par le programmeur permettant d'écrire et de modifier le programme) et codes objets (langage informatique qui traduit le code source) sont protégés par le droit d'auteur[104], à condition que l'individu à l'origine d'une contribution originale sur un logiciel mis en œuvre par une *blockchain* prouve un « *apport intellectuel propre* » suffisant pour le rendre titulaire de droits (droit moraux sur la création et droits patrimoniaux sur l'exploitation)[105]. Le logiciel produit par son auteur resterait donc nécessairement attaché à sa personne dans la mesure où il n'est pas possible de renoncer à son droit moral en France[106]. Il existe néanmoins une possibilité d'éviter en pratique cette logique personnaliste du droit d'auteur français en divulguant un logiciel sous un pseudonyme ou de manière totalement anonyme, à l'image de la divulgation du logiciel du protocole Bitcoin par Satoshi Nakamoto.

36. **Définition juridique de la *blockchain*.** Une définition de la *blockchain* issue de la Commission générale de terminologie et de néologie de l'Académie Française publiée le 23 mai 2017 au Journal Officiel de la République Française au sein « *Vocabulaire de l'informatique* » est, pour le moment, la seule ayant une valeur juridique. Cette commission - assemblée de personnalités bénévoles, au centre d'un dispositif interministériel, placée sous le contrôle du premier ministre - est effectivement chargée de produire des termes et définitions correspondants aux nouvelles réalités d'un domaine. Derrière le terme « *chaîne de blocs* », cette commission a ainsi dégagé la définition d'un « *mode d'enregistrement de données produites en continu, sous forme de blocs liés les uns aux autres dans l'ordre chronologique de leur validation, chacun des blocs et leur séquence étant protégés contre toute modification* »[107]. Si la valeur de cette définition dans la hiérarchie des normes n'est pas évidente, elle serait, à tout le moins, assimilable aux « *autres* » actes administratifs.

---

[103] C. Caron, « Les licences de logiciels dits "libres" à l'épreuve du droit d'auteur français », D. 2003, p.1556.
[104] C. propr. intell., art. L112-2, 13°.
[105] Cass., ass. plén., 7 mars 1986, Pachot, n°83-10477, SA Babolat Maillot Witt c/ Pachot.
[106] C. propr. intell., art. L121-1 du code de la propriété intellectuelle « *L'auteur jouit du droit au respect de son nom, de sa qualité et de son œuvre. Ce droit est attaché à sa personne. Il est perpétuel, inaliénable et imprescriptible…* ». Voir : M. Clément-Fontaine, *Les œuvres libres*, thèse ss dir. M. Vivant, Montpellier, 2006, n°142.
[107] Vocabulaire de l'informatique (liste de termes, expressions et définitions adoptés), publié au JORF n°0121 du 23 mai 2017 texte n°20.

37. Employant l'expression du DEEP telle que mentionnée ci-avant[108], le Code monétaire et financier fait aussi référence, par circonlocution, à la *blockchain* pour son usage dans certains secteurs et cas précis. C'est le rapport au Président de la République de l'ordonnance n°2017-1674 du 8 décembre 2017 qui mentionne que ce dispositif recouvrira les principales caractéristiques de la technologie *blockchain* en tant que registre partagé[109]. La consécration du DEEP est reçue pour la première fois par l'ordonnance n°2016-520 du 28 avril 2016 relative aux bons de caisse dite « *minibons* » qui vise d'abord la possibilité d'inscrire dans ce dispositif l'émission et la cession de minibons[110]. C'est au tour ensuite de l'ordonnance n°2017-1674 du 8 décembre 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers dite « *blockchain* » d'ouvrir la possibilité d'une inscription en DEEP en lieu et place de celle en compte-titres[111]. Enfin, la dernière venue en sa représentation de la loi PACTE permet d'émettre, d'inscrire, de conserver ou de transférer dans un DEEP des jetons utilitaires[112]. Toujours est-il que ces ordonnances et la loi PACTE ne déterminent pas les caractéristiques et l'ensemble des propriétés essentielles ni du DEEP, ni de la *blockchain*, au sein d'une définition[113]. Ces textes n'apportent pas, en d'autres termes, de définition juridique au sens propre à cette technologie en tant que support d'échanges et de conservation de ces échanges[114]. Si le Professeur Hervé Causse condamne l'« *absence* » de définition juridique par l'impossible qualification juridique de la *blockchain*,

[108] Voir *supra* n°18.

[109] Rapport au Président de la République relatif à l'ordonnance n°2017-1674 du 8 décembre 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers, publié au JORF n°0287 du 9 décembre 2017 texte n°23 : « *Le terme de « dispositif d'enregistrement électronique partagé » (DEEP), employé dans l'habilitation, correspond à la manière dont la technologie « blockchain », entre autres, est déjà désignée par les dispositions de l'article L223-12 du Code monétaire et financier relatives aux minibons, introduites par l'ordonnance n°2016-520 du 28 avril 2016 relative aux bons de caisse. Cette désignation demeure large et neutre à l'égard des différents procédés afin de ne pas exclure des développements technologiques ultérieurs. Cette dénomination recouvre les principales caractéristiques de la « blockchain » : sa vocation de registre et son caractère partagé* ».

[110] C. mon. fin., art. L223-13.

[111] C. mon. fin., art. L211-3, al. 2.

[112] C. mon. fin., art. L552-2. Voir n°13 et s. pour la définition du jeton et ses différentes catégories.

[113] Voir les commentaires doctrinaux de la loi PACTE : O. Grégoire, « Loi PACTE », Dossier spécial sur la loi relative à la croissance et la transformation des entreprises, JCP E n°26, 27 Juin 2019, p.1317 et s., D. Legeais, « Loi PACTE : les dispositions relatives aux actifs numériques et aux prestataires de services numériques », Dossier spécial sur la loi relative à la croissance et la transformation des entreprises, JCP E n°26, 27 Juin 2019, p.1322 et s. ; F. Drummond, « Loi PACTE et actifs numériques », BJB n°4, juill. 2019, p.60 et s. ; T. Bonneau, A.-C. Rouaud, P.Pailler, R. Vabres, A. Tehrani, *Droit financier*, Précis Domat coll. droit privé, LGDJ, 2e ed., oct. 2019, n°447-504.

[114] La définition de « *définition* » selon le Larousse est le « *fait de déterminer les caractéristiques d'un concept, d'un mot, d'un objet, etc., ensemble des propriétés essentielles de quelque chose : La définition de ce mot n'est pas facile. La définition de produits nouveaux, du public à atteindre* » (https://www.larousse.fr/dictionnaires/francais/d%C3%A9finition/22700 (consulté le 31/05/2020).

il ne propose pas toutefois de définition pleinement satisfaisante, réduisant cette technologie à ses simples opérations juridiques, ce qui semble borner et restreindre son champ[115].

38. La loi PACTE précise, en revanche, quelle est la nature des unités échangées dans la *blockchain* : les actifs numériques. Cette nouvelle classe d'actifs n'est pas strictement définie par le législateur mais vise deux sous-catégories juridiques, elles-mêmes définies : les jetons et les crypto-monnaies[116]. D'une part, constituent des jetons inclus dans la loi PACTE les biens incorporels représentant des droits et, sont exclus expressément du champ de cette règlementation, les jetons qui remplissent les caractéristiques des instruments financiers et des bons de caisse[117]. Retenons que seuls les jetons utilitaires sont compris dans la loi PACTE, alors que les jetons financiers susceptibles de représenter des titres financiers sont soumis, quant à eux, à la règlementation relative aux titres financiers traditionnels[118]. D'autre part, la loi PACTE intègre dans son champ « *toute représentation numérique d'une valeur qui n'est pas émise ou garantie par une banque centrale ou par une autorité publique, qui n'est pas nécessairement attachée à une monnaie ayant cours légal et qui ne possède pas le statut juridique d'une monnaie, mais qui est acceptée par des personnes physiques ou morales comme un moyen d'échange et qui peut être transférée, stockée ou échangée électroniquement* »[119]. Cette définition en creux, introduit de manière non explicite au sein cette loi les « *monnaies virtuelles* » ou « *crypto-monnaies* ». Elle est d'ailleurs empruntée d'une définition de droit européen retenue dans la cinquième directive relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme[120]. Le choix sémantique de ne pas employer le terme « *monnaie* » virtuelle ou crypto-« *monnaie* » traduit la

[115] Selon le Professeur Hervé Causse : « *la blockchain est l'opération juridique par laquelle des blockchaineurs, réunis dans un système informatique qui vaut convention, sont des utilisateurs des droits que le système reconnaît, certifie, conserve et permet de transmettre, que le système soit libre et universel ou qu'il soit tenu par une personne, le blockchainant, qui en est, soit pleinement responsable en qualité propriétaire, soit simplement présumé responsable en qualité de gestionnaire.* » (H. Causse, « Première définition juridique de la *blockchain* ! », https://www.hervecausse.info/Premiere-definition-juridique-de-la-*blockchain*-_a1509.html, (consulté le 31/05/2020).

[116] C. mon. fin., art. L54-10-1.

[117] C. mon. fin., art. L552-2 : le jeton est défini ici comme « *tout bien incorporel représentant, sous forme numérique, un ou plusieurs droits* ».

[118] Voir aussi dans « - Procédure d'instruction et établissement d'un document d'information devant être déposé auprès de l'AMF en vue de l'obtention d'un visa sur une offre au public de jetons » l'inapplication de l'instruction aux jetons sécuritaires (*in* Instruction AMF DOC-2019-06, procédure d'instruction et établissement d'un document d'information devant être déposé auprès de l'AMF en vue de l'obtention d'un visa sur une offre au public de jetons, applicable au 6 juin 2019) .

[119] C. mon. fin., art. L54-10-1, 2°.

[120] Directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018 modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme ainsi que les directives 2009/138/CE et 2013/36/UE (Texte présentant de l'intérêt pour l'EEE), art. 1, 2), d).

réserve du législateur quant à l'ambiguïté qu'induit cette notion avec les monnaies ayant cours légal[121].

39. **Définition technique de la *blockchain*.** C'est au travers d'une infrastructure informatique originale que la singularité de la technologie *blockchain* se révèle. Elle désigne techniquement plusieurs éléments : des chaînes de blocs liés les uns aux autres constituant un registre support des transactions et un réseau organisé créant un consensus.

40. La *blockchain* vise des « *blocs* » regroupant des transactions qui se succèdent et contiennent l'empreinte numérique du bloc précédent. Ils constituent à ce titre une « *chaîne* » continue d'empreintes numériques reliées les unes aux autres, d'où le terme anglais « *block* »-« *chain* ». Ces blocs sont ajoutés à la chaîne successive des autres blocs et ceux-ci sont recensés dans un registre considéré, en conséquence, comme immuable[122]. La *blockchain* se rapporte, de cette façon, à un registre immatériel retraçant les blocs et les transactions des participants. Sur celui-ci, une ou plusieurs entrées (ou « *inputs* ») sont équivalentes à des débits sur un compte, alors qu'une ou plusieurs sorties (ou « *outputs* ») sont équivalentes à des crédits vers un compte[123]. Ces entrées et sorties constituent des transactions entre les participants, émetteurs et destinataires des transactions, dont les blocs sont vérifiés et validés par les validateurs du réseau. En effet, l'architecture du réseau d'une *blockchain* implique qu'aucun participant ne soit considéré comme *a priori* fiable, d'où la nécessité d'un consensus[124]. Par exemple, certains participants pourraient vouloir s'attribuer des bitcoins et ainsi inscrire une transaction fausse dans le registre.

41. La vérification des transactions d'un bloc permet de s'assurer qu'elles sont dites « *bien formées* ». Les validateurs du réseau doivent en ce sens vérifier l'authenticité de l'émetteur qui réalise la transaction et, que ce dernier dispose des fonds suffisant pour l'effectuer. Dans un premier temps, cette vérification permet d'avoir la garantie que l'émetteur qui réalise une transaction au destinataire, est effectivement celui qu'il prétend être (et non un tiers), tout en conservant son pseudonymat[125]. Pour cela, il est fait appel à la « *signature blockchain* » à l'aide

[121] A. Barbet-Massin, P. Lorentz, J. Brosset, « Les activités sur actifs numériques issues de la loi PACTE », RLDA, sept. 2019, p.16.
[122] Voir *infra* n°43 les limites à cette immuabilité.
[123] A. M. Antonopoulos décrit le fonctionnement du registre Bitcoin qui induit le transfert sur un compte (adresse publique ou clé publique) de la crypto-monnaie bitcoin (A. M. Antonopoulos, *Mastering Bitcoin : Unlocking Digital Cryptocurrencies*, *op.cit.*, p.22-26).
[124] R. Baron, « Introduction aux technologies blockchain supports des crypto-monnaies », *op.cit.*, p.38, n°2.
[125] Voir les développements *infra* n°299 et s. sur l'anonymat et le pseudonymat.

d'un procédé connu de cryptographie asymétrique[126]. Dans un second temps, les validateurs du réseau doivent vérifier que le montant de la transaction n'est pas supérieur au montant total détenu par l'émetteur. Cette vérification fait référence au problème mathématique de la double dépense[127].

42. La validation du bloc de transactions s'opère, quant à elle, grâce à un algorithme de consensus distribué. C'est un algorithme qui prévoit l'action par laquelle les validateurs vont approuver le bloc de transactions. Celui-ci sera de nature différente en fonction du protocole et de la typologie de *blockchain* (algorithme de la preuve de travail, de la preuve d'enjeu, de la preuve d'autorité)[128]. En théorie, cette validation pourrait être corrompue par la trahison de validateurs malveillants[129]. Ladite validation des transactions est, en effet, garantie par un algorithme de consensus tant que la majorité des participants sont honnêtes[130].

43. Cette possibilité - bien que rare en pratique - est une attaque informatique spécifique nommée « *l'attaque Goldfinger* » ou « *l'attaque des 51%* ». Dans le cas où 50% du réseau est fiable, la confiance est possible mais dès lors que 51% du réseau est malveillant, il se pourrait qu'une attaque survienne. En effet, si 51% de la puissance de calcul permettant de valider les transactions sont détenues par un validateur ou un groupe de validateur, il leur serait réalisable d'exclure ou de modifier l'ordre des transactions[131]. Avec cette attaque, la modification de l'historique du registre de la *blockchain* est envisageable engendrant la possibilité de dépenser davantage que ce l'on détient, à l'encontre du principe de la double dépense précité. C'est pourquoi, l'immuabilité des registres *blockchains* peut trouver une certaine limite[132].

---

[126] Voir les développements *infra* n°133 et s. sur la signature *blockchain*.

[127] Voir des « *corrections* » de ce théorème de la double dépense sur bitcoin proposée par des chercheurs (C. Grunspan et R. Pérez-Marco, « Double spend races », https://hal.archives-ouvertes.fr/hal-01456773/document (consulté le 31/05/2020)).

[128] Voir plus en détails, les développements n°117 et s. sur les algorithmes de consensus dans la partie préliminaire.

[129] A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder, *Bitcoin and Cryptocurrency Technologies*, *op. cit.*, p.71-72.

[130] R. Pérez Marco, « *Blockchain* : l'autre révolution venue du bitcoin », *op.cit.*

[131] Voir à ce sujet le fonctionnement technique des différentes attaques des 51% : miner des blocs dans une nouvelle chaîne de manière à dépasser l'ancienne qui sera invalidée ou encore réaliser une attaque du déni de service contre d'autres participants du réseau en invalidant leurs transactions (I. Pavel, La *blockchain* – Les défis de son implémentation, Annales des Mines, août 2017, p.22).

[132] Cambridge Centre for Alternative Finance, University of Cambridge Judge Business School, Global blockchain benchmarking study, *op.cit.*, p.17 : « *les blocs regroupant des transactions peuvent, en théorie, être inversés si un nombre suffisant de nœuds décident de s'associer. L'inversion des transactions peut être encore plus facile avec des blockchains privées que des blockchains publiques dans laquelle les mineurs ont besoin de dépenser de la puissance de calcul et/ou des crypto-monnaies pour le faire. Toutefois, les acteurs autorisés de la blockchain privée sont liés par des contrats qui visent à décourager la collusion ou d'autres comportements répréhensibles.*

44. **Domaine de la preuve dans la *blockchain*.** Ces précisions techniques étant faites, le domaine de la preuve dans la *blockchain* doit être délimité. La *blockchain* s'insère en droit de la preuve car elle constitue elle-même l'objet de plusieurs preuves que nous appellerons « *les preuves blockchains* ». Celles-ci ne sont pas un bloc monolithique mais plutôt une série de plusieurs monades, unités, qui ont chacune un sens propre, pouvant être isolée, utilisée et appuyée d'autres éléments de preuve. Prosaïquement, plusieurs éléments technologiques participent à la constitution de ces preuves, tels que la signature *blockchain*, l'empreinte *blockchain*, l'horodatage *blockchain*, le registre de transactions[133]. En droit, ces preuves *blockchains* pourront être utilisées au soutien de faits ou d'actes en fonction des situations. Alors que la *blockchain* enrichit et innerve par elle-même le droit de la preuve, cette « *machine à preuve* » - dont les termes prégnants de preuve se retrouvent dans le champ lexical technique du consensus de validation « *preuve de travail* », « *preuve d'enjeu* », « *preuve d'autorité* »[134] - , se voit confrontée aux notions juridiques de la preuve en droit.

45. **Définition de la preuve.** La notion de preuve provient du latin « *probare* » qui signifie « *pousser droit* » mettant en avant l'idée d'éprouver des faits pour dégager la vérité[135]. Étymologiquement le verbe « *prouver* » a d'abord signifié « *mettre à l'épreuve* »[136]. Cette action de prouver dénote violence et souffrance ancrées dans l'histoire de la preuve. Le recours à l'ordalie - soumettant un individu à l'épreuve pour déterminer la véracité de ses affirmations - pour apporter une preuve judiciaire dans les sociétés archaïques en est une illustration marquante. Il était jugé de la culpabilité d'un individu à sa survie et à la nature de ses convulsions à la suite de son ingurgitation d'un poison. Il pouvait aussi être jeté dans une cuve, dans la mer ou un fleuve et son aptitude à flotter déterminait sa liberté. Ou encore l'accusé était amené parfois à saisir un objet dans un récipient d'eau bouillante[137]. Au sens juridique premier, la preuve est une démonstration de l'existence d'un fait (matérialité d'un dommage) ou d'un acte (contrat, testament) dans les formes admises ou requises par la loi[138]. La preuve est définie

Si le minage dans une blockchain privée est suffisamment décentralisée entre des entités distinctes ayant des motivations différentes, nous pouvons considérer la blockchain comme inviolable ».

[133] Voir les développements *infra* n°133-135, et 139 et s.

[134] Voir les développements *infra* n°131 et s.

[135] E. Jeuland, *Droit processuel général*, LGDJ Précis Domat, dec. 2014, n°497.

[136] A. Rey, M. Tomi, T. Hordé, C. Tanet, *Dictionnaire historique de la langue française*, Le Robert, mars 2000 5 (réimpression), Voir Prouver.

[137] H. Lévy-Bruhl, *La Preuve judiciaire. Étude de sociologie juridique*, Librairie Marcel Rivière et Cie, 1964, p.63 et s.

[138] G. Cornu (dir.), *Vocabulaire juridique de l'Association Henri Capitant*, Puf, 8e éd., 2007, Voir Preuve. Voir aussi pour la preuve d'un fait : G. Baudry-Lacantinerie, *Précis de droit civil*, 1re éd., 1983, L. Larose et Forcel,

aussi, selon un second sens, comme un moyen employé pour faire la preuve, autrement dit, comme un mode de preuve[139].

46. **Conception de la preuve dans la doctrine classique et contemporaine.** Les doctrines classiques de la preuve présentent plusieurs perceptions de la définition de preuve. Bonnier définit de façon large la preuve comme « *tout moyen direct ou indirect d'arriver à la connaissance des faits* »[140]. Domat, quant à lui, introduit la notion de vérité indiquant que la preuve est « *ce qui persuade l'esprit de la vérité* » et la preuve en justice serait « *les manières réglées par la loi pour découvrir et pour établir avec certitude la vérité d'un fait contesté* »[141]. Planiol ajoute deux éléments à la définition de la preuve, soit « *le fait de produire devant le juge l'élément de conviction d'où se tire l'existence du droit* » et « *le résultat procuré par la démonstration du plaideur* ». S'agissant de la doctrine contemporaine, Jean Larguier et Henri Levy-Brulh présentent la preuve comme « *un procédé par lequel un fait ou un droit controversé et douteux acquiert (…) la valeur d'une vérité* »[142]. À travers cette définition, il y aurait deux temps dans la notion de preuve : une opération matérielle et intellectuelle. D'une part, une opération matérielle car elle renvoie aux faits, aux documents qui prouvent quelque chose et d'autre part, une opération intellectuelle puisqu'elle est un processus, une démonstration juridique à proprement parler[143].

47. **Preuve et vérité.** Preuve et vérité constituent, de tout temps, une équation avec un lien consubstantiel avéré[144], « *on appelle preuve ce qui persuade l'esprit d'une vérité* » disait Jean Domat[145]. La vérité est une notion qui fluctue en fonction de facteurs spatiaux et temporels[146]. Bien que la loi instaure une obligation générale de concourir la vérité[147], elle constitue une

t. II, p.807 et éd. successives : la preuve est la démonstration « *de l'exactitude d'un fait qui sert de fondement à un droit prétendu* ».

[139] G. Cornu, *Vocabulaire juridique*, Puf, 12e éd., 2018, p.802.

[140] E. Bonnier, *Traité théorique et pratique des preuves en droit civil et en droit criminel,* Joubert, librairie de la cour de cassation, 1843, p.3.

[141] J. Domat, *Les loix civiles dans leur ordre naturel*, Première partie, L.III, Titre VI, 1689, p.137 et 141.

[142] J. Larguier, H. Levy-Brulh cités par J. Pradel, Procédure pénale, Cujas, 14e éd. 2008-2009, n°404.

[143] Pour cette distinction d'opération matérielle et intellectuelle de la preuve voir : L. Cadiet, J. Normand et S. Amrani- Mekki, *Théorie générale du procès*, 2e éd., Puf, coll. Thémis, 2013, n ° 250, p.839 et s. ; M. Mekki, « Regards substantiel sur le « risque de la preuve ». Essai sur la notion de charge probatoire », in *La preuve : regards croisés*, ss dir. M. Mekki, L. Cadiet, C. Grimaldi, Thèmes et commentaires, Dalloz, 2015, p.7 ; M. Mekki, « Vérité et preuve. Rapport français », *in* La preuve. Journées internationales 2013 d'Amsterdam, Pays-Bas et Liège, Belgique, coll. Travaux Henri Capitant, vol. LXIII, Paris / Bruxelles, LB2V et Bruylant, 2015, p.813-814.

[144] M. Mekki, « Vérité et preuve. Rapport français », *op.cit.*, p.813.

[145] J. Domat, *Lois civiles*, 1ère partie, Livre III, Tome 6, édition Rémy, II, 1828, p.137.

[146] Y. Chartier, Avant-propos, *in* Cour de cassation, Rapport, La vérité, 2004, p.39-40.

[147] C. civ. art. 10.

représentation déformée de la réalité[148] et est de l'ordre du discours[149]. Elle a, en effet, une fonction déclaratoire et récognitive en ce qu'elle permet la reconstitution du passé[150]. La vérité est bicéphale dans la mesure où elle est découverte par le juge mais aussi construite par les parties[151]. La vérité juridictionnelle est somme toute singulière et relative, c'est une croyance subjective en une vérité[152]. Elle passe par le juge qui dit une vérité[153]. La preuve ne serait qu'un instrument de cette vérité juridictionnelle[154]. Le juge, pour construire la vérité juridictionnelle, s'appuie sur des vérités provenant de « *données probatoires* » extérieures à lui pour ensuite procéder à un raisonnement probatoire le « *construit probatoire* » aux fins de créer sa vérité[155]. Le Professeur Jean-Francois Cesaro rappelle que la vérité juridictionnelle naît dans un contexte difficile de conflit[156]. La vérité juridictionnelle n'est pas une simple controverse scientifique ou intellectuelle portant sur la validité d'une théorie et ayant pour enjeu la reconnaissance de ses pairs, mais elle émerge d'une recherche qui s'effectue lors d'un procès pouvant mettre en cause la liberté, la filiation ou encore l'honneur des justiciables[157].

48. **Vérité scientifique et vérité juridictionnelle.** La vérité scientifique - présentée comme une vérité absolue - n'est, par principe, pas égale à la vérité juridictionnelle[158]. La vérité juridictionnelle poursuit davantage la recherche du juste que la recherche du vrai, elle est la «

[148] P. Louis-Lucas, *Vérité matérielle et vérité juridique*, *in* Mélanges R. Savatier, Dalloz, 1965, p.583 et s.
[149] G. Cornu, La vérité et le droit, *in* L'art du droit en quête de sagesse, Puf, coll. Doctrine juridique, 1998, p.211 et s.
[150] G. Dalbignat-Deharo, *Vérité scientifique et vérité judiciaire en droit privé*, thèse ss. dir. L. Cadiet, Paris 1, LGDJ, Bibliothèque de l'institut André Tunc, 2002, n°24.
[151] A. Etchegoyen, *Vérité ou libertés, La justice expliqués aux adultes*, éditions Fayard, p.61 et s., cité par Y. Chartier, Avant-propos, in Cour de cassation, Rapport La vérité, 2004, p.39.
[152] M. Mekki, « Vérité et preuve. Rapport français », *op.cit.*, p.814. Notons que la vérité juridictionnelle n'est, en droit français, pas aussi exigeante que dans les pays de *common law*, pour des raisons notamment de coût et de temps, à l'image de la procédure de *discovery* (C. Grimaldi, « Les moyens légaux sont-ils suffisants ? », *in* V. Boccara, « Du droit de la preuve au droit à la preuve, question de mots ou changement de cap ? », *op.cit.*, p.5).
[153] C. Aubry, C. Rau par E. Bartin, *Cours de droit civil français selon la méthode de Zachariae*, t. 12, 1897, § 749, p.84, note 19b.
[154] Cour de cassation, Rapport annuel, La preuve, 2012, p.85.
[155] M. Mekki, « Vérité et preuve. Rapport français », *op.cit.*, p.816.
[156] Le droit de la preuve, plus généralement, a toujours été travaillé par des tensions entre preuve écrite et orale preuve scientifique et juridique, preuve rationnelle et sensible (C. Foulquier, *La preuve et la justice administrative française*, thèse ss. dir. Jean-Arnaud Mazères, Toulouse 1, 2009).
[157] Cour de cassation, Rapport annuel, La preuve, *op.cit.*, p.85.
[158] Opposition de principe de la doctrine entre vérité juridictionnelle et vérité scientifique : G. Dalbignat-Deharo, *Vérité scientifique et vérité judiciaire en droit privé*, thèse ss. dir. L. Cadiet, Paris 1, LGDJ, Bibliothèque de l'institut André Tunc, 2002, n°28 ; J.-R. Demarchi, *Les preuves scientifiques et le procès pénal*, Préf. C. Ambroise-Castérot, LGDJ, Bibliothèque des sciences criminelles, Tome 55, 2012, n°67, p.42 ; M. Mekki, « Vérité et preuve. Rapport français », *op.cit.*, p.821.

justesse de la justice »[159], contrairement à la vérité scientifique qui cherche avant tout le vrai[160]. La preuve scientifique reste au service du procès qui est à la quête fondamentale d'une solution juste, et non de la vérité absolue mais relative[161]. La preuve scientifique apporte une plus grande précision et certitude permettant de convaincre le juge d'un fait[162]. Quant à la vérité juridictionnelle, elle a pour but de participer au fonctionnement harmonieux de notre société parce qu'il s'agit intrinsèquement davantage de renouer les hommes, que de révéler des faits[163]. C'est pourquoi, cette vérité juridictionnelle attribue une place fondamentale à l'adhésion : la vérité juridictionnelle doit être pour le moins acceptable. Cette preuve de la vérité suppose une « *homologation de la collectivité* », la preuve remplit donc une fonction sociale[164]. Jean Carbonnier écrivait ainsi que « *la chose jugée n'est pas la vraie vérité* », qu'elle est surtout « *reçue par le bon peuple pour tenir lieu* »[165], ce qui renvoie finalement à l'adage latin *res judicata pro veritate habetur* signifiant que la chose jugée est tenue pour vérité. Cette recherche de la vérité est destinée à « *légitimer* » les décisions judiciaires[166]. Or, il est fréquent que la preuve scientifique soit utile au juge pour établir l'existence objective de certains faits et aider utilement à la construction d'une décision[167]. « *La preuve scientifique propose et le juge dispose* » écrivait en ce sens le Professeur Mustapha Mekki[168]. La vérité scientifique ne doit donc pas être antinomique mais un complément à la vérité juridictionnelle, sans pour autant se

---

[159] G. Cornu, Rapport de synthèse, *in* La vérité et le droit, Actes des conférences Journées canadiennes à Montréal, 1987, éditions Association Henri Capitant, Economica, 1989, p.2.

[160] P. Ricœur, *Histoire et vérité*, Seuil, 1955, p.156. Voir des exemples en matière civile : les incertitudes scientifiques ne dont pas obstacles à la certitude juridique par exemple en usant des présomptions du fait de l'homme de l'article 1353 du Code civil (Civ. 1re, 22 mai 2008, n°06-14.952) ; en matière pénale : le bénéfice du doute est une question de justice (T. Fossier et F. Lévêque, « Le presque vrai et le pas tout à fait faux : probabilités et décisions juridictionnelles », JCP 2012, n°14, n°427).

[161] « *Dès sa formation, la vérité judiciaire est, non pas absolue, mais cumulativement relative. Elle l'est car elle n'est jamais que l'expression d'un débat (...). Elle l'est aussi parce qu'elle est comparative et que, dans l'obligation où il est de statuer, le juge n'est pas en droit de suspendre sa décision jusqu'à ce qu'il accède à une certitude parfaite, réduit à se prononcer en faveur de la meilleure preuve* » (G. Cornu, Rapport de synthèse, *in* La vérité et le droit, Actes des conférences Journées canadiennes à Montréal, 1987, éditions Association Henri Capitant, Economica, 1989, p.6 et 7).

[162] R. Houin, « Le progrès de la science et le droit de la preuve », Revue internationale de droit comparé, Vol. 5 n°1, janv.-mars 1953, p.70.

[163] Cour de cassation, Rapport annuel, La preuve, *op.cit.*, p.85-86. H. Lévy-Bruhl déclare d'ailleurs : « *À chacun son métier : l'expert résout un problème technique ; le juge un problème qui, en fin de compte, est un problème humain* » (H. Lévy-Bruhl, *La preuve judiciaire. Étude de sociologie juridique*, Librairie Marcel Rivière et Cie, Paris, 1964, p.117).

[164] H. Lévy-Bruhl, *La preuve judiciaire. Étude de sociologie juridique*, *op.cit.*, p.22 et s.

[165] J. Carbonnier, *Droit civil, Introduction*, 27e éd., PUF, 2002, n°192.

[166] La vérité ne serait pas seulement qu'un « *arsenal rhétorique* » (X. Lagarde, *Réflexion critique sur le droit de la preuve*, thèse ss. dir. J. Ghestin, Paris 1, LGDJ, coll. Bibliothèque de droit privé, Tome 239, 1994, n°160, p.272).

[167] M. Mekki, « La vérité scientifique s'oppose-t-elle à la vérité juridique ? » *in* V. Boccara, « Du droit de la preuve au droit à la preuve, question de mots ou changement de cap ? », *op.cit.*, p.5. ; J. Moury, « Les limites de la quête en matière de preuve : expertise et *jurisdictio* », RTD civ., 2009 ; G. Dalbiagnat-Deharo, « Vérité scientifique et vérité judiciaire en droit privé », *op.cit.*

[168] M. Mekki, « Vérité et preuve. Rapport français », *op.cit.*, p.821.

confondre à elle[169]. Des difficultés sont, pour le reste, notables au sujet de l'association de ces deux notions de vérité, comme le relève Monsieur Guy Canivet lors de l'ouverture d'un colloque « *…le juge est contraint d'accorder foi à la science dont il ne maîtrise ni la connaissance, ni la méthode, mais il n'est pas asservi à la preuve scientifique…* »[170].

49. **Nouvelle venue : la « *vérité cryptographique* ».** L'avènement et la pratique de la technologie *blockchain* fait naître le nouveau concept de « *vérité cryptographique* ». C'est un type de vérité issue des sciences dures qui s'est formée au cœur de la grande catégorie des vérités scientifiques, particulièrement au sein de la sous-classification de la vérité informatique. Cette dernière est obtenue par le truchement de la preuve cryptographique analogue à une forme de preuve informatique, laquelle serait assimilée à la preuve scientifique pour certains auteurs[171]. La preuve fournie par une méthode scientifique s'apparente à une preuve scientifique[172], la preuve amenée par une méthode cryptographique s'apparenterait donc à une preuve cryptographique permettant l'accès à cette vérité cryptographique. Contrairement à la vérité de l'homme - qui selon Protagoras, philosophe présocratique est « *ce que l'homme appelle vérité, c'est toujours sa vérité, c'est-à-dire l'aspect sous lequel les choses lui apparaissent* », la vérité cryptographique est rigoureuse et invariable car elle est objective : il n'y a pas de doute sur cette vérité. Elle possède les propriétés de l'essence de ce qui est exact. Le flegme cryptographique de cette preuve fait naître une vérité froide qui est inaltérable[173]. Précisons que ses attributs seront, au demeurant, dépendants de son protocole et de ses procédés sous-jacents et ainsi soumis à fluctuations (voir partie préliminaire).

[169] H. Lévy-Bruhl, *La preuve judiciaire. Étude de sociologie juridique*, *op.cit.*, p.118.
[170] G. Canivet, discours d'ouverture du colloque « Le droit des preuves au défi de la modernité », le 24 mars 2000, actes de colloque, La documentation française, juin 2000.
[171] S. Migayron, « Informatique – pratique contentieuse. De l'information numérique à la preuve », Comm. com. électr. n°4, avr. 2017. Voir un avis consistant à proposer une distinction entre les preuves issues des nouvelles technologies de l'information et de la communication et les preuves scientifiques : A. Debet, « Existe-t-il encore aujourd'hui des problèmes de préservation et d'authenticité de la preuve notamment en raison des nouvelles technologies ? » *in* V. Boccara, « Du droit de la preuve au droit à la preuve, question de mots ou changement de cap ? », *op.cit.*, p.5.
[172] R. Houin, « Le progrès de la science et le droit de la preuve », *op.cit.*, p.74.
[173] Voir *supra* n°43 les tempéraments à ce postulat.

50. **Sources du droit de la preuve.** Le droit de la preuve mobilisé pour cette étude fera appel à des sources plurielles : des corpus textuels confondant droit substantiel et processuel[174], des jurisprudences et de la doctrine[175].

51. Touchant aux intérêts privés[176], le corpus légal du droit commun de la preuve en France est constitué par le droit de la preuve civile. Si les règles de droit positif en matière de preuves ont un caractère privé, ce ne fut pas de tous temps le cas. Avant la première moitié du XXe siècle la conception étatique du procès portait avec force le domaine de la preuve selon la chose publique du procès[177]. Les règles gouvernant l'administration de la justice auxquelles sont inclues les règles de preuves étaient donc d'ordre public.

52. Désormais, toutes les règles de preuve en matière civile se situent au sein du Code civil (des articles 1353 à 1386-1) et du Code de procédure civile (des articles 9 à 11 et 132 à 322). Au cœur de son livre trois « *des différentes manières dont on acquiert la propriété* », le Code civil prévoit les modes de preuve admissibles dans son titre quatre bis « *de la preuve des obligations* » aux chapitres deux « *l'admissibilité des modes de preuve* » et trois « *les différents modes de preuve* ». Ils énoncent la légalité de certaines preuves, par la détermination des modes de preuve admissibles ainsi que leurs valeurs[178]. Ce même livre contient également un certain nombre de règles éparses dans son premier chapitre « *dispositions générales* » au sujet de la charge de la preuve des obligations[179], du principe de la présomption légale[180], et des conventions de preuve[181]. S'agissant de l'emplacement de la preuve dans ce Code, les rédacteurs initiaux auraient repris - sans nécessaire cohérence - le traité des obligations de Pothier qui s'achevait par la façon dont les preuves sont constatées[182]. Certains auteurs ont émis

[174] Pour certains auteurs, la preuve se situe à la limite du droit substantiel et processuel : F. Girard, *Essai sur la preuve dans son environnement culturel*, PUAM, 2013, 2 t., n°4 s., p.26 s. ; E. Vergès, « La réforme du droit de la preuve civile : enjeux et écueils d'une occasion à ne pas manquer », D. 2014. 617 s., p.618 et 619.
[175] M. Fabre-Magnant, *Introduction au droit*, 2016, p.33-76 : « *Dans la vision classique, enseignée dans les facultés de droit, les sources du droit sont hiérarchiquement organisées : on emprunte au juriste autrichien Hans Kelsen (1881-1973) l'image qu'elles formeraient une sorte de pyramide, au sommet de laquelle on place la Constitution, puis les sources internationales, la loi et les règlements autonomes, les règlements d'application de la loi, et enfin les conventions. D'autres sources ont une place et/ou une nature un peu particulières : la jurisprudence, les usages, ou encore la doctrine* ».
[176] P. Stoffel-Munck, P. Malaurie, L. Aynès, *Droit des obligations*, 9e éd., LGDJ, coll. Droit civil, sept. 2017, n°557.
[177] C. Puigelier (dir.), *La preuve. Etudes juridiques*, Economica, 2004, 246 p.
[178] Voir *infra* n°192-203.
[179] C. civ., art. 1353.
[180] C. civ., art. 1354.
[181] C. civ., art. 1356.
[182] E. Bonnier et F. Larnaude, *Traité des preuves en droit civil et criminel*, 5e éd., 1888, p.4.

des critiques sur le positionnement des règles de la preuve dans ce bloc du droit des obligations, qui n'a pas été remis en cause à l'occasion de la réforme du droit des contrats de 2016 se contentant d'une simple mise à jour terminologique et mise en conformité des textes avec leurs interprétations par les juges de Cassation[183].

53. Le Code de procédure civile, quant à lui, aménage sous l'angle processuel, les techniques de recherche et de production de la preuve en justice. Il prévoit *en sus* du Code civil, d'autres modes de preuve (la vérification personnelle du juge et les mesures d'instruction exécutées par un technicien). Ces mesures sont regroupées dans le titre sept qui organise « *l'administration judiciaire de la preuve* ». La section quatre « *la preuve* » du premier titre sur les « *dispositions liminaires* » développe des principes directeurs supplémentaires à ceux du Code civil relatifs à la charge de la preuve[184] et l'obligation de concourir à la vérité[185]. Ces travaux tendront en toute logique à une étude approfondie de ce corpus de droit commun mais d'autres sources sectorielles de droit seront abordées comme le droit de la preuve pénale, commerciale, financière, administrative ou encore fiscale.

54. Sont également inclus dans ces travaux, l'analyse des lois de la Commission des Nations unies pour le droit commercial international (CNUDCI) (de 1985 sur l'arbitrage commercial international[186], de 1996 sur le commerce électronique[187], de 2001 sur les signatures électroniques[188], de 2005 sur l'utilisation de communications électroniques dans les contrats internationaux[189], et de 2017 sur les documents transférables électroniques[190]), la Convention Européenne des Droits de l'Homme (CESDH) du 4 novembre 1950, les règlements européens (le règlement (UE) n°910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur dit « *eIDAS* » entré en application le 1er juillet 2016, le règlement (CE) n°593/2008 du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles dit « *Rome I* », et le règlement (CE) n°864/2007 du Parlement

[183] M. Mekki, « Charge de la preuve et présomptions légales – L'art de clarifier sans innover », Droit et patrimoine sept. 2015, p.36 ; E. Vergès, « Droit de la preuve : une réforme en trompe-l'œil », JCP n°17, 17 avr. 2016, 486, p.837 : cet auteur indique que cette réforme lacunaire « *préserve l'esprit de Pothier à l'air du numérique* ».
[184] C. proc., civ., art. 9.
[185] C. proc., civ., art. 11.
[186] Loi type CNUDCI sur l'arbitrage commercial international, 1985.
[187] Loi type CNUDCI sur le commerce électronique, 1996.
[188] Loi type CNUDCI sur les signatures électroniques, 2001.
[189] Loi type CNUDCI sur l'utilisation de communications électroniques dans les contrats internationaux, 2005.
[190] Loi type CNUDCI sur les documents transférables électroniques, 2017.

européen et du Conseil du 11 juillet 2007 sur la loi applicable aux obligations non contractuelles dit « *Rome II* ») et certaines règles d'ordres juridiques externes pertinentes.

55. Bien que l'ancien débat du pouvoir normatif et créateur de droit des juges soit toujours ouvert[191], il n'est plus à démontrer le rôle significatif du juge dans l'évolution du droit de la preuve[192]. La jurisprudence nationale mais aussi internationale en matière de preuve seront ainsi étudiées, de même que celle de Strasbourg déterminante dans l'encadrement du droit des preuves, des principes et des préceptes, dans un objectif de sauvegarde des droits et libertés individuelles.

56. Peu de recherches doctrinales d'ensemble ont été menées sur le sujet du droit de la preuve, les études consacrées au droit de la preuve restant sectorielles et disparates[193]. Ceci justifie le fait qu'il existe peu d'ouvrages consacrés à la preuve en droit privé et droit public[194].

---

[191] La code civil vise qu'il est par principe « *défendu aux juges de prononcer par voie de disposition générale et réglementaire sur les causes qui leur sont soumises* » (C. civ., art.5) mais voir les positions doctrinales suivantes : H. Dupeyroux, *Les grands problèmes du Droit*, APD, 1938, p.71 ; M. Waline, « Le pouvoir normatif de la jurisprudence », *La technique et les principes du droit public. Études en l'honneur de Georges Scelle*, Paris, LGDJ, 1950, p.613 ; J. Maury, « Observation sur la jurisprudence en tant que source du droit », *in* Etude offertes au Professeur Ripert, LGDJ, Tome 1, 1950, p.28 ; G. Ripert, *Les forces créatrices du droit*, Paris, Librairie générale de droit et de jurisprudence, 1955, VII, p.386 ; S. Belaïd, « Essai sur le pouvoir créateur et normatif du juge », Revue internationale de droit comparé, 1975, p.311 ; J. Boulanger, « Notation sur le pouvoir créateur de la jurisprudence civile », RTD Civ., 1961, p.424 ; P. Coppens, *Normes et fonction de juger*, Bruylant, LGDJ, coll. La pensée juridique, 1998, p.174 ; M.-C. Ponthoreau, « Réflexions sur le pouvoir normatif du juge constitutionnel en Europe continentale sur la base des cas allemand et italien », Cahier du conseil constitutionnel n°24, Dossier : le pouvoir normatif du juge constitutionnel, juill. 2008.

[192] En matière de preuve, de nombreuses décisions ont participé à la construction et l'avancée du droit de la preuve, que ce soit du point de vue des principes du droit de la preuve (nul ne peut se constituer de preuve à lui-même : Cass.1ère civ., avril 1996 *Bekkrar c/ SNCF* (Bull. civ. n°170) ou la loyauté de la preuve : Cass. crim., 27 févr. 1996, n°95-81.366, bull.), de la reconnaissance d'un droit subjectif à la preuve (Cass. 1ère Civ., 5 avr. 2012, n°11-14.177: Bull. civ. 2012, I, n°85 ; D.2012, 1596 note G. Lardeux ; D. 2012, 2826, obs. J.-D. Bretzner ; D.2013,269, obs. N. Fricero ; D.2013 ? 457, obs. E. Dreyer ; RTD civ. 2012, 506 obs. J. Hauser), de la confirmation de validité des conventions de preuve (concernant le renversement de la charge de la preuve par convention : Cass. req. 13 déc. 1911 : DP 1912, 158. confirmé par Cass. civ, 18 janv. 1933 : DP 1933, I, 115 et Cass. 1ère civ., 30 oct. 2007, I, n°328 ; D.2008, 2820 obs. P. Delebecque ou encore la validité de la convention bancaire qui accorde une valeur probatoire au ticket de carte bleue, quand bien même il était dénué de toute signature, dès lors que le client a composé son code confidentiel : Cass. 1ère civ., 8 nov. 1989, n°86-16196, D. 1990, 369, note Gavalda ; JCP 1990 II 21576, note Virssamy ; D. 1990, Somm. 327, obs. J. Huet ; D. 1991, somm. 38, obs. Vasseur), jusqu'à la dématérialisation de la preuve (même si l'intégralité de l'acte était rédigé par l'intermédiaire d'un logiciel de traitement de texte, la reconnaissance de dette revêtant la signature manuscrite du débiteur pouvait constituer un mode de preuve parfait dès l'instant où son auteur était identifié comme débiteur de l'engagement : Cass. civ. 1ère, 13 mars 2008, n°06-17534, bull).

[193] Les seules recherches soumettant une vue générale du droit de la preuve : J. Bentham, *Traité des preuves judiciaires*, t. I, Bossange Frères, Paris 1823 ; E. Bonnier, *Traité théorique et pratique des preuves en droit civil et en droit criminel*, 2e ed. 1852 ; R. Legeais, *Les règles de preuve en droit civil, permanence et transformation*, LGDJ, 1955 ; X. Lagarde, *Réflexion critique sur le droit de la preuve*, *op.cit.* ; C. Perelman et P. Foriers (ss. dir.), *La preuve en droit*, coll. Travaux du Centre national de recherches de logique, Bruylant, 1981 ; C. Puigelier (ss. dir.), *La preuve*, Economica, 2004 ; F. Ferrand, Preuve, rép.pr. civ., Dalloz, dec. 2013.

[194] Actes de colloque « Du droit de la preuve au droit à la preuve, question de mots ou changement de cap ? » organisé par l'Association Henri Capitant, intervention de C. Grimaldi, *in* V. Boccara, « Du droit de la preuve au droit à la preuve, question de mots ou changement de cap ? », *op.cit.*, p.5.

Pour la doctrine, la preuve constitue encore une véritable inconnue en droit français, alors qu'elle est élémentaire en précontentieux et contentieux pour les praticiens[195]. Le droit de la preuve est qualifié par Alain Benabent de « *droit-rizière* » au carrefour entre théorie et pratique car il expose sa tête au soleil des grands principes et ses pieds dans la glaise du vivant quotidien[196].

II. Les intérêts de l'étude

57. **Origines historiques des preuves issues de la *blockchain*.** La *blockchain* puise ses origines dans la démonstration de deux scientifiques Stuart Haber et W. Scott Stornetta en 1991 concernant une méthode d'horodatage des données distribuées ou semi-distribuées[197]. Deux solutions étaient développées, une première méthode d'empreintes numériques horodatées de documents liées entre elles, couplée d'un système de certificat de ce lien, distribués à l'ensemble des participants avant et après la certification du document. De plus, une deuxième méthode selon laquelle plusieurs participants choisis aléatoirement devaient horodater l'empreinte était mise en avant (sans centralisation). Cette démonstration scientifique initiale a été améliorée en 1992 incorporant à cette solution des « *arbres Merkle* »[198]. Elle a, entre autres, permis de rassembler plusieurs documents en un seul bloc de documents.

58. La création effective de la première sacro-sainte *blockchain* est celle de Bitcoin en 2008, qui est le fait d'un groupe d'internautes activistes baptisés « *Cypherpunk*s »[199]. Ce nom est inspiré du courant littéraire « *Cyberpunk* » des années 1970-1980 mélangeant la science-fiction et le numérique. « *Cipher* » signifiant chiffrement, ce groupe - de mathématiciens, cryptographes, informaticiens et hackers -, par l'usage de la cryptographie, milite pour la protection de la vie privée[200]. Ce besoin de réaliser des échanges dans l'anonymat en toute

[195] M. Mekki, avant-propos *in La preuve : regards croisés*, *op. cit.*, p.1.
[196] A. Benabent, Observations finales in *La preuve : regards croisés*, *op.cit.*, p.279.
[197] S. Haber et W.S. Stornetta, « How to Time-Stamp a Digital Document », Journal of Cryptology, vol. 3, janv 1991 p.99-111. Voir aussi l'état de la recherche informatique en France à la même période sur des mécanismes d'estampillages définissant l'ordre d'évènements : C. Valot, « Accuracy of distributed timestamps », Rapport de recherche n°1804, Programme 1 Architecture parallèles, Bases de données, Réseaux et systèmes distribués, Inria, dec. 1992.
[198] Voir *supra* n°137.
[199] Ce terme de « Cypherpunk » aurait été inventé par Jude Milhon une informaticienne et écrivaine pour décrire ce groupe de mathématiciens, cryptographes, informaticiens et hackers qui avaient recours à la cryptographie. (R. U. Sirius, S. Jude, *How to Mutate and Take Over the World*, Ballantine Books, févr. 1996).
[200] Voir les premiers manifestes sur ce mouvement : T. May, « Crypto Anarchist Manifesto », 1988 ; E. Hugh, « A Cypherpunk's Manifesto », 1993 ; C. A. Kirtchev, « Cyberpunk Manifesto », 1997.

sécurité est ancien dans l'histoire de la cryptographie. Cette technique consistant à protéger un message confidentiel, authentique et intègre date de l'antiquité. Elle fut au début considérée comme un art[201], pour ensuite être consacrée au XX^{ème} siècle comme une véritable science[202], incluant désormais dans son large spectre les signatures numériques, l'authentification, les enchères, les élections électroniques, ainsi que les crypto-actifs[203]. Ces scientifiques *Cypherpunks* se sont donc attelés à développer pendant les années 1980-1990 des protocoles protecteurs des libertés individuelles, contre les ingérences de la surveillance des États et des entreprises. Pour ces derniers, les systèmes monétaires et financiers modernes informatisés rendraient l'anonymat très difficile avec des risques conséquents d'atteinte à la vie privée. Ils soutiennent une protection de la vie privée « *nécessaire pour une société ouverte dans l'ère électronique (…)* » et l'idée que « *nous ne pouvons attendre des gouvernements et des entreprises et des autres organisations majeures sans visage de nous accorder une vie privée par acte bienveillant (…)* »[204]. Ceux-ci proposent ainsi de la défendre « *avec la cryptographie, avec des systèmes de renvoi anonymes, avec des signatures digitales, et avec une monnaie électronique (…)* »[205]. Tim May est un contributeur parmi les plus connus de ces militants, grâce à la rédaction de son « *Crypto Anarchist Manifesto* » en 1988, qui lui vaut le titre de fondateur de ce mouvement[206].

59. Dans ces circonstances, certains *Cypherpunks* ont travaillé pour la création de systèmes financiers alternatifs cherchant à établir un anonymat des transactions sans le contrôle des banques et des États[207]. Depuis les années 2000, plusieurs expérimentations et initiatives de système monétaire et de paiement autonome précédant la venue de Bitcoin, ont été pensées -

[201] J. Katz, Y. Lindell, *Introduction to Modern Cryptography*, *op.cit.*, p.3 : « *Etablir de bons codes, ou casser les codes existants, reposait sur de la créativité et des compétences. Il y avait très peu de théorie sur laquelle on pouvait se fier et il n'y avait même pas une notion bien définie de ce qui constitue un bon code* ».
[202] La cryptographie concerne de la conception de mécanismes destinés à garantir les notions de sécurité, autrement dit, elle représente « *l'écriture secrète* » qui diffère de la cryptanalyse consistant à tenter d'attaquer un système cryptographique pour en étudier le niveau de sécurité, notamment. Ces deux domaines constituent la cryptologie qui est issue étymologiquement du grec « *kryptos* » (caché) et « *logos* » (science), « *cryptologie* ». Elle signifie ainsi littéralement science du secret et a pour objet de cacher les informations d'un message (Conférence de presse Médaille d'or 2006, Glossaire. La cryptologie en 10 mots clés, CNRS, 6 oct. 2006 et Conférence de presse Médaille d'or 2006, Les enjeux de la cryptologie, CNRS, 6 oct. 2006).
[203] J. Katz, Y. Lindell, *Introduction to Modern Cryptography*, *op.cit.*, p.3.
[204] E. Hugh, « A Cypherpunk's Manifesto », *op.cit.*
[205] *Ibid.*
[206] T. May, « Crypto Anarchist Manifesto », 1988, https://www.activism.net/cypherpunk/crypto-anarchy.html (consulté le 31/05/2020).
[207] Y. de Monbynes, « Anarchie, cypherpunk et libertés : les racines philosophiques de bitcoin », Contrepoints, mars 2018, https://www.contrepoints.org/2018/03/17/311911-anarchie-cypherpunk-et-liberte-les-racines-philosophiques-du-bitcoin (consulté le 31/05/2020).

telles que Digicash par David Chaum[208], Hashcash par Adam Back[209], B-money par Wei Dai[210], ou encore BitGold par Nick Szabo[211] - mais se heurtèrent à des difficultés techniques maintenant des liens de dépendance avec un intermédiaire centralisé[212].

60. C'est en 2008 dans un environnement de crise généralisée et de défiance envers les institutions bancaires et financières que la proposition du ou des fondateur(s) de Bitcoin répondant au pseudonyme de Satoshi Nakamoto, s'est imposée comme la solution viable pour un système monétaire libre et autonome gouverné par le seul consensus mathématique[213]. Cet activiste proposait une solution différente de système de paiement utilisant un registre distribué, dupliqué et public, réussissant enfin à se passer d'un organe central. Le protocole Bitcoin, réussissait finalement à résoudre le problème mathématique de la double dépense et celui jusqu'alors insoluble, connu sous le nom de « *Problème des généraux Byzantins* ». Ce dernier, identifié depuis le début des années 1980, posait la question de savoir comment des systèmes informatiques distribués pouvaient parvenir à un consensus sans dépendre d'une autorité centrale, de telle sorte que le réseau d'ordinateurs aurait pu résister à une attaque d'acteurs mal intentionnés[214]. Il convenait alors de résoudre la possibilité de s'accorder sur les actions à mener en échangeant des informations par le biais d'un réseau possiblement non fiable[215]. La solution fut trouvée par l'algorithme de la preuve de travail proposé dans le protocole Bitcoin permettant d'arriver à un consensus des acteurs[216]. Cet algorithme, innovation au cœur du protocole Bitcoin, est à présent considéré comme une incroyable découverte dans la science du calcul distribué.

61. En janvier 2009, après quelques améliorations, le protocole Bitcoin fut mis en circulation. Lors d'un test de fonctionnalité du protocole, la première transaction de dix bitcoins eu lieu entre Satoshi Nakamoto et Hal Finney, et fut intégré dans ce qui sera appelé plus tard le

---

[208] D. Chaum, « Blind signatures for untraceable payments », Advances in Cryptology Proceedings of Crypto, vol. 82, n°3, 1982, p.199-203.
[209] A. Back, « A partial hash collision based postage scheme », 1997, http://www.hashcash.org/papers/announce.txt (consulté le 31/05/2020).
[210] W. Dai, « B-Money », 1998, http://www.weidai.com/bmoney.txt (consulté le 31/05/2020).
[211] N. Szabo, « Unenumerated: Bit gold », 2005, http://unenumerated.blogspot.com/2005/12/bit-gold.html (consulté le 31/05/2020).
[212] Y. de Monbynes, « L'enfance mystérieuse du bitcoin », Contrepoints, déc. 2017. https://www.contrepoints.org/2017/12/01/304400-lenfance-mysterieuse-bitcoin (consulté le 31/05/2020).
[213] S. Nakamoto., « Bitcoin : A Peer-to-Peer Electronic Cash System », nov. 2008, https://bitcoin.org/bitcoin.pdf (consulté le 31/05/2020).
[214] L. Lamport, R. Shostak, M. Pease, « The Byzantine Generals Problem », 4 ACM Transactions on Programming Languages and Systems at 382, vol. 4, issue 3, juill. 1982.
[215] A. M. Antonopoulos, *Mastering Bitcoin : Unlocking Digital Cryptocurrencies*, *op.cit.*, p.4.
[216] Voir *supra* n°129 en partie préliminaire.

bloc « *genesis* »[217]. Le projet progressa peu jusqu'à juin 2009 où furent comptabilisés quelques centaines de téléchargements du programme bitcoin uniquement. À cette période, la majeure partie des bitcoins étaient émis par les ordinateurs de Satoshi Nakamoto, seuls quelques mineurs existaient sur le réseau, et peu de participants s'échangeaient cette crypto-monnaie. Le bitcoin n'avait d'ailleurs aucun cours et n'était pas encore fonctionnel dans son usage de paiement puisque non admis par les opérateurs classiques. Une première personne aurait accepté l'échange de deux pizzas contre 10 000 bitcoins, réalisant ainsi le premier achat en bitcoin, et constituant, par la même, les pizzas les plus chères de l'histoire (en comparant au cours actuel)[218]. Très rapidement, la première plateforme d'échange de crypto-monnaies « *Mt. Gox* » fut créée par Jed McCaleb pour faciliter la vente et l'achat de bitcoins. Dès cet instant, l'arrivée de nouveaux mineurs rendit croissantes les difficultés de minage des personnes physiques seules et la création de bitcoins. Pour des risques liés à la croissance de la plateforme et aux contraintes réglementaires associées, cette société fut ensuite revendue à Mark Karpeles, informaticien français installé au Japon. Mt. Gox fit faillite en février 2014 après le détournement de centaines de milliers de bitcoins (soit 450 millions de dollars à cette époque), ce qui amorçait l'une des premières controverses entachant la réputation des crypto-monnaies[219]. L'essor et la fermeture du site « *Silk Road* » une plateforme du Dark net où les bitcoins étaient utilisés comme moyen de paiement en échange de biens et de services issus d'activités illicites exacerbèrent l'embrasement de ces polémiques[220].

62. **Intérêts de la *blockchain* dans l'économie politique : la promesse politique d'une société sans banques.** Le protocole Bitcoin trouve ses origines au sein de l'école autrichienne du courant économique libertarien selon laquelle la monnaie fiduciaire et les différentes interventions des États ne seraient pas nécessaires[221]. Les manipulations monétaires par les différentes interventions d'États, auraient tendance à provoquer des cycles économiques exacerbés et une conséquente inflation[222]. Pour cette école, il conviendrait de supprimer le système bancaire à réserves fractionnaires et revenir à l'étalon-or afin d'éviter un déséquilibre généralisé et une récession des entreprises[223]. Cette vision antiétatique ou à intervention

[217] /pages/Bloc-Genesis (consulté le 31/05/2020).
[218] http://bitcoin.fr/histoire/ (consulté le 31/05/2020).
[219] *Ibid.*
[220] Y. de Monbynes, « L'enfance mystérieuse du bitcoin », *op.cit.*
[221] Voir notamment les auteurs : F. A. Hayek, L. von Mises, et E. von Bohm-Bawerk.
[222] BCE, Virtual currency schemes, oct. 2012, p.22.
[223] S. Caré, *Les libertariens aux États Unis : sociologie d'un mouvement asocial*, Pur, coll. Res publica, 2010, p.10.

minimale de l'État des libertariens cherche à dénouer le lien qui unit l'État aux citoyens[224]. Elle a pour objectif un dépérissement du politique comme fin mais aussi comme moyen, contrairement à l'idéologie marxiste[225]. Autrement dit, elle désapprouve tous les moyens employés qui impliqueraient une coercition.

63. L'idéologie libertarienne prend essor par la constitution d'un véritable mouvement dans les années 1970 au sein duquel des courants de pensée disparates sont recensés[226]. Ces libertariens embrassent, plus largement, la grande famille politique des anarchistes, lesquels se divisent en deux courants : les libertaires et les libertariens (plus populaires en Amérique du nord)[227]. Le représentant des auteurs anarchistes cherchant des concepts concurrents à l'autorité de l'État dans l'émission de la monnaie est Proudhon. Souvent qualifié de « *père* » aux prémices du développement des crypto-monnaies, il critique en particulier la dette et l'usure se rapprochant de la création du bitcoin, une crypto-monnaie sans dette[228]. En 1849, il établit la « *Banque du Peuple* » dans une intention de suppression progressive du taux d'intérêt du crédit, de démonétisation de l'or et de l'argent, remplacé par un « *bon d'échange* » sans condition de remboursement en espèces et de généralisation de la lettre de change payable contre des marchandises ou des services[229]. C'est cette idée de création du bon d'échange en tant que monnaie de la Banque du Peuple, autrement dit, d'une émission de monnaie par les individus, qui place les crypto-monnaies dans le sillon des idées proudhoniennes[230]. Ses idées antiétatiques

[224] Pour Robert Nozick, il convient que l'État se limite à ses fonctions étroites de protection comme un « *veilleur de nuit* » (R. Nozick, *Anarchie, État et Utopie*, Puf, trad. française E. d'Auzac de Lamartine et P.-E. Dauzat (1e éd. 1974), 2016).

[225] Cependant, pour le philosophe Mark Alizart, les crypto-monnaies pensées par un groupe limité de libertariens font désormais l'objet d'une appropriation collective rendant possible l'idéologie communiste. Il nomme cette forme nouvelle de communisme : le « *cryptocommunisme* » en référence aux marxistes cachés (M. Alizart, *Cryptocommunisme*, perspectives critiques, Puf, fevr. 2019, p.13).

[226] S. Caré, *Les libertariens aux États Unis : sociologie d'un mouvement asocial*, *op.cit.*, p.10.

[227] Le terme « *anarchie* » est un dérivé du grec « *anarkhia* » qui étymologiquement renvoie à l'absence d'autorité de commandement (C. Bertrand (dir.), R. Brett, F. Pulliero, N. Wagener, « Droit et anarchie », (actes de colloque du « Droit et anarchie », Université Paris-Sud, le 23 nov. 2012), Éditions L'Harmattan, coll. « Presses universitaires de Sceaux », 2013, p.103-118).

[228] P.-J. Proudhon, *Manifeste électoral du peuple*, *in* œuvres complètes de P.-J Proudhon, Tome XVII, Mélanges, Articles de journaux 1849-1852, Premier volume, Librairie internationale, 1848 : « *la Productivité du capital, ce que le Christianisme a condamné sous le nom d'usure, telle est la vraie cause de la misère, le vrai principe du prolétariat, l'éternel obstacle à l'établissement de la République* ».

[229] France Culture, Pierre-Joseph Proudhon (1809-1865), L'anarchie, c'est l'ordre, 28 nov. 2017, https://www.franceculture.fr/emissions/une-vie-une-oeuvre/pierre-joseph-proudhon-1809-1865-lanarchie-cest-lordre (consulté le 31/05/2020).

[230] La scission entre les idées de Proudhon et des libertariens crypto-anarchistes se trouve dans la conception de la propriété. La célèbre citation « la propriété, c'est le vol » distinguant propriété qui n'est à personne et possession qui est à tous (P.-J. Proudhon, *Qu'est-ce que la propriété ? ou recherche sur le principe du droit et du gouvernement*, Garnier Frères Libraires, 1849, p.29-67), alors que pour les libertariens la propriété est un concept sacré. Voir aussi : E. Castelon, « Le banquier, l'anarchiste et le bitcoin », Le Monde diplomatique, mars 2016, https://www.monde-diplomatique.fr/2016/03/CASTLETON/54957 (consulté le 31/05/2020).

trouvent cependant une divergence avec celles des crypto-anarchistes : il s'agit par cette crypto-monnaie non plus d'abolir l'État mais de se protéger de celui-ci par le chiffrement.

64. L'absence de droit, l'anomie est un concept anarchiste qui fait d'ailleurs écho aux idéaux de la *blockchain*. Max Stirner dans « *L'Unique et sa propriété* » explicite que le droit n'existe pas car seul l'individu a le droit, et si lui seul a le droit alors il n'existe pas[231]. La vision d'une technologie auto-régulatrice avec la *blockchain* qui s'opposerait aux mécanismes de règlementation par le droit selon la très célèbre formule « *Code is law* » de Laurence Lessig est prégnante chez les promoteurs de cette technologie[232]. Ceux-ci faisant souvent référence à la déclaration d'indépendance du cyberespace de John Perry Barlow dans laquelle il indiquait que « *vos concepts légaux de propriété, d'expression, d'identité, de mouvement, de contexte, ne s'appliquent pas à nous. Ils sont basés sur la matière, et il n'y a pas ici de matière* »[233]. Le message est clair pour cet auteur, le droit n'a pas sa place au sein de la communauté des anarchistes technophiles. Parallèlement à cette doctrine radicale du code est la loi, la notion plus tempérée de « *lex cryptographia* » est développée par les universitaires Primavera de Filippi et Aaron Wright. Ces auteurs soutiennent que le déploiement de cette technologie à grande échelle mènera au développement d'un nouveau sous-ensemble de lois baptisées « *lex cryptographia* », des règles administrées par des contrats intelligents auto-exécutés et des organisations (autonomes) décentralisées[234]. Par l'architecture même de la *blockchain*, les individus pourraient construire leurs propres règles technologiques, un « *cadre réglementaire privé* » en somme[235]. Plus encore, pour le Professeur de droit Mustapha Mekki, un nouveau courant doctrinal juridique émergerait avec la *blockchain* après le « *réalisme juridique* » et le « *naturalisme juridique* » : celui du « *numérisme juridique* »[236].

[231] M. Stirner, *L'Unique et sa propriété*, coll. Etudes, 2013, 416 p.
[232] L. Lessig, « Code Is Law. On Liberty in Cyberspace », Harvard Magazine, janv. 2000. Cependant, cet article est extrait d'un ouvrage développant le précepte selon lequel, sur internet, la liberté et le respect des droits sont dépendants de la manière dont le code est conçu (L. Lessig, Code Version 2.0, Basic Books, USA, 1e éd. 1999, 2006).
[233] J.-P. Barlow, « Déclaration d'Indépendance du Cyberespace », 8 févr. 1996, http://editions-hache.com/essais/barlow/barlow2.html (consulté le 31/05/2020).
[234] A. Wright, P.de Filippi, « Decentralized Blockchain Technology and the Rise of Lex Cryptographia », *op.cit.* La notion de « *lex cryptographia* » émerge dans la continuité de celles de « *lex mercatoria* » et « *lex informatica* » conçue comme un ensemble de règles (ou standards) et de normes techniques coutumières élaborées par les utilisateurs issus des usages au sein d'une communauté de commerçants et d'internautes respectivement.
[235] P.de Filippi, A. Wright, *Blockchain and the Law*, Harvard University Press, 2018, p.5.
[236] M. Mekki, « Blockchain, smart contracts et notariat : servir ou asservir ? », JCP N n°27, 6 juill. 2018, act.599, p.8.

65. La raison pour laquelle le mouvement libertarien a tant séduit les milieux futuristes et technophiles appelés dès lors « *crypto-anarchistes* », tire son origine dans l'idée que les prises de décision s'opèrent à l'encontre de la ploutocratie par l'interaction des citoyens et non « *d'en haut* ». C'est la notion d' « *ordre spontané* », popularisée par l'économiste prix Nobel Friedrich Hayek, qui trouverait à s'appliquer à l'économie[237]. Des économistes autrichiens contemporains ont malgré tout émis des critiques au sujet de la crypto-monnaie bitcoin, considérée comme d'ordinaires octets stockés dans un ordinateur. Elle n'aurait, selon eux, aucune valeur intrinsèque, à l'instar de l'or. En outre, le protocole ne réussirait pas à satisfaire le « *théorème de régression de Mises* », explicitant qu'une monnaie a nécessairement une valeur d'usage avant d'avoir une valeur d'échange. L'argent est accepté parce qu'il tient ses racines d'une marchandise exprimant un certain pouvoir d'achat de l'individu, et non en raison de normes ou d'une convention sociale[238].

66. **Idéal libertarien crypto-anarchiste rattrapé par les réalités financières : une nouvelle désillusion ?** C'est à la suite d'une crise de confiance globale des sociétés modernes - entrechoquées avec ses institutions - que ce solutionnisme technologique *blockchain* fut envisagé comme une quatrième révolution industrielle[239]. Le « *lubrifiant* » des échanges qu'est la confiance[240], se situerait dorénavant avec la *blockchain* en son point névralgique : la cryptographie. Mais cette technologie semble à certains égards dévoyée de son usage initial d'échange de valeurs sans banques par des monnaies virtuelles de protestation[241], devenues des

[237] F. Hayek, *Droit, législation et liberté*, Puf, Trad. française, 1979, 960 p.

[238] J. Matonis, « Why Are Libertarians Against Bitcoin ? », The Monetary Future, 16 juin 2011, https://themonetaryfuture.blogspot.com/search?q=Why+Are+Libertarians+Against+Bitcoin (consulté le 31/05/2020).

[239] Y. Algan, C. Cahuc, « La société de défiance : comment le modèle social français s'autodétruit », ENS, 2007 ; A. Manas, Y. Bosc-Haddad, « La (ou les) *blockchain* (s), une réponse technologique à la crise de confiance », Annales des mines – réalités industrielles 2017/03, août 2017, p.102. Voir aussi : la notion dégagée par Jérémy Rifkin de troisième révolution industrielle et sa conception horizontale de la société (J. Rifkin, *La troisième révolution industrielle – Comment le pouvoir latéral va transformer l'énergie, l'économie et le monde*, Les liens qui libèrent, 2011, 415 p.).

[240] La confiance est définie par kenneth arrow prix nobel d'économie, comme un « *lubrifiant social* », un bien public facilitateur des relations économiques (K. Arrows, *the limits of organizations*, Harvard University Press, 1974. Trad. Française : K. Arrows, *les limites de l'organisation*, Puf, paris, 1976). Voir sur le sujet de la redéfinition de la confiance depuis la *blockchain* et la difficile définition de la confiance : K. Werbach, *The blockchain and the new architecture of trust*, MIT Press, Information Policy, nov. 2018, 305 p.

[241] Pour Nicolas Colin, « *Les créateurs de protocoles ont compris cette dynamique. Ils ont imaginé les crypto-monnaies non pour spéculer, mais pour orchestrer l'émergence et le déploiement d'une nouvelle génération de protocoles réseau et ainsi combler les lacunes du Code de la Route sur internet* ». Il conviendrait donc de regarder les crypto-monnaies comme « *une tentative de relancer l'innovation dans le domaine des protocoles réseau, aujourd'hui délaissés par les géants d'internet* » puisque « *la principale fonctionnalité d'une crypto-monnaie, c'est en effet d'intéresser les premiers utilisateurs d'un nouveau protocole à son déploiement à plus grande échelle. Plus nombreux sont les individus qui achètent les crypto-monnaies (comme le bitcoin) liées à un protocole, plus ils contribuent à augmenter son échelle d'opération ; et plus ce protocole est utilisé, plus la valeur des crypto-monnaies augmente* » (N. Colin, « Crypto-monnaies, un peu de cohérence », L'Obs, 25 janv. 2018

devises de spéculation[242]. À peine cette nouvelle infrastructure protocolaire « *holacratique* » voyait le jour, qu'elle constituait progressivement de nouveaux modèles d'affaires et des opportunités de marché[243]. Ré-intermédiation des acteurs du marché financier, créations de crypto-monnaies par les banques privées[244], les banques centrales ou autrement appelée « *Monnaie digitale de Banque centrale* » (MDBC)[245], pratique du *trading* de crypto-monnaies, indexations de crypto-actifs à des sous-jacents en devises (crypto-actifs nommés « *stablecoins* »)[246], sont autant de pratiques qui ne semblent pas en adéquation avec l'engagement politique initial projeté par les libertariens[247]. Ces risques avaient déjà été anticipés par certains auteurs alarmant sur les dérives existantes au sein des espaces décentralisés, à l'instar des GAFA avec Internet[248].

https://www.nouvelobs.com/chroniques/20180126.OBS1279/crypto-monnaies-un-peu-de-coherence.html (consulté le 31/05/2020)).

[242] En décembre 2017, les offres étant nettement supérieures aux demandes, le cours du bitcoin s'est envolé avoisinant le montant de 20 000 dollars.

[243] K. Löber, « Central bank considerations around digital currencies », Dossier « Monnaies », RDBF n°4, juill. 2019, p.40, n°2 : « *From these anarchic origins, the focus shifted quickly from the payment aspect to the underlying technology, and considerations on whether DLT could bring enhancements in terms of safety or efficiency compared to traditional methods to record and transfer value between economic actors, such as by deploying DLT in the financial market infrastructure as a substitute to existing payments or settlement systems. The initial hype has given way to more informed assessments on potential benefits or risks, including attempts to identify business cases for the use of DLT and in particular the ability to create tokens, i.e. digital representations of value or assets, based on new technology. As part of this exercise, the focus has again shifted back to the original proposition of Bitcoin, i.e. the payment function and whether there might be a case for a digital representation of money* » ; P.- J. Benghozi, « Blockchain : objet à réguler ou outil pour réguler ? », JCP E n°36, 7 sept. 2017.

[244] Communiqué de presse, « Credit suisse announces participation in utility settlement coin initiative », août 2017, https://www.credit-suisse.com/about-us-news/en/articles/media-releases/credit-suisse-announces-participation-in-utility-settlement-coin-initiative-201708.html (consulté le 31/05/2020) ; Actualité, « J.P. Morgan creates digital coin for payments », fevr. 2019, https://www.jpmorgan.com/global/news/digital-coin-payments (consulté le 31/05/2020)

[245] Committee on Payments and Market *infra*structures, Markets Committee, Central bank digital currencies, mars 2018 ; European Central Bank, exploring anonymity in central bank digital currencies, in Focus, Issues n°4, dec. 2019 ; Banque de France, La monnaie digitiale de banque central, janv. 2020 ; Banque de France, Note d'information – monnaie digitale de banque centrale, Experimentations de la Banque de France sur la monnaie digitale de banque centrale : appel à candidature, mars 2020.

[246] J. M. Griffin, A. Shams, « Is Bitcoin Really Un-Tethered ? », Librairie SSRN, juin 2018, 66 p., https://ssrn.com/abstract=3195066 (consulté le 31/05/2020) : « *First, if the Tether (stablecoin) founders, like most early cryptocurrency adopters and exchanges, have large holdings of Bitcoin, they generally profit from the inflation of the cryptocurrency prices. Second, the coordinated supply of Tether (stablecoin) creates an opportunity to manipulate cryptocurrencies* ». Voir les avis et mises en garde du G7 et du G20 : G7 Working Groupe on Stablecoins, Investigating the impact of global stablecoins, oct. 2019 ; FSB, Regulatory issues of stablecoins, oct. 2019.

[247] Arvind Narayanan décrit la distinction entre le « *crypto-cypherpunk* » ou « *le rêve d'utiliser la cryptographie comme une arme pour le social et le politique le changement* », et le « *crypto-pragmatique* » qui, quant à lui, a « *une vision plus terre-à-terre qui cherche à concevoir que modestement l'amélioration de la protection de la vie privée dans des applications spécifiques* » (A. Narayanan, « What happened to the crypto dream ? », Part 2, IEEE Security & Privacy, Vol. 11, Issue 3, mai-juin 2013, p.68-71).

[248] P. de Filippi, « What *Blockchain* Means for the Sharing Economy », *op. cit.* (consulté le 31/05/2020).

67. **Intérêts des preuves *blockchains* dans la philosophie.** De longue date, l'envergure de la notion de preuve fut comprise et intégrée dans les raisonnements d'illustres philosophes. « *Ce qui caractérise le philosophe et le distingue du vulgaire, c'est qu'il n'admet rien sans preuve, qu'il n'acquiesce point à des notions trompeuses et qu'il pose exactement les limites du certain, du probable et du douteux* », ainsi s'exprimait Diderot au sujet de l'importance de la preuve dans le raisonnement du philosophe [249]. Tandis qu'elle représenterait seulement « *un fait purement intellectuel, ou un ensemble de faits purement intellectuels, qui est la condition suffisante d'un autre fait intellectuel* »[250], sous la plume de Goblot. Selon Mark Alizat, philosophe contemporain étudiant la preuve cryptographique, cette preuve dans le protocole Bitcoin crée une « *flèche du temps* » rendant irréversible l'écriture et la lecture du registre de transactions[251]. Cette notion de temps n'a pas été interprétée de façon identique au fil des époques. Alors que sous l'antiquité, le temps est relayé à une place de second plan pour Platon qui lui concède, tout au plus, une représentation inférieure de l'éternité, au XVIIIe siècle[252], Kant accorde, lui, de l'importance au rôle du temps, par lequel il y voit une forme universelle permettant de saisir les phénomènes[253]. Conformément à l'avis de Bergson, le temps doit être considéré, soit de manière subjective par la conscience, soit de façon objective par la technique. Selon l'approche de la conscience, le temps est lié à nos représentations (pensées, sentiments, etc.), alors que l'approche technique le considère en référence à l'horloge qui agit comme une mesure commune, universelle[254]. C'est cette deuxième conception objective qui retentit dans la perception de la technologie *blockchain* fournissant cette mesure commune du temps.

68. **Preuves *blockchains* et leurs intérêts mathématiques.** Le combiné de preuves issues de la *blockchain* se fonde sur des primitives cryptographiques, précisément des primitives de cryptographie mathématique. Il relève donc avant tout du progrès du domaine des mathématiques fondamentales de la science informatique[255]. Ces preuves cryptographiques fondées sur les mathématiques sont considérées comme des preuves « *froides* ». Elles sont utilisées pour signer les transactions, les ordonner, les organiser et contrôler la création de blocs

[249] D. Diderot, *Lettre à Sophie Volland*, 26 sept. 1762.
[250] E. Goblot, *Traité de logique*, Librairie Armand Colin, 1918, p.21.
[251] M. Alizart, *Cryptocommunisme, perspectives critiques*, op. cit., p.73.
[252] M. Blay, *Dictionnaire des concepts philosophiques*, Larousse, 2013, p.780.
[253] E. Kant, *Critique de la raison pure*, Trad. française par A. Tremesaygues et B. Pacaud 1905.
[254] E. Bergson, *Essai sur les données immédiates de la conscience*, thèse, Félix Alcan, coll. Bibliothèque de philosophie contemporaine, 1889.
[255] J.-P.Delahaye, Du bitcoin à la *blockchain* n°1, Mooc sur l'Informatique et la Création Numérique, Inria Learning Lab, mai 2017, https://www.lemonde.fr/blog/binaire/tag/bitcoin/ (consulté le 31/05/2020).

de transactions, pour enfin rendre ces transactions infalsifiables[256]. Une des conséquences du développement des protocoles *blockchains* est la « *création d'une chronologie interne propre au réseau* » par l'enregistrement des transactions sur une « *base de données* » sécurisée cryptographiquement et mise à jour par le protocole de consensus grâce à la validation de nouveaux blocs de transactions[257]. Chaque nouveau bloc validé fournit un « *tic-tac* » de l'horloge interne de la *blockchain* selon le mathématicien chercheur au CNRS Ricardo Perez Marco. Cette horloge constituerait donc une horloge universelle inviolable[258].

69. ***Blockchain* et intérêts probatoires pratiques.** De la preuve matérielle à la preuve immatérielle, les nouvelles technologies portent en germe un renouvellement rationalisé du droit de la preuve, la *blockchain* en est la continuité. Dans l'ancien droit, l'écrit avait moins de valeur que le témoignage, les témoins « *passaient lettres* »[259]. Cette preuve par témoins supposait cependant d'importants efforts pour déceler le mensonge[260], les imprécisions, et encore stimuler la mémoire des témoins[261]. En 1566, Charles IX décida à l'article 54 de l'ordonnance de Moulins d'imposer la supériorité de l'écrit, renversant alors la règle : désormais les lettres « *passaient témoins* »[262]. L'objectif poursuivi était de lui attribuer la valeur de vérité préférable et non d'affirmer une vérité absolue de l'écrit[263]. Avec l'évolution des procédés modernes de reproduction, tels que les microfilms, photocopies, micro-fiches, vidéo-disques et le développement des chèques, une nouvelle réforme de la preuve inspirée par les banques fut adoptée[264]. Si la jurisprudence interprétait ensuite de manière large la notion

[256] Conférence « Les mardis de l'espace des sciences », organisée avec l'Université de Rennes 2- CREA, intervention de J.-P.Delayahe « Les mathématiques et la cryptographie réinventent la monnaie : le bitcoin », 14 oct. 2014.
[257] R. Perez Marco, « Blockchain time and Heisenberg Uncertainty Principle », 2016.
[258] Etant précisé que selon ce mathématicien plus le temps avance, plus la probabilité de modifier la chronologie de la chaîne de blocs diminue de façon exponentielle avec le nombre de validations.
[259] J.-P.Lévy, A. Castaldo, *Histoire du droit civil*, Dalloz 2002, n°581 et s.
[260] Œuvres de Pothier : annotées et mises en corrélation avec le Code civil et la législation actuelle par M. Bugnet, tome 2, Cosse et Marchal, 2e éd., 1861, p.423 : « *La corruption des mœurs et les exemples fréquents de subornation de témoins, nous ont rendu beaucoup plus difficiles à admettre la preuve testimoniale que ne l'étaient les Romains* ».
[261] Jaubert déclare dans son rapport destiné au Tribunat : « *Des hommes d'une égale bonne foi ne racontent-ils pas souvent d'une manière différente ce qu'ils ont vu, ce qu'ils ont entendu ? (...) Si nous n'avions que la tradition orale, que deviendraient la plupart de nos conventions lorsque les années en auraient altéré les traces ? Que d'erreurs, que d'incertitudes, que de procès, enfin que de sujets de triomphes pour l'injustice !* », cité par M. le Baron Locré, in *La Législation civile, commerciale et criminelle de la France*, tome 7, Treuttel, 1828, p.526.
[262] P. Malaurie, L. Aynes, P. Stoffel-Munck, *Les obligations*, 4e éd., Defrénois, Lextenso éditions, coll. Droit civil, 2009, n°559.
[263] Art. 54, ordonnance de Moulins 1566 : car il permet « *d'obvier à la multiplication de faits que l'on a vu ci-devant estre mis en avant en jugement, sujets à preuves de témoins et reproches d'iceux dont adviennent plusieurs inconvénients et involutions de procès* ».
[264] Loi n°80-525 du 12 juillet 1980.

d'écrit[265], l'écrit électronique n'a été reconnu comme un mode de preuve équivalent à celui de l'écrit sur support papier qu'à partir de la loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique. Cette loi a reconnu l'écrit électronique, admettant une force probante identique - sous certaines conditions - à l'écrit sur support papier[266]. L'état technologique fut ainsi évoluer les textes et inspirait le législateur pour actualiser et moderniser les modes de preuve érigeant progressivement la preuve immatérielle comme nouvelle reine des preuves[267].

70. De tout temps, il a toujours été fondamental de savoir qui était l'auteur d'une preuve ou d'une « *trace* » laissée dans le temps et si celle-ci était la restitution exacte du contenu de l'acte à la date à laquelle il fut établi[268]. « *Idem est non esse et non probari* » a-t-on pu écrire[269], signifiant qu'il en est de même de ne pas être ou ne pas être prouvé. Adage soutenu par la doctrine, Raymond Legeais indiquait que « *la preuve se réalise grâce à des preuves* »[270]. Cet adage ancien, trouve toujours une résonance contemporaine puisqu'en pratique, si un droit est contesté et que son titulaire ne parvient pas à le prouver, tout se passera comme si ce droit n'existait pas[271]. En cas de perspective d'une action en justice, avec les espoirs ou inquiétudes qui s'y attachent, la preuve constitue l'enjeu fondamental des rapports juridiques au sein de tous les secteurs de notre société. Qui plus est, lors de contentieux, la preuve et sa charge sont effectivement des clés essentielles dépendantes de la réussite du litige. La preuve sera vaine si elle n'est pertinente[272]. Mais en dehors des prétoires, la preuve n'implique pas nécessairement un contentieux, il est des situations selon lesquelles la preuve doit nécessairement être apportée

---

[265] Concernant l'usage du crayon dans l'écrit notamment : CA Aix-en-Provence, 27 janvier 1846 : « *(…) mot écrire signifie tracer des lettres, des caractères ; que la loi n'a spécifié ni l'instrument ni la matière avec lesquels les caractères seraient tracés* » ; Com. 8 oct. 1996 n°94-17967, Publié au bulletin : « *(…) aucun principe ni aucun texte ne prohibe l'usage du crayon dans la rédaction d'un acte sous seing privé (…)* ».

[266] C. civ, ancien art. 1366. Voir : P. Catala, « Le formalisme et les nouvelles technologies », Defrénois 2000 ; A. Raynouard, « Adaptation du droit de la preuve aux technologies de l'informatique et à la signature électronique », Defrénois, mai 2000 ; P. Y. Gautier et X. Linant de Bellefonds, « De l'écriture électronique et des signatures qui s'y attachent », JCP G, 2000.

[267] Voir les interrogations soulevées par les rôles probatoires du phonographe (J. Valéry, « Examen des applications que le phonographe peut recevoir dans la correspondance commerciale et de leurs conséquences juridiques », Ann. De droit commercial 1890, doctr., p.95) ou encore du magnétophone (P. Mimin, « La preuve par magnétophone », JCP G, 1957, I, 1370).

[268] E. A . Caprioli, A. Cantero, « Traçabilité et droit de la preuve électronique », Droit et patrimoine n°93, 1er mai 2001.

[269] H. Roland, L. Boyer, *Adages du droit français*, Litec, 4e éd., 1999, n°161, p.312 : proclamant que « *la preuve double droit, comme l'ombre suit le corps* ».

[270] R. Legeais, *Les règles de preuve en droit civil. Permanences et transformations*, thèse ss. dir . R. Savatier, Poitier, LGDJ, p.144.

[271] « *Un fait peut être parfaitement vrai ; s'il n'est pas prouvé, il ne sera pas source de droit* » rappelait Laurence Pecaut-Rivolier magistrate auprès de la Cour de Cassation.

[272] Selon l'adage latin « *frustra probatur quod non relevat* ».

(date de naissance, domicile, et autres)[273]. De façon plus générale, il est en effet usuel que celui qui revendique un droit - même si ce n'est pas devant un tribunal - étaye ses prétentions car rares seront ceux qui prêteront foi à un droit ou un fait non établi[274].

71. À l'échelle du numérique, le contenu étant réplicable indéfiniment, il est devenu cardinal de connaître techniquement la possibilité de restituer juridiquement une preuve par souci stratégique défensif et/ou en cas de contentieux[275]. C'est dans ce contexte, que la *blockchain* apparaît comme, d'une part, la future clé moderne au verrou du procès et, d'autre part, profitable dans une stratégie probatoire d'acteurs publics et privés.

72. Cette preuve distribuée sans limite géographique constitue une véritable promesse de preuve universelle admissible devant tous les tribunaux par-delà les frontières. Elle permettrait de pallier certaines limites des preuves numériques existantes, comme l'enveloppe e-soleau qui n'est pas reconnue comme preuve lors d'une action en contrefaçon devant les tribunaux étrangers. La fiabilité de la conservation de ces preuves répliquées sur un grand nombre de nœuds en fait un atout majeur. Dans le même temps que cette admission standardisée par les tribunaux profitable aux plaideurs, le registre des transactions est accessible en tout lieu aux tribunaux. C'est un avantage notable dans un contexte où l'accès transfrontalier aux preuves reste encore difficile[276].

73. Depuis notre ouverture à cette société numérique, la sécurisation des échanges et le rassemblement de preuves numériques font partie des principaux objectifs stratégiques des acteurs publics et privés afin de se prémunir d'un certain nombre de risques économiques et industriels[277]. La *blockchain* fournit, à ce titre, des preuves bien plus fines et systématiques que certaines preuves classiques[278]. Ce sont des risques tant traditionnels, que nouveaux, auxquels s'exposent ces acteurs. Alors que les risques traditionnels tels que la contrefaçon, la

[273] E. Vergès, G. Vial, O. Leclerc, *Droit de la preuve*, Puf, coll. Thémis, 2015, n°6, p.8.
[274] A. Aynès, X. Vuitton, *Droit de la preuve. Principes et mise en œuvre processuelles*, Droit & Professionnels, Lexis Nexis, 2018, p.1.
[275] J. Huet, « Preuve et sécurité juridique en cause dans l'immatériel », Arch. phil. droit n°43, 1999, p.164.
[276] Voir *infra* n°608 et s.
[277] Voir cette même question de sécurisation technique des échanges soulevée concernant l'acte authentique électronique en 2001 : Travaux du groupe de réflexion sur les actes authentiques électroniques formés par le GIP Droit et Justice, J.-F. Blanchette, « La technologie de l'écrit électronique : synthèse et évaluation critique », janv. 2001.
[278] E. Jeuland, *Droit processuel général*, *op.cit.*, n°497 ; E. Netter, « Blockchain et professions réglementées », Cahiers de droit de l'entreprise n°3, Dossier 21, mai 2018, p.1 : « *c'est alors un vaste renouvellement des technique probatoire qui se dessine* ».

concurrence déloyale, le patent troll, l'espionnage industriel d'anciens employés ou encore de partenaires, les placent en situation de danger, de nouveaux risques technologiques issus des hackers ou de cyberattaques diverses, deviennent exponentiels. La protection des innovations, telles que les savoir-faire ou les secrets d'affaires, est ainsi au cœur des stratégies d'entreprises. Ce sont malgré tout grâce à des preuves « *faibles* » conservées, des documents de la vie des affaires (factures, bons de commande, plaquettes commerciales, e-mails) que l'on continue à prouver des droits de grandes valeurs. Ces preuves sont souvent réunies - qui plus est, lorsque cela est envisageable -, en urgence, peu de temps avant un contentieux, alors qu'elles constituent « *une exigence au cœur du procès* »[279].

74. **Prémices du droit de la *blockchain* et enjeux législatifs : de l'absence de droit à un droit uniquement expérimental.** Force est d'admettre que l'architecture décentralisée de la technologie *blockchain* se voit difficilement appréhendée par le droit[280]. La *blockchain* originelle, Bitcoin, a été au cœur de tous les débats éristiques. Le premier rapport du Sénat mettait en exergue un ensemble de risques à surveiller, tels que la volatilité, l'absence de garantie de convertibilité en monnaie ayant cours légal par les pouvoirs publics, le piratage des plateformes d'échanges comme Mt. Gox précitée ou encore l'anonymat[281], mais ne tarissait pas d'éloges sur la technologie et ses opportunités de valider « *d'autres choses* » que des transactions, comme des mots de passe, des titres d'identités, des diplômes et autres certificats, ou même des votes électroniques[282].

[279] C. Castet-Renard, « Quelles nouveautés en matière de preuve numérique », in Justice et cassation, Revue annuelle des avocats au Conseil d'État et à la Cour de cassation, Dossier La preuve, mai 2017, p.23.

[280] EU Blockchain Observatory and Forum, Legal and regulatory framework of *blockchains* and smart contracts, le 28 sept. 2019, p.11 : « *….tension between blockchain technology in general and prevailing legal and regulatory frameworks. Many of these tensions arise from fundamental properties of blockchain protocols, which are built on decentralized paradigms conceptually quite different from the more centralised approaches that are currently the norm* ». Pour la Professeure Florence G'Sell, il est possible de se demander « *si ces "architectures juridiques décentralisées" que sont les droits de Common Law n'auraient pas, de ce simple fait, plus de facilité à appréhender les réseaux décentralisés que les droits de tradition civiliste* » (F. G'Sell, « Comment traiter juridiquement la décentralisation ? Les ordonnances blockchain et la Lex Cryptographia », Blog de Florence G'Sell, dec. 2017, https://gsell.tech/traiter-juridiquement-decentralisation-ordonnances-blockchain-lex-cryptographia/ (consulté le 31/05/2020)).

[281] Sénat, commission des finances, Rapport d'information fait au nom de la commission des finances sur les enjeux lies au developpement du bitcoin et des autres monnaies virtuelles, P.Marini, F. Marc, « la regulation a l'epreuve de l'innovation : les pouvoirs publics face au developpement des monnaies virtuelles », coll. Les rapports du Sénat, juill. 2014, p.9-10.

[282] Notons qu'il est, à ce stade technologique, difficile de dissocier la technologie, des échanges de valeurs, car une blockchain nécessite obligatoirement une transaction avec des échanges de valeurs.

75. À la suite de la publication de ce rapport et de celui de Tracfin[283], c'est le droit fiscal qui se positionna pour la première fois en France de façon à lever l'impôt sur les crypto-monnaies. Une première instruction fiscale fut publiée le 11 juillet 2014 imposant au barème progressif de l'impôt sur le revenu les plus-values réalisées sur les crypto-monnaies. Les crypto-monnaies entrèrent après dans le patrimoine imposé au titre de l'impôt de solidarité sur la fortune (ISF) et furent aussi soumis aux droits de mutation à titre gratuit (DMTG). Elles restent néanmoins à ce jour toujours exonérées de TVA[284].

76. De cette mainmise fiscale sur les crypto-monnaies, le droit français décida d'exploiter le potentiel de transformation de la technologie qui les liait. La réception expérimentale de la preuve *blockchain* à travers le prisme du DEEP promettait alors d'assurer sécurité et traçabilité de certains titres et des minibons sur un support dématérialisé[285]. Cette consécration a ainsi donné une valeur légale aux registres de la *blockchain*, soit une efficacité juridique, une opposabilité aux tiers et une valeur probatoire aux inscriptions dans la *blockchain*. Première pierre à l'édifice qui est suivie de la récente adoption de la loi PACTE visant à accorder un cadre aux activités sur actifs numériques attractif et propice à l'innovation[286]. Nonobstant ces avancées normatives désireuses d'encadrer des pratiques et de donner plus de forces juridiques à certains usages, ces textes ne posent pas les linéaments de droit commun des preuves *blockchains*. Cette forme d'« *atrophie probatoire* »[287] entraine un flou juridique qui n'est dès lors pas dénué de risques.

III. La construction de l'étude

77. Les preuves *blockchains* bénéficient d'un ensemble de procédés cryptographiques les rendant fiables techniquement mais ne se voient pas transposées juridiquement. La question est

[283] Tracfin, Rapport « l'encadrement des monnaies virtuelles », recommandations visant a prevenir leurs usages a des fins frauduleuses ou de blanchiment, groupe de travail « monnaies virtuelles », juin 2014.
[284] CJUE 22 octobre 2015, aff. C-264/14 Skatteverket c. David Hedqvist ; note J. Huet, RDC 2017, n°113, p.54 ; note R. Vabres RISF 2016 n°1, p.170 ; adde T. Bonneau, « Analyse critique de la contribution de la CJUE à l'ascension juridique du bitcoin », *in* Liber amicorum Blanche Sousi, L'Europe bancaire, financière et monétaire, Rev. Banque 2016. Voir aussi pour les ICOs : rescrit fiscal du 7 aout 2018 BOI-RES-000054-20190807 : ce rescrit à portée générale précise que l'opération d'émission des jetons n'est pas soumise à TVA.
[285] Voir *supra* n°37.
[286] Cette nécessité législative est principalement ressortie des réponses à une consultation publique de l'Autorité des Marchés Financiers (AMF) de février 2017 (AMF, Document de consultation sur les *Initial Coin Offerings* (ICOs), le 26/10/2017 ; AMF, Synthèse des réponses à la consultation publique portant sur les *Initial Coin Offerings* (ICO) et point d'étape sur le programme « UNICORN », 22 fevr. 2018). S'en est suivi de près, le lancement d'un programme UNICORN dédié au suivi des ICOs (AMF, Communiqués de presse « L'AMF lance une consultation sur les Initial Coin Offerings et initie son programme UNICORN », 26 nov. 2017).
[287] Voir *infra* n°422 et s.

redoutablement complexe, tant elle touche une distorsion entre ces preuves cryptographiques de la *blockchain* issues des mathématiques pures et la preuve juridique. Cette distorsion a pour conséquence de générer une difficile détermination des qualifications applicables en droit et des imprécisions quant aux régimes afférents. Ces problématiques peinent à se résoudre sans étude approfondie. Ces preuves essuient un manque de conceptualisation juridique générale et une quasi-absence de reconnaissance normative, ne permettant pas de donner aux pratiques existantes dans le secteur de la *blockchain* des effets suffisamment importants en droit de la preuve. Ce problème ne saurait être éludé puisqu'il met en péril leur efficacité et admissibilité probatoire, qui ne sont pas actuellement pleinement garanties, notamment en cas de litige.

78. **Problématique.** L'étude s'attelera à comprendre comment les données enregistrées dans la *blockchain* - objets de preuves au concours de la vérité cryptographique - peuvent être admises en droit et reçues par les juridictions lors d'un contentieux.

79. Pour cela, sera mise en œuvre une opération de traduction juridique dont le résultat tendra à refléter la valeur des preuves *blockchains* cryptographiques, en matière probatoire. La signification du terme « *à l'aune de* » employé dans le titre de la recherche permet de comprendre le but de cette opération. Ce terme signifie initialement « *unité de mesure* » et puise ses origines dans d'anciennes unités de longueur appliquées au mesurage des étoffes[288]. De là, découle l'expression « *à l'aune de* » courrament utilisée pour signifier « *en considération de* ». Les preuves *blockchains* seront alors « *mesurées* » au regard du droit de la preuve. C'est en effet le droit de la preuve qui sera étudié en considération de ce nouveau sujet technologique : la blockchain. À la sincérité et sécurité cryptographique devra correspondre une sécurité juridique pour les sujets de droit quant au recours à cette technologie. L'étude suivra pour cela le cheminement traditionnel de la preuve au cours d'un procès : de son admission en droit, à son accès au débat judiciaire, pour finir par sa réception ou non par le juge.

80. D'une part, il s'agira d'accorder à ces preuves la force juridique requise avec toutes les réserves opérationnelles nécessaires. Ces preuves devront pouvoir être apportées au soutien d'un acte ou d'un fait dans les hypothèses de litiges. Ces développements auront trait à la question de savoir par quel moyen rendre admissible ces preuves juridiquement. À ce titre, la manière de transposer en droit la « *vérité cryptographique* », résultat des procédés techniques

[288] https://www.cnrtl.fr/definition/aune (consulté le 31/05/2020). Voir : E. Estaunie, *L'empreinte*, Ferenczi (ed. 1935), 1896, p. 28 : « *Ce drap, vendu à l'aune sur la voie publique* ».

des protocoles *blockchains*, sera précisément recherchée. Dans un contexte sans cesse renouvelé et adapté du droit de la preuve aux nouvelles technologies, il conviendra de reconnaître la vérité cryptographique comme une forme de vérité scientifique autonome, profitable à la vérité juridictionnelle.

81. Une fois ces preuves admises au débat judiciaire, les réflexions porteront d'autre part, sur la question de la réception de ces preuves par le juge et l'utilité *per se* de cet arsenal probatoire cryptographique pour les juridictions. C'est précisément l'appréhension de cette vérité cryptographique par le juge qui sera ici analysée.

82. Le cœur de cette démarche résidera concrètement dans la proposition d'une valeur juridique des preuves *blockchains* par leurs qualifications de droit commun et leurs régimes applicables associés. Cette proposition impliquera des suggestions d'adaptation, voire de reformulation du corpus de règles existant en droit de la preuve. Les limites des régimes spéciaux actuels (minibons, titres financiers et jetons) seront établies ainsi qu'une proposition de création de régime général international des preuves *blockchains*.

83. Par ailleurs, des développements seront consacrés à l'analyse du concours des juridictions et des auxiliaires de justice, *via* la détermination de leurs rôles dans la reconnaissance de ces preuves *blockchains*. En fonction des pouvoirs plus ou moins importants des juges, des huissiers de justice et des auxiliaires, des recommandations et des propositions seront formulées pour garantir l'équilibre dans leurs interventions respectives. Le renforcement de leur intervention et/ou des garanties d'indépendance seront ainsi suggérées.

84. **Méthodologie.** Disposant de peu d'antériorités doctrinales, les travaux menés constituent un sujet à « *défricher* », à la fois au niveau des opérations de conceptualisation et de définition, des développements théoriques, que des interrogations matérielles. Par conséquent, pour étudier ce sujet très émergent et d'une grande richesse, nous emprunterons plusieurs axes de recherche.

85. Selon une méthode empirique, l'intention essentielle des présents travaux est de comprendre et révéler la nature des preuves *blockchains* pour permettre leur transposition en droit et anticiper leur appréhension juridictionnelle. Le point de départ nécessaire à cette réflexion se concentrera alors sur des études de cas de dossiers traités en cabinet d'avocats tout au long de ces années de recherche qui ont mis en jeu des preuves *blockchains*. L'octroi de

conseils sur des analyses de risque de ces activités, la structuration juridique et la contractualisation de projets sont des pistes de réflexion à partir desquelles des résultats viables empreints de la pratique peuvent être dégagés. L'étude se situant trop en amont par rapport à l'avancement des usages et du marché de la *blockchain*, elle ne pourra mettre en lumière des résultats certains sur la partie contentieuse (les litiges sur les preuves *blockchains* étant peu présents, voire quasi-absents du paysage juridictionnel français) mais proposera des grandes tendances et des scenarii vraisemblables.

86. Les entretiens menés avec des praticiens, des experts techniques, et professeurs et/ou chercheurs en sciences dures, comme en sciences sociales, permettront également de mettre en perspective les différents avis sur ces preuves *blockchain*, d'inciter à remettre en cause les biais cognitifs, ainsi que d'abreuver cette étude.

87. Elle invitera à la mobilisation d'une grande variété de sources matérielles du droit - qu'il s'agisse des règles de droit de la preuve (théorie générale[289] et modes de preuves spécifiques), de la jurisprudence relativement peu dense à ce stade ou de la doctrine. Cette étude impliquera de plus de mettre en contraste ces sources et d'interroger leurs révisions compte tenu de ces nouvelles preuves *blockchains*. Cette démarche nous permettra de mettre en exergue l'évolution forte de la notion même de preuve et de vérité, ce qui confirmera les importants bouleversements que subit la « *branche* » du droit de la preuve au sujet de l'avancée de cette nouvelle technologie. Comme énoncé ci-après, ces règles de droit seront étudiées de manière non perméable avec les règles techniques (protocoles, algorithmes, autres applications développées sur la technologie). L'approche de cette étude sera justement de ne pas confronter ces règles de genres différents.

88. Si ces travaux seront essentiellement focalisés sur le droit français, européen, et international à venir, il conviendra de ne pas occulter le droit nord-américain et d'autres droits étrangers plus mûrs en la matière. Il s'agira de réaliser une comparaison entre tous les systèmes de preuves *blockchains* existants. Les preuves *blockchains* étant déjà reconnues dans certains droits positifs étrangers, une approche comparatiste constitue une ouverture sur l'opportunité et la méthode de consécration de ces preuves à emprunter ou non. De la même manière, les

[289] Etienne Vergès propose une restauration de cette théorie générale (E. Vergès, « Eléments pour un renouvellement de la théorie de la preuve en droit privé », *in* Mélanges J.-H Robert, Lexis Nexis 2012, p.853 et s.) alors qu'il s'agirait déjà de la construire selon Mustapha Mekki (M. Mekki, avant-propos in *La preuve : regards croisés*, *op. cit.*, 2015).

décisions jurisprudentielles françaises, européennes mais aussi étrangères, notamment chinoises, seront étudiées compte tenu de leurs avancées.

89. De façon générale, outre ces sciences sociales, précisément juridiques, devra être mobilisé l'ensemble des sciences qui concourent à ces preuves *blockchains*, appelées par certains la « *science de la preuve* »[290], pour correctement appréhender leurs transpositions juridiques. Afin d'éviter l'écueil d'un détachement des réalités techniques et d'occulter les particularismes des preuves *blockchains*[291], il s'agira par cette étude de s'aventurer en dehors de l'approche du droit de la preuve et des systèmes juridictionnels, ne suffisant pas à elle seule. Une approche interdisciplinaire sera alors mobilisée, par l'examen des notions des sciences mathématiques, cryptographiques et informatiques fondamentales. Cette étude n'aura toutefois pas la prétention de résoudre des problématiques ou d'émettre des propositions en sciences dures.

90. **Annonce du plan.** Tout d'abord, une partie préliminaire à cette étude posera les concepts juridiques et techniques de la recherche du droit de la preuve à l'aune de la *blockchain* (partie préliminaire). Il s'agira ensuite d'établir les jalons requis d'un cadre juridique des preuves de données enregistrées dans la *blockchain* au soutien de la traduction de la « *vérité cryptographique* » (partie 1), pour enfin dénoncer l'insuffisante appréhension juridictionnelle de ces preuves et y apporter des réponses (partie 2).

[290] O. Leclerc, J. Wigmore, *Un jalon vers une « science de la preuve ». La représentation graphique des raisonnements probatoires*, Tiré à part, Dalloz, févr. 2019 : ces auteurs soutiennent et militent pour la reconnaissance d'une science de la preuve, soit des principes de la preuve, complétement indépendants des règles qui régissent la procédure.

[291] Certains auteurs critiquent l'analyse sous le prisme unique du droit : « *La pensée juridique est trop souvent repliée sur son objet privilégié : le droit. Elle ne s'aventure guère au dehors* » (S. Hennette Vauchez, R. Encinas de Munagorri, O. Leclerc, C. Herrera, C. Miguel Herrera, *L'analyse juridique de (x): Le droit parmi les sciences sociales*, Kimé. Kimé, 2016).

PARTIE PRELIMINAIRE

A L'ETUDE DU DROIT DE LA PREUVE A L'AUNE DE LA *BLOCKCHAIN*

92. Pour mener à bien l'étude du droit de la preuve au regard de la *blockchain*, sans analyses arguties mais considérant sa technicité et son caractère nouveau, il sera dressé des prérequis tant techniques (titre 1), que juridiques (titre 2).

TITRE 1

LES PREALABLES TECHNIQUES A L'ETUDE DU DROIT DE LA PREUVE A L'AUNE DE LA *BLOCKCHAIN*

93. Le caractère abscons des preuves *blockchains* n'est pas de nature à clarifier la compréhension des opportunités qu'elles représentent. Nous établirons des préalables techniques dans l'intention de rendre plus intelligibles ces preuves pour les développements de l'étude. Ces préalables techniques catégorisent les preuves *blockchains* en fonction de leurs supports sous-jacents (chapitre 1), constituant un ensemble de données que nous pouvons ordonner selon une certaine classologie (chapitre 2).

CHAPITRE 1

LE SUPPORT DES PREUVES *BLOCKCHAINS*

94. Les preuves *blockchains* s'appuient sur des supports, bases de celles-ci. Sont propres à faire évoluer ces preuves et relever leurs spécificités, les différentes natures des *blockchains* utilisées (section 1) et les procédés attingents (section 2).

Section 1 : La nature des *blockchains* utilisées

95. Les *blockchains* sont par essence à géométrie variable, selon leurs typologies, comme mentionné en introduction : *blockchain* publique (paragraphe 1), et *blockchain* privée (paragraphe 2), ainsi que leurs protocoles[292]. Cela emporte des conséquences sur les preuves *blockchains*. Chaque architecture implique divers choix de conception impactant directement ces preuves, tels que la topologie du réseau (ouvert ou fermé), la formation d'un consensus (comment parvient-on à un consensus et qui y participe ?), le partage des données (qui reçoit les données ? comment sont-elles diffusées ? et qui y a accès ?). Les preuves seront alors variables en fonction d'une part, du nombre de nœuds, c'est-à-dire de la résilience du réseau : plus ce nombre est grand, moins le risque de collusion entre eux ou de manipulation du consensus est important. La répartition des pouvoirs d'autre part, aura son importance, c'est-à-dire de la gouvernance prévue et établie (par exemple, si l'un des membres dispose de droits exorbitants de modifier le registre, cela porterait atteinte à l'immuabilité de ces preuves).

[292] Voir *supra* n°19 et s.

Paragraphe 1 : La *blockchain* publique

96. Les *blockchains* publiques utilisent pour l'essentiel les protocoles Bitcoin (A) et Ethereum (B) marqués de particularismes. Elles sont réputées sécurisées, stables, et composées de registres difficilement altérables. Cependant, certains cas d'usage prévoient que ces protocoles initialement mobilisés pour le développement de *blockchains* publiques servent de modèle protocolaire pour le déploiement de *blockchains* privées[293]. Nous présenterons ces protocoles à la « *manière manichéenne* » (avantages et inconvénients) pour relever leurs caractéristiques déterminantes par rapport aux preuves *blockchains*.

A. Le protocole Bitcoin

97. Le choix du protocole Bitcoin induit des avantages (1) et des inconvénients (2) qui sont autant de particularités distinguant les preuves *blockchains*.

1. Les avantages probatoires issus du protocole Bitcoin

98. Les protocoles publics sont étudiés pour offrir une sécurité importante dans la réalisation de transactions entre participants : ces dernières sont cryptées et validées par le réseau, de manière décentralisée, sans passer par un système « *central* » par définition plus vulnérable[294]. En l'absence de piratage ou d'attaque goldfinger, ce réseau non erratique est considéré comme particulièrement stable car il ne comptabilise pas de dysfonctionnement majeur depuis 2009[295].

99. De surcroît, c'est un réseau « *résilient à la censure* » qui est robuste[296]. Plus les nœuds sont importants (ce qui est le cas du protocole Bitcoin), plus les transactions sont difficilement

[293] Le protocole Ethereum par exemple, a été largement testé par les banques : 57 % des banques font l'expérience de l'une ou l'autre des deux méthodes du réseau public Ethereum ou de sa version privée (Cambridge Centre for Alternative Finance, University of Cambridge Judge Business School, Global blockchain benchmarking study, *op.cit.*, p.8).
[294] Sénat, Commission des finances, rapport d'information fait au nom de la commission des finances sur les enjeux liés au développement du bitcoin et des autres monnaies virtuelles, P.Marini, F. Marc, « La régulation à l'épreuve de l'innovation : les pouvoirs publics face au développement des monnaies virtuelles », coll. Les rapports du sénat, juill. 2014.
[295] EU Blockchain Observatory and Forum, Scalability interoperability and sustainability of *blockchains*, le 6 mars 2019, p.10.
[296] Parlement européen, Résolution du 3 oct. 2018 sur les technologies des registres distribués et les chaînes de blocs: renforcer la confiance par la désintermédiation (2017/2772(RSP)), P8_TA(2018)0373, point J :

altérables, voire inaltérables[297]. Le registre qui répertorie les transactions est par conséquent quasiment infalsifiable. Pour le modifier, il conviendrait de déployer la totalité de la puissance de calcul utilisée pour valider chacun de ses blocs. Cette opération semble actuellement impossible au vu de la puissance du réseau Bitcoin[298]. Enfin, ce protocole mis en œuvre par des logiciels libres peut être audité et vérifié (comme les autres protocoles publics).

2. Les inconvénients probatoires issus du protocole Bitcoin

100. Tout d'abord, les bonnes pratiques de développeurs déconseillent d'utiliser le protocole Bitcoin pour la pratique du stockage de données pure et simple dans cette *blockchain*[299]. Il doit être en effet relevé que seule une quantité limitée de données peuvent être stockées dans la *blockchain* publique[300]. Précisément, dans une transaction de la *blockchain* Bitcoin, seule une place de 80 octets est disponible[301]. Ce faisant, les données en clair ajoutées pour se préconstituer des preuves grâce à cette technologie ne pourront être ajoutées en grande quantité. Pour pallier cette carence de place, le stockage de l'empreinte numérique de ces données pourra être utile[302].

101. En outre, dans l'objectif de parvenir à la validation des transactions, le protocole Bitcoin fait face à deux types d'obstacles. D'une part, un obstacle quant aux imperfections du réseau, telle que la « *latence* », soit le délai de transmission des communications informatiques, puisque le réseau est distribué partout sur Internet et il arrive qu'il soit amené à faire face aux plantages de « *nœuds* ». Il peut effectivement exister des défaillances dans le réseau en raison d'une mauvaise connectivité Internet, par exemple. Dans cette hypothèse, il n'est pas vraiment

« *considérant que les cyberattaques sont considérées comme ayant moins d'impact sur de telles chaînes, étant donné qu'elles doivent réussir à cibler un grand nombre de copies plutôt qu'une version centralisée* ».

[297] Cambridge Centre for Alternative Finance, University of Cambridge Judge Business School, Global blockchain benchmarking study, *op.cit.*, p.17, 21.

[298] R. Pérez Marco, « Blockchain : l'autre révolution venue du bitcoin », *op.cit.*

[299] voir « OP_RETURN and data in the block chain », https://bitcoin.org/en/release/v0.9.0#opreturn-and-data-in-the-block-chain (consulté le 31/05/2020)

[300] Voir *supra* n°21.

[301] A. M. Antonopoulos, *Mastering Bitcoin : Unlocking Digital Cryptocurrencies*, *op.cit.*, p.133 : « *In version 0.9 of the Bitcoin Core client, a compromise was reached with the introduction of the OP_RETURN operator. OP_RETURN allows developers to add 80 bytes of nonpayment data to a transaction output. However, unlike the use of "fake" UTXO, the OP_RETURN operator creates an explicitly provably unspendable output, which does not need to be stored in the UTXO set. OP_RETURN outputs are recorded on the blockchain, so they consume disk space and contribute to the increase in the blockchain's size, but they are not stored in the UTXO set and therefore do not bloat the UTXO memory pool and burden full nodes with the cost of more expensive RAM* ».

[302] Voir les développements *infra* n°100 ; 136 et s ; n°145.

possible d'exécuter le consensus auquel tous les nœuds doivent participer[303]. D'autre part, une difficulté demeure quant aux tentatives délibérées de la part de quelques validateurs malveillants de subvertir le processus[304]. L'ensemble de ces raisons rendent ainsi moins efficientes la possibilité de générer des preuves *blockchains*.

102. Enfin, le nombre de transaction possible par seconde a nécessairement un impact sur la quantité potentielle de preuves ancrées dans la *blockchain*. Le manque de performance de ce réseau ne peut pas être évité. Il est sacrifié sur l'autel de sa sécurisation. Le nombre de transactions par seconde imposé par le protocole, est de sept[305]. Cette vitesse est considérée comme très lente comparée au débit de grands processeurs de cartes de crédit. Le réseau de Visa serait capable de traiter vingt-quatre mille transactions par seconde dans le monde entier[306]. Le bloc de transactions est par ailleurs limité en taille à un mégaoctet, ce qui limite le nombre de transactions validées dans un bloc[307]. Le temps moyen pour miner un bloc de transactions d'environ dix minutes est également lent[308]. S'ajoute à cela, un temps de latence moyen de douze secondes pour propager un bloc vers l'ensemble des nœuds. C'est seulement après quarante secondes que les nœuds reçoivent le bloc[309]. Partant de ces constats, des solutions à ces problématiques pour un passage à l'échelle du protocole Bitcoin ou autrement appelé « *scalabilité* » sont étudiées par les développeurs et experts techniques[310].

[303] A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder, *Bitcoin and Cryptocurrency Technologies*, *op. cit.*, p.54.
[304] Voir *infra* n°43 sur l'attaque Goldfinger.
[305] A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder, *Bitcoin and Cryptocurrency Technologies*, *op. cit.*, p.95.
[306] EU Blockchain Observatory and Forum, Scalability interoperability and sustainability of *blockchains*, *op.cit.*, p.10.
[307] *Ibid.*, p.95.
[308] C. Berbain, « La *blockchain* : concept, technologies, acteurs et usages », Annales des mines - réalités industrielles, août 2017, p.7.
[309] I. Pavel, « La blockchain – les défis de son implémentation », Annales des mines - réalités industrielles, août 2017, p.21.
[310] Conférence Scaling Bitcoin, Synthèse partie 2 : scalabilité, Université de Stanford, 4 et 5 nov. 2017, https://bitconseil.fr/scaling-bitcoin-synthese-2-scalabilite/ (consulté le 31/05/2021).

B. Le protocole Ethereum

103. Les avantages (1) et inconvénients (2) du protocole Ethereum, protocole ajoutant un degré de sophistication à la *blockchain* Bitcoin de référence, doivent être précisés.

1. Les avantages probatoires issus du protocole Ethereum

104. C'est le protocole qui rassemble, dans une large mesure, la majeure partie des développeurs, des applications et utilisateurs de l'écosystème de la technologie *blockchain*. Ce protocole repose sur un réseau étendu et complet avec son propre navigateur Internet, son langage de programmation du *smart contract* (le « *solidity* ») et son système de paiement (les « *ethers* »)[311]. Le temps moyen de minage des blocs dans Ethereum est de douze secondes, ce qui atteste de validations plus rapides que dans bitcoin[312].

105. Outre sa sécurité cryptographique, ce protocole propose une couche technologique additionnelle car elle intègre la création de *smart contracts* qui s'auto-exécutent[313]. L'usage de ce protocole pour des applications d'ancrage de données est, à l'accoutumé, plus usuel. Le *smart contract*, intégré dans une transaction, disposera alors d'une fonction qui prendra les paramètres des ancrages comme suit : « *si* » tu me donnes une empreinte, la « *conséquence* » sera que je la conserve dans la *blockchain*. Il peut être intéressant d'utiliser le *smart contract* pour cet usage car on peut y mettre, en outre, des métadonnées qui permettent de retrouver la correspondance entre la donnée et l'identité de la personne.

2. Les inconvénients probatoires issus du protocole Ethereum

106. Le problème majeur du protocole est le codage des *smart contracts* en « *solidity* ». Peu de programmeurs connaissent parfaitement ce langage ce qui laisse à douter du caractère infaillible de chaque instruction et, scientifiquement prouvé de chaque commande. Par ce

---

311 V. Butterin, « A next-generation smart contract and decentralized application platform », dec. 2013, https://eth.wiki/en/white-Paper (consulté le 31/05/2020).

312 https://www.ethereum-france.com/quest-ce-que-la-preuve-denjeu-proof-of-stake-faq-par-v-buterin-traduction-francaise/ (consulté le 31/05/2020).

313 Voir *infra* n°16.

langage, les erreurs de code ne sont pas exclues. Ce protocole laisse alors plus de place à l'erreur humaine et, par la même occasion, à l'exploitation de celles-ci par des acteurs malintentionnés.

107. Également, le problème identique à celui de Bitcoin est le passage à l'échelle, malgré des efforts évidents pour désengorger le réseau. Les architectures de ces *blockchains* de seconde génération sont tout de même structurellement plus adaptées à une mise à l'échelle et partent avec un avantage technique. Afin de contingenter la consommation de ressources et d'assurer la stabilité du réseau, les blocs d'Ethereum sont limités à la taille de huit millions d'unités de « *gas* »[314].

108. Enfin ce protocole, bien que stable dans sa version originelle[315], a fait l'objet d'une attaque Goldfinger sur Ethereum classique (le *fork* d'Ethereum) comptabilisant une perte d'environ un million de dollars[316]. Plusieurs autres incidents importants sont répertoriés, comme celui du détournement de 3 million d'ethers (environ 62 millions de dollars au cours de l'époque) le 17 juin 2016, suite à l'exploitation d'une erreur dans le code sur l'entité autonome dite « *The DAO* »[317], ou encore celui en date du 19 juillet 2017 durant lequel 587 des portefeuilles « *Parity* » comptabilisant 513 774 ethers en totalité (environ 120 millions de dollars au cours de l'époque) auraient été perdus suite à une vulnérabilité dans le code d'un *smart contract* déployé sur tous les portefeuilles virtuels [318].

Paragraphe 2 : La *blockchain* privée

109. Le protocole Hyperledger a pour objectif d'offrir des canevas permettant le développement d'applications décentralisées *blockchains*[319], à destination essentiellement des entreprises, ce qui présente certains avantages (1) et inconvénients (2) pour la preuve.

[314] Pour faire fonctionner un smart contract sur le réseau Ethereum, il convient d'utiliser de la puissance de calcul. Le *« gas »* (essence en français) est une unité de mesure du temps de travail informatique nécessaire pour mener à bien cette opération.
[315] Ethereum a fait l'objet d'une divergence idéologique suite à l'évènement « *The DAO* » en 2016 qui a abouti à la naissance Ethereum Classic et ainsi la séparation entre Ethereum et Ethereum Classic en deux lors d'un *Hardfork*. Dans sa version originelle, aucune cyber-attaque réussie n'a été recensée.
[316] https://www.coinhouse.com/fr/ethereum-classic-subit-une-attaque-51/ (consulté le 31/05/2020).
[317] https://www.ethereum-france.com/the-dao-post-mortem/ (consulté le 31/05/2020).
[318] https://www.parity.io/a-postmortem-on-the-parity-multi-sig-library-self-destruct/ (consulté le 31/05/2020).
[319] Le protocole Ethereum en sus des *blockchain* publique, offre dorénavant des possibilités de concevoir des *blockchains* de types privées.

A. Les avantages probatoires issus de la *blockchain* privée

110. De nature flexible et adaptable, ces protocoles permettent de constituer des composants *sui generis* pour une *blockchain* en vue d'établir un réseau interne privé ou un réseau entre plusieurs acteurs économiques ayant des intérêts à détenir une source de vérité partagée. Certains choix stratégiques comme le nombre de nœuds hébergeant les données, la gouvernance, les acteurs tranchant la validation, le choix des destinataires pour une éventuelle « *diffusion sélective* » des données sont opérés[320].

111. Outre le fait de pouvoir mutualiser des moyens et des expertises dans une *blockchain* entre plusieurs entreprises, la cause qui pousse au choix de ces *blockchains* est souvent liée à des contraintes opérationnelles comme un besoin de stockage plus important de données[321], des transactions plus nombreuses et une validation plus rapide. Par exemple, le consortium Libra annonce une moyenne de mille transactions par seconde[322]. En définitive, la possibilité de générer des preuves de données par une *blockchain* privée aura pour effet de réaliser davantage d'opérations plus rapidement et de stocker plus de données, que dans la *blockchain* publique.

B. Les inconvénients probatoires issus de la *blockchain* privée

112. La limite essentielle de ces *blockchains* est le caractère isolé du registre en ce qu'il n'a de valeur qu'entre les membres de la *blockchain*[323]. Ce sont les membres autorisés qui valident eux-mêmes les transactions et hébergent des nœuds. Ce registre est dès lors exposé à plus de risques de modifications, voire de falsifications et d'effacements (sauf conventions contraires prévues par les parties). Pour offrir davantage de garanties, certaines pratiques permettent d'ancrer dans une *blockchain* publique immuable, des données inscrites dans une *blockchain*

[320] Uniquement 30% des opérationnels, participants à l'étude du Cambridge Center for Alternative Finance disent utiliser ce système de diffusion sélective (Cambridge Centre for Alternative Finance, University of Cambridge Judge Business School, Global blockchain benchmarking study, *op.cit.*, p.53).

[321] Cambridge Centre for Alternative Finance, University of Cambridge Judge Business School, Global blockchain benchmarking study, *op.cit.*, p.53.

[322] https://www.numerama.com/business/527274-crypto-monnaie-comment-la-libra-compte-surmonter-les-defauts-du-bitcoin-et-dethereum.html (consulté le 31/05/2020).

[323] Résolution du 3 oct. 2018 sur les technologies des registres distribués et les chaînes de blocs: renforcer la confiance par la désintermédiation (2017/2772(RSP)), P8_TA(2018)0373, point 42 : « *souligne que pour que les TRD inspirent confiance, il est nécessaire de disposer d'un grand nombre de registres distribués solides et développés afin d'éviter que les données ne se concentrent dans les mains de quelques acteurs du marché, ce qui pourrait donner lieu à des collusions; encourage la création de pôles de TRD dans toute l'Union européenne* ».

privée afin de procéder à une forme de ré-ancrage. Il ne serait même plus nécessaire en pratique de déployer une *blockchain* privée dans ces cas mais sa substitution par un simple coffre numérique interne ou intra-structure permettrait d'ancrer ensuite les données dans une *blockchain* publique pour se prémunir du caractère infalsifiable de celle-ci.

113. Qui plus est, la mise en place de ces *blockchains* peut souvent se révéler complexe puisqu'elle nécessite de mettre en œuvre des mesures complémentaires techniques avec une habilitation des participants, des audits[324] et un encadrement juridique impliquant d'établir les termes et conditions entre les membres de la *blockchain* (incluant les modalités de preuves, de confidentialité, de partage des résultats, de désignation de la juridiction compétente, de clause de non concurrence), de créer une société de projet avec un pacte d'actionnaires et des statuts, et de réaliser des notifications en droit de la concurrence dans l'hypothèse de consortium d'acteurs[325].

Section 2 : Les procédés techniques utilisés

114. De ces typologies de *blockchains* et différents protocoles, se dégagent des procédés techniques assemblés, plus ou moins identiques à tous, outils de preuves (paragraphe 1) que nous tenterons de classifier (paragraphe 2).

Paragraphe 1 : Les procédés techniques combinés formant les preuves *blockchains*

115. Des procédés cryptographiques déjà connus (A) sont mobilisés dans les *blockchains* mais d'autres constituent des avancées technologiques capitales (B).

A. Les procédés techniques traditionnels constitutifs de preuves *blockchains*

116. Au sein de la *blockchain*, des procédés techniques classiques sont utilisés tels que la cryptographie asymétrique au soutien de la création de signatures numériques (1) et la fonction de hachage pour la formation d'empreintes numériques (2).

[324] S. de Thésut Dufournaud, « La blockchain de consortium », *op. cit.*, p.2.
[325] *Ibid*., p.3.

1. La cryptographie asymétrique au soutien de la création de signatures numériques

117. **Cryptographie Moderne.** La cryptographie traditionnelle désigne selon le Professeur Richard Baron, chercheur en sciences informatiques un « *ensemble des méthodes permettant de protéger une information en la recodant de façon à ce qu'elle ne soit pas compréhensible pour un tiers non-autorisé* »[326]. Cet ensemble de méthodes doit répondre à trois enjeux : un service d'intégrité garantissant le contenu d'un fichier, un service d'authenticité pour assurer l'identité d'une donnée ou d'un fichier par une signature numérique (la non-réputation) et un service de confidentialité pour garantir que le contenu d'un fichier n'est pas accessible aux tiers[327]. Alors que la cryptographie moderne est entendue plutôt comme « *l'étude scientifique des techniques de sécurisation des informations numériques, des transactions et des calculs distribués* » et dont l'objet porte sur « *des problèmes qui peuvent survenir dans tout calcul distribué (...)* »[328]. La nouvelle conception de la cryptographie inclut désormais l'étude scientifique des calculs distribués. Or, notons que ces techniques et ce conception poursuivent un but unique de réponse aux « *... problèmes majeurs posés à la fois aux pouvoirs publics et à la communauté scientifique pour que la cryptographie puisse assurer la protection des libertés individuelles, dans un monde envahi par le numérique, sans risquer d'être détournée à des fins malhonnêtes* »[329].

118. **Distinction entre cryptographie symétrique et asymétrique.** Il existe une distinction entre la cryptographie symétrique et asymétrique ou la cryptographie dite respectivement à « *clé privée* » et à « *clé publique* »[330]. La cryptographie est symétrique lorsqu'un message est chiffré par l'émetteur à l'aide d'une clé. Ce message chiffré est ensuite transmis au destinataire qui, à l'aide de cette même clé, déchiffre le message pour pouvoir le lire en clair. Ce procédé est peu coûteux en temps de calcul[331]. Il est souvent fait référence à Alice et Bob pour expliquer la cryptographie. L'idée est de supposer qu'Alice veuille transmettre un message à Bob sur un

[326] R. Baron, « Introduction aux technologies blockchain supports des crypto-monnaies », *op.cit.*, p.37 n°1.
[327] Conférence de presse Médaille d'or 2006, Les enjeux de la cryptologie, CNRS, 6 oct. 2006, http://www2.cnrs.fr/sites/communique/fichier/6_enjeux_charte.pdf (consulté le 31/05/2020).
[328] J. Katz, Y. Lindell, *Introduction to Modern Cryptography*, *op.cit.*, p.3.
[329] Conférence de presse Médaille d'or 2006, Les enjeux de la cryptologie, CNRS, 6 oct. 2006, http://www2.cnrs.fr/sites/communique/fichier/6_enjeux_charte.pdf (consulté le 31/05/2020).
[330] J. Katz, Y. Lindell, *Introduction to Modern Cryptography*, *op.cit.*, p.45-226 et p.229-494.
[331] F. Recher, A. Bodin, « Chapitre "Cryptographie" - Partie 4 : La cryptographie à clé publique », Cours et exercices de mathématiques, Université de Lille et Unisciel, 4 nov. 2013 https://m.youtube.com/watch?v=M7vOxKVLsVY&list=PL024XGD7WCIEii2U_HKeprCTJA4xb-uJ6&index=7&t=0s (consulté le 31/05/2020).

réseau tout en maintenant secret ce message en présence d'un tiers qui écoute. C'est grâce à une clé secrète partagée entre eux que le message pourra être sauvegardé et ensuite découvert par Bob[332]. Les protocoles de chiffrement à clé privée peuvent s'illustrer par l'image du coffre-fort. L'émetteur et le destinataire possèdent chacun la clé d'un même coffre-fort. L'émetteur peut déposer lorsqu'il le souhaite un message qu'il destine à une personne. Ce destinataire pourra venir en prendre connaissance quand bon lui semble. La cryptographie symétrique nécessite que les deux correspondants se partagent et connaissent la clé, avant l'échange, ce qui n'est pas sans risque. Pour pallier cet inconvénient, la cryptographie asymétrique permet de partager de manière sécurisée, une clé entre deux correspondants, afin de prévenir l'interception de cette clé par une personne tierce, et ainsi contrecarrer la lecture des données chiffrées sans autorisation[333].

119. **Atouts de la cryptographie asymétrique dans l'authentification.** La cryptographie asymétrique permet grâce à une paire de clés par correspondant de chiffrer des données confidentielles avec une clé publique et de les déchiffrer avec une clé privée[334]. Autrement dit, deux clés sont préparées par le destinataire : une clé publique qu'il diffuse à tout le monde et une clé privée qu'il conserve secrète. Si l'émetteur souhaite envoyer un message au destinataire, il récupère la clé publique dudit destinataire et va chiffrer son message à l'aide de sa propre clé privée pour transmettre le message au destinataire. Le destinataire sera le seul à pouvoir déchiffrer le message en utilisant sa propre clé privée.

120. Ici, il peut être fait référence à l'image d'une boîte aux lettres, si l'émetteur souhaite envoyer un message au destinataire, il le dépose dans sa boîte aux lettres, dont le destinataire sera logiquement le seul à en avoir la clé et donc à prendre connaissance du message envoyé. La clé publique est symbolisée par la boîte aux lettres dans laquelle tout le monde pourra déposer un message car elle est publique et la clé privée qui ouvre la boîte aux lettres, quant à elle, est la clé secrète[335].

121. Le lien mathématique particulier existant entre les clés privée et publique de chacun permet la vérification, à l'aide de la clé publique de l'émetteur, que l'auteur est bien celui qui a

[332] D. Boneh, V. Shoup, *A Graduate Course in Applied Cryptography*, Université de Stanford, sept. 2017, p.4.
[333] F. Recher, A. Bodin, « Chapitre "Cryptographie" - Partie 4 : La cryptographie à clé publique », *op.cit.*
[334] Il est créé en 1976 par deux scientifiques Whitfield Diffie et Martin Hellman qui ont imaginé une solution rendant le processus de chiffrement public (les algorithmes ainsi que la clé publique) gardant seulement la clé de déchiffrement secrète.
[335] F. Recher, A. Bodin, « Chapitre "Cryptographie" - Partie 4 : La cryptographie à clé publique », *op.cit*.

écrit au destinataire. On parle alors « *d'authentification* »[336]. L'authentification en cryptographie signifie donc l'« *action de s'assurer de l'identité d'une entité donnée ou de l'origine d'une communication ou d'un fichier* », laquelle devra faire l'objet d'une attention particulière lors de sa confrontation avec la définition juridique de ce terme[337]. Ce chiffrement a été mis en œuvre par l'algorithme RSA considéré comme la « *cheville ouvrière* » de nombreux protocoles de cryptographie et toujours considéré comme sûr[338]. Cet algorithme porte les initiales de ses inventeurs Ronald Rivest, Adi Shamir et Leonard Adleman à son origine en 1978[339]. Nonobstant sa sécurité importante, il n'est toutefois pas impossible, bien que laborieusement[340], de voir aboutir un processus de déchiffrement, surtout dans le contexte du calcul quantique[341].

2. La fonction de hachage au soutien de la création d'empreintes numériques

Une fonction de hachage engendre la création d'une empreinte numérique permettant parallèlement d'y associer une unité de temps.

122. **Le fonctionnement du hachage cryptographique : un procédé technique sécurisé permettant le calcul d'une empreinte numérique.** La fonction de hachage est une fonction mathématique à sens unique, permettant d'obtenir à partir d'une valeur d'entrée de données (textes ou fichiers), une valeur de sortie appelée « *empreinte* » ou « *condensat* ». Les fonctions de hachage sont dites cryptographiques même si elles ne font aucun usage des clés précitées pour la cryptographie asymétrique[342]. Il convient de distinguer la fonction de l'algorithme. L'algorithme de hachage détermine la manière dont la fonction de hachage sera utilisée. Un algorithme de hachage est un programme qui a pour objectif d'appliquer la fonction de hachage de données entrées en vue d'obtenir une valeur de sortie.

---

[336] F. Cayre, « Cryptographie, du chiffre et des lettres », Revue DocSciences n°5, Les clés de la révolution numérique, CRDP de l'académie de Versailles, nov. 2008, https://interstices.info/cryptographie-du-chiffre-et-des-lettres/ (consulté le 31/05/2020).
[337] Voir *supra* n°265.
[338] CultureMATH, « Sur l'algorithme RSA », ENS, janv. 2003, https://culturemath.ens.fr/content/sur-lalgorithme-rsa (consulté le 31/05/2020).
[339] CultureMATH, « Sur l'algorithme RSA », *op.cit.*
[340] J. Gómez, *Codage et cryptographie. Mathématiciens, espions et pirates informatiques*, coll. Le monde est mathématique, RBA, Ed. L'Obs août 2019, p.104.
[341] https://www.coinhouse.com/fr/lordinateur-quantique-menace-le-bitcoin/ (consulté le 31/05/2020) ; https://journalducoin.com/bitcoin/google-va-t-il-tuer-bitcoin-avec-la-suprematie-quantique/ (consulté le 31/05/2020).
[342] R. Baron, « Introduction aux technologies *blockchain* supports des crypto-monnaies », *op.cit.*, p.37, n°1.

123. Tout d'abord, les fonctions de hachage cryptographiques disposent de plusieurs propriétés ordinaires intéressant la preuve :

- La résistance aux collisions est la première propriété reconnue à la fonction de hachage[343]. Une collision est le fait que deux valeurs d'entrées différentes engendrent une valeur de sortie identique. Autrement dit, le risque de collision correspond au fait que deux ensembles de données puissent donner la même empreinte. Être résistant à cette collision est dès lors l'impossibilité de produire deux fois la même sortie, pour des données différentes[344].

- La fonction de hachage est, en outre, résistante à la première pré-image signifiant qu'il est calculatoirement impossible de trouver l'entrée qui a produit la valeur de sortie[345].

- C'est une fonction déterministe. Un résultat identique est obtenu si on hache un même ensemble de données.

- Elle est à sens unique ou dite « *bijective* » ce qui signifie qu'il n'existe pas de fonction inverse permettant de récupérer les données ancrées à partir de l'empreinte[346]. Autrement dit, il est possible de calculer une empreinte mais il n'est pas possible de l'inverser, de remonter à l'ensemble de données à partir desquelles cette empreinte a été calculée[347].

- Elle permet la compression de données car la valeur d'entrée est plus grande que la valeur de sortie. Autrement dit, la fonction de hachage permet de transformer une chaine de caractères de longueur indifférente en une autre chaine de longueur fixe. Par exemple, il sera calculé 64 caractères pour la fonction utilisée par le protocole Bitcoin.

[343] A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder, *Bitcoin and Cryptocurrency Technologies*, *op. cit.*, p.23.
[344] S. Zimmer, *Mécanismes cryptographiques pour la génération de clefs et l'authentification*, thèse ss. dir. D. Pointcheval, Ecole polytechnique, 2008, p.25-26.
[345] Séminaire IRT SystemX, D. Augot, fonction de hachage et blockchain, 22 nov. 2017.
[346] A. Takkal Bataille, J. Favier, *Bitcoin. La monnaie acéphale*, *op.cit.*, p.92.
[347] OPECST, Les enjeux technologiques des *blockchains* (chaînes de blocs), *op.cit.*, p.27.

124. Pour ce qui est de l'algorithme de hachage cryptographique, autrement appelé « *SHA* » (*Secure Hash Algorithm* signifiant Algorithme de Hachage Sécurisé), il a évolué en fonction des capacités de calcul de nos ordinateurs dans le dessein essentiel d'éviter de devenir vulnérable. Il existe plusieurs versions de SHA : SHA0 introduit en 1993 par la National Security Agency (NSA), soit l'agence nationale de la sécurité américaine, qui est devenue désormais obsolète puisque totalement vulnérable[348]. SHA1, son algorithme remplaçant créé en 1995 est désormais cassé et est sorti des standards[349]. La norme SHA256 est développée par la NSA et est publiée en 2001. Ce dernier avec SHA512 sont créées pour offrir des sorties plus importantes[350]. Enfin, les algorithmes SHA3[351] et BLAKE2[352] sont nés en 2012, l'un offrant sécurité, et l'autre vitesse.

125. Le résultat d'une fonction de hachage - issu d'un algorithme précis - d'un ensemble de données est la création d'une empreinte numérique. Elle comporte de nombreuses caractéristiques propres à la détection de l'altération de cet ensemble de données.

126. **Les caractéristiques de l'empreinte numérique intéressant la preuve de l'intégrité des données.** L'empreinte numérique de données ou « *hash* » est une courte suite de caractères alphanumériques (chiffres et lettres à la suite les uns des autres) qui lui est propre[353]. C'est en effet une empreinte de taille fixe créée à partir d'une donnée de taille variable, fournie en entrée[354]. Elle ne contient aucune information de la donnée initiale.

127. Des caractéristiques inhérentes à l'empreinte numérique de données sont observées :

- L'empreinte est unique. Le changement d'une lettre de la valeur d'entrée - même un seul bit d'un fichier - peut donner une valeur de sortie complètement différente[355]. Si les données sont effectivement modifiées, l'empreinte calculée sera différente[356]. Si la même opération de calcul d'empreinte est réalisée pour le même ensemble de données,

[348] D. Boneh, V. Shoup, *A Graduate Course in Applied Cryptography*, *op.cit.*, p.299.
[349] *Ibid.*
[350] *Ibid.*
[351] SHA-3 ou initialement appelé « *Keccak* » est un algorithme de fonction de hachage cryptographique conçu par Guido Bertoni, Joan Daemen, Michaël Peeters et Gilles Van Assche et élu par la NIST hash function competition.
[352] Z. O'Whielacronx, « introducing BLAKE2 – an alternative to SHA-3, SHA-2 and MD5 », 21 déc. 2012, https://lists.randombit.net/pipermail/cryptography/2012-December/003562.html (consulté le 31/05/2020).
[353] OPECST, Les enjeux technologiques des *blockchains* (chaînes de blocs), *op.cit.*, p.26.
[354] *Ibid*., p.27.
[355] R. Baron, « Introduction aux technologies *blockchain* supports des crypto-monnaies », *op.cit.*, p.37, n°1.
[356] A. Evans, W. Kantrowitz, E. Weiss, « A User Authentication Scheme Not Requiring Secrecy in the Computer », Communications of the ACM 17(8):437–442, 1974 ; G. B. Purdy, « A High Security Log-in Procedure », Communications of the ACM 17(8):442–445, 1974.

le résultat obtenu sera identique[357]. Par exemple, l'empreinte calculée avec l'algorithme SHA256 du terme « *thèse* » équivaut à : « *5d7df63d74998fafd63b9ff79dae8cd3aaacbe9d41f73ef98b71916bf6226e04* », alors que l'empreinte du terme « *thèses* » équivaut à une autre empreinte : « *5d44f3c27e1b0294965b478c77c22e0f0c1068a3a953486a4b7622593899e81a* ».

- L'empreinte d'un ensemble de données est imprédictible. Il est impossible de prévoir la valeur qu'elle aura même en ayant connaissance des empreintes de données proches.

- L'empreinte est irréversible. Il est impossible à partir de l'empreinte (64 lettres de a à f ou chiffres de 0 à 9) de remonter aux données en clair[358].

Par exemple, dans le domaine des activités postales, le cachet postal électronique use de l'empreinte numérique « *horodatée et scellée par chiffrement, qui est apposée par un opérateur postal et accompagne un objet postal transmis sous forme électronique* »[359].

B. Les procédés techniques particuliers des preuves *blockchains*

128. En fonction des protocoles de *blockchains*, des algorithmes développés - dont les plus couramment utilisés sont la « *preuve de travail* » (ou « *Proof-of-Work* ») (1) et la « *preuve d'autorité* » (ou « *Proof-of-Authority* ») (2) - permettent d'arriver à un consensus informatique. Certains algorithmes sont à l'étude comme la « *preuve d'enjeu* » (ou « *Proof-of-Stake* »), et d'autres sont relativement isolés en pratique tels que la preuve de capacité (ou « *Proof-of-Capacity* »), « *preuve de stockage* » (ou « *Proof-of-storage* ») ou encore la preuve de brûlure (ou « *Proof-of-Burn* »)[360].

[357] A. Takkal Bataille, J. Favier, Bitcoin. *La monnaie acéphale*, *op.cit.*, p.63.
[358] *Ibid*.
[359] Vocabulaire des activités postales (liste de termes, expressions et définitions adoptés), JORF n°0251 du 28 octobre 2011 p.18229 texte n°123, NOR: CTNX1125838K.
[360] J. Mattila, « The *Blockchain* Phenomenon – The Disruptive Potential of Distributed Consensus Architectures », Berkeley rountable on the international economie (BRIE) Working Paper 2016-1, Université de Berkeley, mai 2016, p.25.

1. Les incidences de l'algorithme de consensus de la « *preuve de travail* » sur les preuves *blockchains*

129. L'algorithme de la preuve de travail trouve ses origines dans les années 1990, développé par Adam Back qui décrivait ce type d'algorithme pour éliminer les pourriels[361]. Cet algorithme de la preuve de travail est celui employé pour la crypto-monnaie la plus usuelle : le bitcoin. Considéré comme la véritable pierre angulaire du protocole Bitcoin, il a pour objectif de développer une méthode de validation des blocs de transactions consistant pour un ensemble de mineurs à fournir une puissance de calcul importante afin de trouver une solution à un problème mathématique de plus en plus difficile. Dans l'hypothèse d'une grosse concentration de puissance de calcul détenue par des groupes de mineurs, le risque serait de dicter quelles transactions sont acceptées dans le registre et lesquelles ne le sont pas[362]. Si le principal but de cet algorithme est de s'accorder sur un consensus pour valider les blocs, il a aussi pour dessein de rendre impossible toute réécriture, même partielle, du registre de la *blockchain* par un nœud malhonnête. Cette réécriture est en théorie possible mais elle est quasiment hors de portée, étant trop complexe à réaliser[363].

130. L'algorithme « *Proof of Stake* » (ou « *preuve d'enjeu* ») tente de résoudre la problématique de la consommation électrique de la preuve de travail en supprimant entièrement le concept de minage pour le remplacer par un autre mécanisme. Il permettrait de développer une méthode de validation des blocs dont le principe est de reproduire le processus de minage issu de la preuve de travail en se basant, non plus sur la puissance de calcul, mais sur une mise de jetons[364]. La probabilité qu'un validateur soit sélectionné pour vérifier un bloc de transactions dépend de sa mise : plus sa mise est grande, plus la part d'actifs qu'il pourrait valider sera importante. L'hypothèse sous-jacente de ce mode de validation réside dans l'idée que le validateur détenant une part importante d'actifs du système est plus susceptible de fournir des informations fiables dans le cadre du processus de vérification[365]. Cet algorithme n'a, pour

[361] A. Back, « A Partial Hash Collision Based Postage Scheme », *op.cit.*
[362] P.Tasca, Claudio J. Tessone, « Taxonomy of Blockchain Technologies. Principles of Identification and Classification », mars 2018, p.11.
[363] Voir *supra* n°43.
[364] V. Buterin, « Proof of Stake FAQ», trad. par J. Zundel, S. Polrot et A. Masseron, https://www.ethereum-france.com/quest-ce-que-la-preuve-denjeu-proof-of-stake-faq-par-v-buterin-traduction-francaise/ (consulté le 31/05/2020).
[365] P.Tasca, Claudio J. Tessone, « Taxonomy of Blockchain Technologies. Principles of Identification and Classification », *op.cit.*, p.12-13.

l'heure, toujours pas été prouvé mathématiquement, ni ne semble être réellement mis en application[366]. Les développeurs du protocole Ethereum travaillent tout de même à son développement de façon à minimiser les conséquences énergétiques de la preuve de travail.

2. Les incidences de l'algorithme de consensus de la « *preuve d'autorité* » sur les preuves *blockchains*

131. La preuve d'autorité[367] permet de configurer un consensus pour la validation des blocs de transactions selon l'approbation des entités désignées à l'effectuer pour alors aboutir à la création de blocs selon des modalités définies[368]. Cette preuve d'autorité est d'usage pour organiser la gouvernance d'une *blockchain* privée et est adaptée aux réseaux centralisés[369]. Ce sont donc les membres désignés ou le gérant qui disposent du pouvoir de validation. Le registre *blockchain* est alors soumis à l'arbitraire du validateur dans ce cas. Même si des règles prévoient les conditions et modalités de validation, le registre n'aura de valeur qu'entre les membres de cette *blockchain*. Dès lors, le registre est exposé à des risques de modifications et effacements de données plus aisés. Le nombre limité de validateurs de blocs en fait toutefois une infrastructure de *blockchain* hautement scalable[370]. Les transactions approuvées par le ou les validateurs autorisés sont ensuite répertoriées dans le registre.

Paragraphe 2 : Essai de classification des procédés techniques formant les preuves *blockchains*

132. Constituent des preuves *blockchains*, les « *procédés techniques blockchains* » que sont la signature *blockchain* (A) qui répond à la question de savoir qui a effectué une transaction dans la *blockchain*, l'horodatage *blockchain* (B) répondant à la question quand a été effectuée

[366] Contrairement à la preuve d'enjeu, la preuve de travail qui a été prouvée mathématiquement et *« permet de se prémunir de façon sûre des attaques sybil, c'est-à-dire de la multiplication de nœuds détenus par un seul utilisateur pour dominer le réseau. Cette protection par la preuve de travail existait déjà pour lutter contre les pourriels, entre autres »* (R. Perez Marco, « Ricardo Perez-Marco : "95 % des monnaies créées aujourd'hui vont disparaître" », bitcoin.fr, juill. 2018, https://bitcoin.fr/ricardo-perez-marco-95-des-monnaies-creees-aujourdhui-vont-disparaitre/ (consulté le 31/05/2020)).

[367] Le terme de la preuve d'autorité aurait été proposé par Gavin Wood pour la première fois en 2017 par l'ancien directeur technique et cofondateur d'Ethereum.

[368] Cambridge Centre for Alternative Finance, University of Cambridge Judge Business School, Global blockchain benchmarking study, *op.cit.*, p.17.

[369] OPECST, Les enjeux technologiques des *blockchains* (chaînes de blocs), *op.cit.*, p.41.

[370] France Stratégie, Rapport, Les enjeux des *blockchains*, *op.cit.*, p.21-22.

une transaction dans la *blockchain*, et l'empreinte *blockchain* (C) consistant à répondre à l'interrogation de savoir si les données d'une transaction n'ont pas été modifiées.

A. La signature *blockchain*

133. La signature *blockchain* prend appui sur la cryptographie asymétrique décrite ci-avant, usant du couple clé publique et clé privée[371]. La clé publique est une adresse *blockchain,* soit une chaîne de caractères (chiffres et lettres) qu'il est possible, d'une part, de communiquer à un individu pour recevoir des crypto-actifs, et de l'autre, qui permet d'envoyer des crypto-actifs en signant une transaction[372]. Ceci est un exemple de clé publique sur Bitcoin : « 1FGAftzSTztFSB8LMwsrdCKTyqGY6zr3sU ». Dans certaines *blockchains,* une nouvelle clé publique est générée à chaque transaction et sans limite de fréquence. La clé privée est une forme de mot de passe qui doit rester secret afin de garder ses fonds sous contrôle. Elle doit aussi être conservée dans la mesure où si elle est égarée, il sera impossible de la régénérer et les fonds afférents seront perdus[373]. La signature *blockchain* poursuit dès lors deux objectifs : assurer que l'émetteur est le seul à pouvoir signer sa transaction tout en permettant à toute personne de la vérifier et de la lier à une transaction en particulier[374].

134. C'est pour l'heure l'algorithme ECDSA (*Elliptic Curve Digital Signature Algorithm*) qui est utilisé, en particulier par le protocole Bitcoin[375]. Schnorr est un autre algorithme de signature à l'étude plus simple et plus résistant qu'ECDSA[376]. Dans le contexte du problème de résistance des algorithmes, le risque est qu'une transaction soit interceptée par un individu malveillant ayant récupéré la signature d'un émetteur, pour ensuite transférer des crypto-actifs à partir du compte de cet émetteur initial. La raison pour laquelle Schnorr n'a pas été implémenté dans Bitcoin est simple : Schnorr était protégée par un brevet américain délivré en

---

[371] Voir *supra* n°117-121.
[372] Conférence, *Blockchain* Protocol Analysis and Security Engineering 2018, intervention de P.Wuille « Schnorr signatures for Bitcoin: challenges and opportunities », Université de Stanford, 24-26 janv. 2018, https://cyber.stanford.edu/bpase18 (consulté le 31/05/2020).
[373] A. M. Antonopoulos, *Mastering Bitcoin : Unlocking Digital Cryptocurrencies*, *op.cit.*, p.63.
[374] E. Felten, Lecture 1 – Introduction to crypto and cryptocurrencies, Pinceton's Bitcoin Mooc, Princeton University, https://www.coursera.org/learn/cryptocurrency (consulté le 31/05/2020).
[375] J. W. Bos, J. A. Halderman, N. Heninger, J. Moore, M. Naehrig, E. Wustrow, « Elliptic Curve Cryptography in Practice », 2013 ; D. R. L. Brown, « Standards for efficient cryptography. SEC 1: Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV) », version 2, 21 mai 2009.
[376] Voir plus en détail l'application des signatures Schnorr dans Bitcoin : Séminaire de « Cryptofinance » organisé par R. Pérez-Marco et C. Grunspan, intervention de Y. Seurin « Les signatures de Schnorr et de leurs applications dans Bitcoin », 14 mars 2018.

1991 et expiré en 2008[377]. Il n'existait pas de standard qui aurait permis aux développeurs du protocole Bitcoin d'implémenter Schnorr. C'est pourquoi ce brevet a poussé les pratiques à adopter ECDSA comme standard en dépit de son infériorité[378]. Les signatures ECDSA prennent effectivement beaucoup de place, elles sont lentes à la validation et ne sont pas optimales pour les transactions incluant des *smart contracts*. Alors que les signatures Shnorr sont plus légères, plus rapides et permettent d'agréger plusieurs signatures accordant plus de garantie de confidentialité des transactions et de possibilités pour les *smart contracts* avec la *blockchain* Bitcoin[379]. La vulnérabilité des *blockchains* publiques actuelles se situe donc en partie dans leur signature *blockchain*.

B. Les horodatages *blockchains*

135. La datation dans la *blockchain* implique deux éléments de temporalité. La date et l'heure de l'entrée de la transaction avant sa validation et la date et l'heure de la validation des blocs de transactions. Dans la blockchain Bitcoin, chaque bloc contient un horodatage Unix[380]. Ces deux temps apparaissent mais sont décalés, ceci est dû, notamment, au temps de validation des blocs de transactions de la *blockchain* en cause. L'horodatage apparaîtra dans la *blockchain* selon le format année:mois:jour et heure:minute:seconde. Par exemple, 2019-09-06 15:27:1. Il permettra de suivre de manière aisée l'ordre chronologique des opérations, soit la validation de chaque bloc liés les uns aux autres admis dans le registre[381]. Les propriétés de sécurité imposent que l'horodatage d'un bloc ne puisse pas être changé[382]. Par exemple, la base de la solution proposée par le protocole Bitcoin est de constituer un serveur d'horodatage distribué comprenant l'empreinte d'un ensemble de données horodatées[383]. Grâce à cette empreinte et son horodatage, il est prouvé que les transactions en bitcoins ont existées à un moment donné dans un ordre précis[384].

---

[377] US 4,995,082.
[378] Voir l'avis du NIST (National Institute of Standards and Technology) sur les risques de l'algorithme Shor's (ordinateurs quantiques) sur la signature ECDSA et ainsi sa vulnérabilité : D. Moody, « NIST status update on Elliptic Curves and Post-Quantum Crypto », mars 2019, p.11.
[379] Entretien de Y. Seurin, « signatures de schnorr et scalabilité », https://bitcoin.fr/signatures-de-schnorr-et-scalabilite/ (consulté le 31/05/2020).
[380] A. M. Antonopoulos, *Mastering Bitcoin : Unlocking Digital Cryptocurrencies*, *op.cit.*, p.113, 114, 192.
[381] OPECST, Rapport, Les enjeux technologiques des *blockchains* (chaînes de blocs), *op.cit.*, p.26.
[382] A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder, *Bitcoin and Cryptocurrency Technologies*, *op. cit.*, p.15.
[383] S. Nakamoto, « Bitcoin : A Peer-to-Peer Electronic Cash System », *op.cit.*, p.3.
[384] *Ibid.*, p.1.

C. Les empreintes *blockchains*

136. Les algorithmes SHA256 et SHA3 des fonctions de hachage sont les plus utilisés pour calculer les empreintes numériques au sein des *blockchains*. Alors que SHA3 est utilisé pour le protocole Ethereum, l'algorithme SHA256 est, quant à lui, utilisé dans le protocole Bitcoin. Les prochains développements seront axés sur cet algorithme puisqu'il constitue un algorithme de base pour la *blockchain*[385]. SHA256 est un algorithme développant une méthode de hachage qui génère une empreinte numérique sur 256 bits, soit 64 caractères en notation hexadécimale complète. Cette fonction exprime les 2256 combinaisons possibles (1,16 x 1077)[386]. Elle exprime un risque de collision quasi-absent[387]. D'une manière générale, le calcul d'empreintes *via* cet algorithme est vivement recommandé par les chercheurs[388] et est considéré par la CNIL comme fiable, tout comme SHA-512[389].

137. Les différentes empreintes que nous pouvons retrouver dans la *blockchain* sont nombreuses. Il existe dans la *blockchain* des empreintes numériques de blocs, de transactions, de clés publiques, un ensemble d'empreintes issues de l'arbre de Merkle[390], ou encore des empreintes de données complémentaires ajoutées dans une transaction. Précisément :

- Dans l'en-tête de chaque bloc sera présente, une empreinte numérique condensée de l'ensemble des transactions du bloc ou autrement appelé « *racine* » de Merkle. La modification d'une transaction dans le bloc modifie cette racine.

- À chaque transaction est rattachée une empreinte correspondante que l'on appelle « *identifiant de transaction* » ou « *txid* »[391].

---

[385] Campbell R. Harvey, Cryptotransactions, Duke University Courses, janv. 2019, p.48-52.
[386] R. Baron, « Introduction aux technologies *blockchain* supports des crypto-monnaies », *op.cit.*, p.37.
[387] A. Takkal Bataille, J. Favier, Bitcoin. La monnaie acéphale, *CNRS Editions*, 2017, p.93.
[388] Séminaire IRT SystemX, D. Augot, fonction de hachage et *blockchain*, *op.cit.*
[389] https://www.cnil.fr/fr/securite-chiffrer-garantir-lintegrite-ou-signer (consulté le 31/05/2020).
[390] L'« *arbre de Merkle* » ou « *arbre de hachage* » est une structure contenant un résumé d'information d'un volume de données. Dans la *blockchain* l'arbre de hachage permet d'organiser plusieurs transactions d'un bloc en les structurant. Les arbres de hachages sont créés par Ralph Merkle en 1979 (R. C. Merkle, *Secrecy, authentication, and public-key systems*, these, Université de Stanford, 1979 ; R. C. Merkle, « Protocols for public key cryptosystems », In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, avr. 1980, p.122-133 ; R. C. Merkle, « A Digital Signature Based on a Conventional Encryption Function » *in* Advances in Cryptology - CRYPTO '87, Lecture Notes in Computer Science book series, LNCS, volume 293, 1987, p.369-978).
[391] A. M. Antonopoulos, *Mastering Bitcoin : Unlocking Digital Cryptocurrencies*, *op.cit.*, p.46.

- Une clé publique[392] est issue d'une fonction de hachage pour la création d'une adresse publique constituée de suite de chiffres alphanumériques[393].

- Outre les empreintes existantes précitées, l'empreinte de données spécifiques peut être calculée par une personne. Il arrive que l'empreinte de l'empreinte (ou « *hash de hash* ») soit ancrée dans une transaction pour permettre de regrouper tous les documents ou fichiers pour lesquels une empreinte a été calculée et réduire le coût d'ancrage à une seule transaction. Pour vérifier que ces données ancrées sont intègres, il convient de procéder une nouvelle fois au calcul de l'empreinte, laquelle devrait donner un résultat identique au premier calcul si les données n'ont pas été modifiées.

De tous ces protocoles sous-jacents et procédés corrélatifs naissent des types de preuves que nous pourrons classer pour une démonstration éclairée de l'étude (chapitre 2).

[392] *Ibid.*, p.64.
[393] J.-L. Parouty, Bitcoin. « Éléments de compréhension technique », CNRS-IBS, 2016, p.5, https://docplayer.fr/18552351-Bitcoin-elements-de-comprehension-technique.html (consulté le 31/05/2020).

CHAPITRE 2

LA CLASSOLOGIE DES PREUVES *BLOCKCHAINS*

138. Se pose à l'évidence, en amont de l'étude des incidences des preuves *blockchains* sur le droit de la preuve, la question de savoir sur quoi portent concrètement ces preuves *blockchains*. Celle-ci pourra trouver une réponse dans la présentation de l'objet de ces preuves *blockchains* (section 1) que nous tenterons ensuite d'organiser afin de les classifier (section 2).

Section 1 : L'objet des preuves *blockchains*

139. Un certain nombre de données peuvent apparaître dans le registre de la *blockchain*, lesquelles pourront constituer de manière pragmatique l'objet de preuves. Nous présenterons les données selon une approche ciblée sur l'apparence des données qui ressortent du registre de la *blockchain* (paragraphe 1), pour ensuite les aborder sous l'angle du résultat des données issues des procédés techniques de la *blockchain* (paragraphe 2).

Paragraphe 1 : Les données selon leurs modalités d'apparition

140. Dans le registre d'une *blockchain* (publique) seule l'existence d'une transaction peut être visible en principe, mais l'identité des émetteurs et destinataires et le but de la transaction sont inconnus. L'essentiel des données sont chiffrées ou hachées. Des données additionnelles peuvent être affichées exceptionnellement en clair. L'ensemble de ces données, objets de preuve, qui apparaissent de manière hachée découlant du calcul d'une empreinte numérique préalable (A) ou en clair (B) seront examinées (les données chiffrées renverront, elles, aux développements sur les données signées).

A. Les données ne figurant pas en clair dans la *blockchain* : les données hachées

141. Certaines données ne figurent pas en clair dans le registre d'une *blockchain* parce qu'elles ont été hachées en amont. À ce titre, ces données hachées apparaissent sous la forme d'empreintes numériques de données[394]. Il existe pour cette raison différentes strates de données hachées ou hash de données ou empreintes comme développées ci-avant[395].

142. Le hash de bloc ou l'empreinte permet d'horodater chaque bloc de transactions, qui traduit ensuite une chaine d'empreinte continue constituant une preuve d'existence des blocs dans un certain ordre. La modification du contenu d'un bloc étant traduite par une empreinte différente, l'empreinte du hash d'un bloc précédent modifié, engendrera un recalcul nécessaire de tous les hashs des blocs qui suivent. Les modifications seront donc visibles.

143. Ensuite, l'empreinte ou hash d'une transaction rattachée à chaque transaction constitue une preuve de celle-ci par son identifiant de transaction. Ce hachage de données du bloc permet ainsi de prévenir toutes modifications de données entrées dans le registre *blockchain*. Puis, l'empreinte ou hash d'une adresse publique est la conversion de la clé publique en un hash de 160 bits et ne présente pas d'intérêts particuliers pour la preuve.

144. Enfin, l'empreinte ou le hash de données complémentaires permet pour une personne ayant intérêt à prouver l'intégrité de données de se préconstituer une preuve de celles-ci. Tel que mentionné ci-avant, il est possible d'obtenir une garantie de l'intégrité de ces données hachées grâce au calcul du même ensemble de données[396]. Le participant émetteur qui intègre dans une transaction des données hachées prouve, en somme, leur existence à un moment donné et l'absence de modifications ultérieures qui seraient détectées. 60% des participants à une étude de l'Université de Cambridge déclaraient que dans leur pratique de hachage de données ancrées, seules les empreintes pointant vers les données étaient stockées dans la *blockchain*[397]. À ce titre, un nombre de plus en plus croissant de fournisseurs de logiciels et de fournisseurs de services

[394] Voir *supra* n°122-127.
[395] Voir *supra* n°137.
[396] Voir *supra* n°127.
[397] Cambridge Centre for Alternative Finance, University of Cambridge Judge Business School, Global blockchain benchmarking study, *op.cit.*, p.51.

blockchains offrent un soutien à l'intégration pour ce stockage de données en dehors de la *blockchain* ou appelé le stockage « *off-chain* ».

B. Les données figurant en clair dans la *blockchain* : les dates de transactions et certaines données ajoutées

145. Les dates de transactions apparaissent dans le registre de la *blockchain* en clair dans l'ordre chronologique de la plus ancienne à la plus récente[398]. De plus, des données ajoutées par un participant dans une transaction de la *blockchain* pour les sécuriser peuvent aussi figurer en clair. Cependant, le protocole Bitcoin par exemple n'a pas comme objectif initial de recevoir des données ajoutées en clair. L'usage du stockage de données en clair est à éviter selon les développeurs en ce qu' « *il est moins coûteux et beaucoup plus efficace de stocker des données non monétaires ailleurs* »[399]. La quantité de données stockées en clair est limitée dans la *blockchain* publique, d'où le fait que des empreintes de ces données soient devenues une solution de substitution[400]. Pour le reste, une tendance à la réduction des données stockées dans la *blockchain* est observée. Seulement 30% des personnes répondant à une étude de l'Université de Cambridge stockent la totalité des données[401].

Paragraphe 2 : Les données selon leurs résultats issus des procédés techniques *blockchains*

146. Les procédés techniques issus de la *blockchain* ont pour résultats de fournir des données signées (A), des données datées (B), ainsi que des données hachées mentionnées ci-avant, constituant des preuves *blockchains*.

[398] Voir *supra* n°39-40.
[399] https://bitcoin.org/en/release/v0.9.0#rebranding-to-bitcoin-core (consulté le 31/05/2020).
[400] Voir *infra* n°100 sur la limite de données dans une transaction bitcoin.
[401] Cambridge Centre for Alternative Finance, University of Cambridge Judge Business School, Global blockchain benchmarking study, *op.cit.*, p.54-55.

A. Les données signées

147. Les données qui font l'objet d'une signature *blockchain* sont les transactions réalisées par un/des participant(s) émetteurs. La donnée porte la signature, adresse publique dudit participant permettant dès lors de l'authentifier. Il s'agit, autrement dit, pour l'émetteur d'une transaction de s'assurer que l'origine de la transaction portera son identité. Les données concernant cette identité ne sont pas relevées dans les *blockchains* publiques grâce à la technique de cryptographie asymétrique développée ci-avant. En revanche, il est considéré que ces données ne sont pas anonymes mais « *pseudonymes* »[402]. Les données signées cryptographiquement sont transmises de l'émetteur au destinataire de manière fiable par le biais de la *blockchain*.

B. Les données datées

148. Les données faisant l'objet d'un horodatage sont les transactions et les blocs de transactions. Ces dernières comportent l'année, le mois, le jour et l'heure, les minutes et secondes de leurs datations qui intéressent la chronologie du registre de la *blockchain*[403]. Ces données permettent aux participants d'apporter la preuve du moment de l'opération de transaction et de son entrée dans le registre. Les accédants peuvent prouver la date et l'heure d'une opération dont ils ne seraient pas à l'origine. Les validateurs prouvent leurs interventions à un moment précis dans la validation et la création d'un bloc de transactions ajouté au registre.

Section 2 : Essai de classification des données formant les preuves *blockchains*

149. Une méthode de classification des preuves *blockchains* doit permettre une représentation hiérarchique des concepts de ces preuves. Nous présenterons la première taxonomie de la preuve *blockchain* selon une classification par nature (paragraphe 1) et par provenance (paragraphe 2) de ces preuves de données dans la *blockchain*.

[402] Voir *infra* n°299 et s. les développements sur le pseudonymat.
[403] Voir *supra* n°135.

Paragraphe 1 : La classification par nature de données dans la *blockchain*

150. Les données présentent dans la *blockchain* peuvent être classifiées compte tenu de leur nature selon qu'elles constituent des données transactionnelles, « *sur* » une transaction (A), ou des données complémentaires, ajoutée « *dans* » une transaction (B).

A. Les données transactionnelles

151. Les données transactionnelles, comme leur nom l'indique, sont toutes les données relatives à la transaction. Ce sont des informations produites par la *blockchain* à partir des transactions, enregistrées dans le registre de façon homogène, ordonnée, et lisible par tout accédant dans une *blockchain* publique et seulement ceux autorisés dans une *blockchain* privée. Constituent ces données transactionnelles au sein des *blockchains* : les adresses publiques des participants à la transaction, les identifiants de transactions, les dates et heures des entrées de transactions, les dates et heures de validations des blocs.

B. Les données complémentaires

152. Les données complémentaires sont toutes les informations qui sont ajoutées dans une transaction réalisée avec la technologie *blockchain* par un participant. La place dans une transaction est limitée selon la nature et le protocole de la *blockchain*[404]. Ces données complémentaires peuvent être hachées ou en clair[405]. Cette terminologie de « *données complémentaires* » que nous déciderons d'employer pour cette étude est dégagée par la CNIL dans ses premiers éléments d'analyse du 24 septembre 2018 pour indiquer la présence et le stockage éventuel de données à caractère personnel au sein de ces données[406]. Cette analyse évoque l'existence possible de deux catégories de données personnelles : les identifiants des participants et mineurs (soit les clés publiques) et les données complémentaires. Elle indique que ces données complémentaires sont des données inscrites « *dans* » une transaction. En mars

[404] Voir *supra* n°100 pour la blockchain Bitcoin.
[405] Voir *supra* n°141-145.
[406] CNIL, *Blockchain.* Premiers éléments d'analyse, 24 sept. 2018, p.7.

2018, 1,4 % des 251 millions de transactions dans la *blockchain* Bitcoin contenaient des données complémentaires[407].

Paragraphe 2 : La classification par provenance des données dans la *blockchain*

153. Les données dans la *blockchain* peuvent être classifiées selon leurs provenances, à savoir si elles sont, grâce à des acteurs de la preuve *blockchain*, ajoutées par un sujet de droit (A) ou générées par la *blockchain* (B).

A. Les données volontaires ajoutées par le sujet de droit

154. Les données ajoutées volontairement par un sujet de droit correspondent à des données complémentaires ajoutées dans une transaction de la *blockchain*. Dans le vocable informatique, ces données complémentaires sont parfois désignées de « *données arbitraires* »[408] mais elles sont en réalité des « *données volontaires* » dans la terminologie juridique dans la mesure où elles sont inscrites par la volonté individuelle d'un participant. Les données complémentaires pourraient ainsi être qualifiées de « *données volontaires* » dès lors que des données en clair ou hachées sont ajoutées dans une transaction volontairement par un sujet de droit. Notons cependant qu'au côté de ces « *données volontaires directes* » ajoutées par un geste extérieur d'un individu, il serait possible d'admettre des « *données volontaires indirectes* ». Elles correspondraient à celles issues d'une volonté de réaliser une transaction - puisque sans la volonté de l'émetteur elle n'aurait pas pu apparaître dans le registre - mais pour lesquelles seules la *blockchain* générerait les données afférentes à cette transaction dans le registre (voir ci-après les données générées par la *blockchain*).

155. Les sujets de droits qui interagissent avec l'objet de ces preuves *blockchains* sont qualifiés de « *participants à la preuve blockchain* » c'est-à-dire qu'ils participent à la création effective d'une preuve *blockchain* par l'entrées de données dans le registre grâce à un agissement externe à la technologie elle-même (soit directement par l'ajout de données

[407] R. Matzutt, J. Hiller, M. Henze, J.-H. Ziegeldorf, « A Quantitative Analysis of the Impact of Arbitrary *Blockchain* Content on Bitcoin », *op.cit.*, fevr. 2018, p.15.
[408] *Ibid*., p.1 et s.

complémentaires ou indirectement par la seule réalisation d'une transaction). Ce participant à la preuve, émetteur de la transaction, a un intérêt particulier à générer cette preuve : il se sert de ces éléments au soutien de ses prétentions. Les « *accédants à la preuve blockchain* » de données dans la *blockchain* ajoutées par le « *participant à la preuve* », sont toutes personnes souhaitant accéder au registre puisque ces données pourraient présenter un intérêt probatoire pour elles. Dans une *blockchain* publique, les données ajoutées par le sujet de droit peuvent être lues par tous les accédants. Ces données sont stockées dans une transaction de manière immuable et elles sont librement accessibles dans les *blockchains*. Cependant, seules les données en clair ajoutées seront lisibles par ces accédants à la preuve. Lorsqu'elles ne le sont pas, elles sont sous forme d'empreinte numérique et seul celui ayant calculé l'empreinte peut connaître les données initiales. Dès lors, l'empreinte numérique de données ajoutée pourra être vérifiée uniquement par les participants à la preuve disposant de l'ensemble de données initiales non hachées. Ces précisions, dans une *blockchain* privée ou publique permissionnée, s'appliquent uniquement aux membres autorisés à lire le registre, à le consulter.

B. Les données générées par la *blockchain*

156. Les données générées par la *blockchain* sont des informations produites mécaniquement, regroupées et stockées dans le registre *blockchain*, dont l'ensemble des procédés et validateurs participent à la production. Les « *validateurs à la preuve blockchain* » sont les validateurs de la transaction[409]. En fournissant une puissance de calcul et validant les transactions, ils garantissent ainsi une légitimité informatique aux preuves *blockchains*. Ces données générées sont ensuite stockées dans ce registre de manière immuable. Elles recouvrent uniquement les données transactionnelles précitées (les adresses publiques des participants à la transaction, l'identifiant de transaction, la date et l'heure de l'entrée de la transaction, la date et l'heure de la validation du bloc). Ces données générées par la *blockchain* sont accessibles à tous les accédants à la preuve pour les *blockchains* publiques, ou uniquement à des membres autorisés à les consulter pour les *blockchains* privées. L'accédant à la preuve *blockchain* peut aussi être un participant à la preuve. Dans l'hypothèse d'un contentieux, il pourrait être admis que les parties et le juge ou encore des tiers puissent être accédants[410].

[409] Voir *infra* n°7 en introduction.
[410] Ceci correspondrait à la possibilité d'accéder à une preuve pour un tiers dans l'hypothèse d'un contrat conclu par la *blockchain* comme l'inscription d'émission et de cession de minibons. Voir *supra* n°424 et s.

Paragraphe 3 : Les classifications par modalités d'ajout de données dans la *blockchain*

157. Cette classification de données qui se chevauchent est présentée en fonction des modalités d'ajout des données dans la *blockchain* de la plus restrictive à la plus large : des données ancrées (A), au données inscrites (B), jusqu'aux données enregistrées (C).

A. Les données ancrées dans la *blockchain*

158. Les données ancrées sont celles pour lesquelles une empreinte numérique a été calculée, laquelle a été ajoutée dans une transaction. Cette opération d'ancrage ne vise que les données complémentaires hachées. Celui qui effectue une opération d'ancrage de donnée est nommé l'« *ancreur* » et celui-ci est inclut dans la catégorie des participants à la preuve *blockchain*. Il participe en effet à la création effective et directe d'une preuve *blockchain* par l'ancrage de données. C'est un sujet de droit personne physique ou morale qui a volontairement ajouté dans une transaction une empreinte numérique d'un ensemble de données. Il peut être représenté par un prestataire de services intermédiaire facilitant l'interface entre un usager non initié à la cryptographie et la *blockchain*. Par exemple, pourrait avoir un intérêt à ancrer, l'ancreur qui souhaite certifier une information relative à l'identité de personnes physiques ou morales, des documents divers, des œuvres de l'esprit pour prouver l'antériorité d'un droit d'auteur, des cahiers de laboratoire, des codes source d'un logiciel, des savoir-faire, ou encore la possession personnelle antérieure pour la période de l'avant brevet.

B. Les données inscrites dans la *blockchain*

159. Les données inscrites sont celles ajoutées volontairement par l'émetteur à la transaction, incluant des données « *complémentaires* » en clair ou hachées (soit des données ancrées) et des jetons utilitaires et financiers (comme les inscriptions de minibons et de titres financiers non cotés, telles qu'envisagées par les ordonnances *blockchain* et minibons). L'inscription pourra avoir en effet pour objectif de refléter une opération déjà existante à l'extérieur de la *blockchain* comme la *tokenisation* qui reflète la souscription d'un actif mais aussi de constituer une opération indépendante dans la *blockchain*, comme une transaction en ethers traditionnelle.

L'« *inscriveur* » de données est inclut dans la catégorie des participants à la preuve *blockchain* ayant précisément un intérêt à inscrire une donnée dans la *blockchain*.

C. Les données enregistrées dans la *blockchain*

160. Les données enregistrées dans la *blockchain* regroupent toutes les données relatives à des opérations réalisées dans la *blockchain* de manière large. Elles sont relatives aux données qui sont mécaniquement enregistrées dans la *blockchain* mais aussi toutes les autres ajoutées. Elles regroupent donc les données « *transactionnelles* » et « *complémentaires* ». En détail, ces données vont regrouper les identifiants de transaction, les adresses publiques, le nombre de crypto-actifs échangés, les dates de transactions, les dates de blocs, ainsi que les données inscrites, et les données ancrées ci-avant développées. Concernant les crypto-actif échangés, la loi PACTE y fait référence en indiquant que cette représentation numérique de valeur, soit la crypto-monnaie est « *transférée, stockée ou échangée électroniquement* ». Les « *enregistreurs* » de données sont non seulement la technologie elle-même mais aussi les validateurs, les inscriveurs de données et les ancreurs de données.

TITRE 2

LES PREALABLES JURIDIQUES A L'ETUDE DU DROIT DE LA PREUVE A L'AUNE DE LA *BLOCKCHAIN*

161. Avant d'examiner plus en détail l'étude du « *droit de la preuve blockchain* », déterminer le droit applicable afin de pouvoir l'étudier est fondamental (chapitre 1). Aussi, des vérifications préliminaires doivent être menées systématiquement quant à l'admissibilité et la recevabilité des preuves *blockchains* en justice (chapitre 2).

CHAPITRE 1

LA DETERMINATION DU DROIT APPLICABLE AUX PREUVES *BLOCKCHAINS*

162. L'architecture décentralisée de la technologie *blockchain* se prête difficilement à la centralisation des systèmes juridiques. En ce sens, elle est irréductible à l'application de règles de droit uniquement nationales[411]. Ces architectures internationales peuvent seulement être appréhendées - bien que difficilement - par des règles de rattachement de droit international privé[412] pour tenter de déterminer un droit applicable aux preuves *blockchains* (section 1). Les parties elles-mêmes ont, pour le reste, tout le loisir d'anticiper une clause attributive de juridiction et de désigner la loi d'un État qui reconnait dans son droit positif les effets juridiques de la technologie *blockchain*[413]. Dans un contexte d'usage conséquent de cette technologie aux États-Unis et en Europe[414], les systèmes juridiques nord-américain et européen de la preuve électronique seront spécifiquement étudiés et comparés. Cette étude permettra de comprendre les spécificités respectives des deux droits de traditions différentes et de les mettre précisément en relief au regard du droit de la preuve *blockchain* au cours de l'étude (section 2).

[411] En ce sens de l'« *irréductibilité* » d'une application des règles de droit français : F. Jault-Seseke, « La blockchain au prisme du droit international privé, quelques remarques », Dalloz IP/IT n°10, oct. 2018 p.544.

[412] Voir les premières réflexions doctrinales à ce sujet : F. Jault-Seseke, « La blockchain au prisme du droit international privé, quelques remarques », *op.cit.*, p.544 et s. ; E. Treppoz, « Quelle régulation internationale pour la blockchain ? Code is law v. Law will become Code », *in La blockchain : big bang de la relation contractuelle*, Dalloz, coll. Thèmes et commentaires, 2019, p.55 et s. ; J.-S. Bergé, Colloque La circulation de l'information dans la blockchain : enjeux pour le droit international privé (organisé par l'Association « Lex »), 28 fév. 2019, https://www.droiteconomique.org/manifestation/la-circulation-de-linformation-dans-la-blockchain-enjeux-pour-le-droit-international-prive/ (consulté le 31/05/2020) ; T. Douville, « *Blockchains* et droit international privé : état sommaire des questions », RDIA n°2, 2019, p.384 et s.

[413] F. Jault-Seseke, « La blockchain au prisme du droit international privé, quelques remarques », *op.cit.*, p.546 ; M. Mekki, « Les mystères de la blockchain », D. n°37, 2 nov. 2017, p.2168, n°28. Voir aussi : les développements n°612-623 sur la convention de preuve.

[414] Pour illustration : voir, notamment, la concentration du nombre le plus important de nœuds de Bitcoin aux États Unis (1941 nœuds) en Allemande (1806 nœuds), en France (518 nœuds) et aux Pays Bas (427 nœuds) : https://bitnodes.earn.com/ (consulté le 31/05/2020).

Section 1 : Les règles de rattachement de droit international privé applicables aux preuves *blockchains*

163. Le caractère transnational de la *blockchain* implique fréquemment un élément d'extranéité nécessitant l'application des règles de rattachement dans l'hypothèse d'un conflit de lois. En l'absence de règles de conflit spécifiques aux preuves *blockchains*, les règles de rattachement générales ont bien vocation à s'appliquer, ce que confirme le rapport de l'Assemblée nationale dit « *De la Raudière/Mis* » du 12 décembre 2018 rendu dans le cadre d'une mission d'information commune sur les « *chaînes de blocs* »[415]. La preuve étant de nature double (procédurale et substantielle), une preuve *blockchain* relève en théorie de la loi du fond ou celle de la procédure[416]. La vision de la doctrine et les décisions jurisprudentielles précise en détail les lois applicables en fonction de l'administration (paragraphe 1), de l'objet et de la charge de la preuve *blockchain* (paragraphe 2). Même si le droit international privé s'est intéressé de près à la preuve, le droit applicable reste relativement incertain[417], ce qui n'épargne pas les preuves *blockchains*.

Paragraphe 1 : Les règles de rattachement s'agissant de l'administration d'une preuve *blockchain*

164. L'admissibilité et l'autorité des modes de preuve disposent d'un caractère procédural marqué, raison pour laquelle la *lex fori* trouve directement à s'appliquer (A). Il pourra cependant être envisagé alternativement la loi du lieu de l'acte (B) et celle applicable au fond d'un acte (C)[418].

---

[415] Assemblée nationale, Rapport d'information n°1501, *op.cit.*, p.88.

[416] Voir l'analyse de cette double nature de la loi applicable à la preuve développée par E. Fongaro, *La loi applicable à la preuve en droit international privé*, LGDJ, thèse ss. dir. B. Beignier, 2004, 368 p. Bien que d'autres indiquent que « *la matière des preuves semblent à première vue relever entièrement de la procédure : il s'agit, indépendamment de l'existence du droit, d'emporter la conviction du juge sur la survenance de certains faits. Mais la réflexion conduit à reconnaitre à la loi du fond et à la loi du lieu de l'acte juridique en cause en rôle étendu* ». Pour l'analyse uniquement procédurale de la preuve et donc relevant entièrement de la loi du for voir : P.Mayer, V. Heuzé, *Droit international privé*, 11. éd., Paris, LGDJ, coll. Domat droit privé, 2014, p.364, n°522.

[417] Voir les travaux de : T. H. Groud, « La preuve en droit international privé », revue internationale de droit comparé vol. n°53, oct.-dec. 2001, p.1005-1008 ; E. Fongaro, *La loi applicable à la preuve en droit international privé*, *op.cit.*, 368 p. ; P. Mayer, V. Heuzé, *Droit international privé*, *op.cit.*, n°522-528, p.364 et s. ; T. Vignal, *Droit international privé*, Sirey, coll. Sirey Université, 4e ed., 2017, 540 p.

[418] Pour Fabienne Jault-Seseke, il convient de privilégier ces règles de conflit de lois alternatives (F. Jault-Seseke « La *blockchain* au prisme du droit international privé, quelques remarques », *op.cit.*, p.547).

A. L'application manifeste de la *lex fori*

165. L'administration de la preuve relève, en principe, de la loi du for car elle touche le plus souvent à des questions liées aux aspects procéduraux du droit de la preuve[419]. Les cas où la *lex fori* s'appliquera quant à la question de l'admissibilité incluront ceux :

En matière de conditions matérielles de preuve c'est-à-dire les conditions selon lesquelles les éléments de preuves doivent être versés au débat (date et mode de communication, langue utilisée.)[420]. En l'occurrence la langue utilisée pourra soulever des difficultés d'application puisque les *blockchains* relèvent essentiellement du langage informatique pour ce qui est du code du protocole lui-même ou des *smart contracts*. Le reste des preuves apparaissent sous forme de suite alphanumériques (pour les données chiffrées et hachées). Seul à ce stade un rapport d'expert en français, si la loi du tribunal français est retenue, pourrait permettre d'expliciter ces preuves *blockchains*[421].

En matière d'écrit, il existe un débat entre l'application de la loi du for pour les actes d'état civil, entre autres, en ce qu'ils ont la force probante que leur accorde cette loi[422], ou la loi qui en régit la forme comme indiqué ci-après. Dans le cas où certaines preuves *blockchains* sont qualifiées d'écrits électroniques, il conviendra de vérifier au cas par cas, si la loi du for ou la loi qui en régit la forme trouve à s'appliquer.

En matière de fait, l'application à la fois de la loi du for gouvernant l'administration de la preuve, comme de la loi du fond apparaît couvrir cette situation[423]. Il sera à tout le moins observé que ces lois concordent la plupart du temps vers le régime de la liberté de la preuve[424].

---

[419] P. Mayer, V. Heuzé, *Droit international privé*, *op.cit.*, p.365, n°528 ; Y. Loussouarn, P. Bourel, P. de Vareilles-Sommières, *Droit international privé*, Dalloz, 10e ed., 2013, p.819, n°803 ; A. Aynès, X. Vuitton, *Droit de la preuve. Principes et mise en œuvre processuelle*, *op.cit.*, p.8.
[420] B. Audit, L. d'Auvout, *Droit international privé*, coll. Traités, LGDJ, sept. 2018, p.447, n°507.
[421] Voir *infra* n°784 et s.
[422] Cass. civ. 1ère, 14 juin 1983, arrêt dit « *Suhami* », Rev. crit. DIP 1984, 316, note B. Ancel ; Cass civ. 1ère, 1e nov. 1986 : Rev. crit. DIP 1987, 557, note Poisson-Drocourt ; Cass. civ 1ère, 29 nov. 1994 : Bull civ. 1994, I, n°349 : Rev. crit. DIP 1995, 543, note Droz.
[423] En France : Bordeaux, 27 août 1877, JDI 1878. 39 ; Cass. civ. 6 mars 1956, JCP 1956. II. 9549, note A. Weill ; Rev. crit. DIP 1956. 305, note Ph. Francescakis ; Lyon, 26 mars 1958, JDI 1960. 172 : ces jurisprudences érigent presque en « *règle de droit matériel* » le rattachement de la loi du fort dans l'hypothèse d'un conflit de loi en matière de fait juridique (E. Fongaro, *La loi applicable à la preuve en droit international privé*, *op.cit.*, p.191, n°339).
[424] D. Bureau, H. Muir Watt, *Droit international privé*, t. I, Partie générale, 4e ed., Puf, Thémos Droit, 2017, p.227, n°193.

Par exemple, si des ébauches de dessins ancrés dans la *blockchain* prouvent la création antérieure d'une peinture en France par un auteur avant un prétendu contrefacteur, il pourra être appliqué la loi française dans la mesure où elle est liée à la loi des tribunaux compétents, comme à la loi du fond, c'est-à-dire au Code de la propriété intellectuelle.

166. La force probante de l'acte touchant « *au plus près du fonctionnement de la justice* »[425], se voit aussi appliquer la loi du for. De jurisprudence constante, lorsqu'un tribunal français doit statuer sur une question de force probante d'un acte en France, il applique la loi française[426]. Par exemple, si une juridiction française doit se positionner sur la force juridique d'une transaction dans le registre de la *blockchain* Ethereum, il appliquera les règles françaises de preuve du Code civil. Remarquons cependant que la jurisprudence accepte l'application de la loi du lieu de conclusion de l'acte dans certains cas[427].

B. L'application envisageable de la loi applicable du lieu de l'acte

167. Cette deuxième solution de la loi applicable est une voie alternative envisagée dans l'hypothèse où des plaideurs qui se seraient conformés aux exigences locales se trouveraient ensuite dans l'impossibilité de faire valoir leurs droits du fait de la nationalité du juge saisi[428]. Les parties sont en effet censées avoir respecté cette loi auparavant pour lui conférer l'efficacité prévue[429]. Certaines décisions ont dès lors statué pour la loi applicable au lieu de la rédaction de l'acte afin de favoriser la preuve des actes juridiques et respecter la prévision des parties[430]. Cette solution a été consacrée dans un article 18.2 du règlement (CE) n°593/2008 sur la loi applicable aux obligations contractuelles dit « *Rome I* » qui prévoit que « *les actes juridiques peuvent être prouvés par tout mode de preuve admis soit par la loi du for, soit par l'une des lois*

[425] D. Bureau, H. Muir Watt, *Droit international privé*, *op.cit.*, n°195.
[426] Cass. civ. 1ère, 14 juin 1983, arrêt dit « *Suhami* », Rev. crit. DIP 1984, 316, note B. Ancel ; Cass civ. 1ère, 1e nov. 1986 : Rev. crit. DIP 1987, 557, note Poisson-Drocourt ; Cass. civ 1ère, 29 nov. 1994 : Bull civ. 1994, I, n°349 : Rev. crit. DIP 1995, 543, note Droz
[427] D. Bureau, H. Muir Watt, *Droit international privé*, *op.cit.*, n°195.
[428] A. Aynès, X. Vuitton, *Droit de la preuve. Principes et mise en œuvre processuelle*, *op.cit.*, p.7.
[429] Cass. civ. 1ère, 24 févr. 1959, arrêt dit « *Isaac* », Rev. crit. DIP 1959. 368, note Y. L. ; D. 1959. 485, note P.Malaurie ; Cass. civ., 23 févr. 1964, DP 1864. 1. 167 ; Cass. civ., 24 août 1880, DP 1880. 1. 447 ; Cass. civ. 1ère, 25 nov. 1981 : Rev. crit. DIP 1982, 701, note P.Ancel ; Cass. civ. 23 mai 1892, DP.1892. 1. 473, note Cohendy ; Cass. civ., 14 juin 1899, JDI 1899. 804 ; Cass. civ. 6 févr. 1905, S.1907. 1. 393, note E. Naquet ; Cass. civ. 12 mai 1926, JDI 1927. 452 ; Cass. civ. 1er fevr. 1944, JCP 1944. II. 2588, note. J.M. ; Cass. civ. 1ère, 5 janv. 1999, arrêt dit « *O.N. Ollanescu c/ N. Culacov* » : Rev. crit. DIP 1999, 293 note A. Huet.
[430] Voir : Rapport Giulano-Lagarde sur la convention de Rome relative à la loi applicable aux obligations contractuelles, JO des Communautés européennes, n°C282/1.

visées à l'article 11, selon laquelle l'acte est valable quant à la forme, pour autant que la preuve puisse être administrée selon ce mode devant la juridiction saisie ».

168. Force est d'admettre aussi que cette alternative est moins préjudiciable, si la loi du lieu de l'acte au sujet des modes de preuve recevables, est plus libérale que celle du juge saisi par exemple[431]. En revanche, elle occulterait la nature procédurale de la question posée pour certains[432]. Par exemple, en matière de *blockchain*, le lieu de la rédaction d'un acte préalablement établi sera possiblement identifié. Seule l'empreinte de cet acte, intégrée dans la *blockchain,* sera difficilement localisable. Le lieu du calcul de l'empreinte pourra être très difficile à détecter. Pour autant, l'emplacement des copies pourrait être estimé par l'intermédiaire de certains outils d'aide à la localisation des nœuds[433]. Si des localisations multiples sont possibles, elles ne permettent pas toutefois l'identification d'un seul point d'ancrage de localisation de l'acte.

A la différence de l'administration de la preuve, les problématiques tenant à l'objet de la preuve *blockchain* ont un aspect procédural moindre, elles touchent davantage au fond du droit.

C. La loi applicable au fond de l'acte

169. L'application de la loi du fond de l'acte en matière d'administration de la preuve *blockchain* est une solution aussi envisagée. L'article 3 du règlement (CE) n°593/2008 dit « *Rome I* » permet l'application de la loi applicable au fond de l'acte. Si une preuve *blockchain* porte sur un acte, les membres identifiés d'une *blockchain* pourront placer leurs relations sous l'égide d'une loi nationale qui admet le recours à la *blockchain,* reconnaissant les inscriptions, la signature et l'horodatage dans la *blockchain*.

170. En principe, dans une *blockchain* publique, les participants à la preuve, les validateurs, et les accédants à la preuve ne sont pas localisables ou difficilement et ne permettent pas un

[431] A. Aynès, X. Vuitton, *Droit de la preuve. Principes et mise en œuvre processuelle*, *op.cit.*, p.7.
[432] V., B. Ancel et H. Muir Watt, note sous Cass., 1ère civ., 28 juin 2005, et Com. 28 juin 2005, Rev. crit. DIP 2005 : « *Il ne s'agit pas de résoudre un conflit de lois relatif à la force probante d'un acte étranger, mais d'en déterminer la conformité aux conditions d'accueil posées par l'ordre juridique français* » ; F. Jault-Seseke, « La blockchain au prisme du droit international privé, quelques remarques », *op.cit.*, p.547.
[433] Voir des outils comme Bitnodes utilisant une méthodologie d'envoi de message pour localiser les nœuds de bitcoin. En revanche, les nœuds employant une ancienne version du protocole sont exclus de cette méthode (https://bitnodes.earn.com/ (consulté le 31/05/2020)).

rattachement aisé à une loi de fond de l'acte supposément favorable. Or, dans une *blockchain* privée ou publique permissionnée, cette règle trouve aisément une application car il est envisageable de prévoir une loi de ce type au fond de l'acte entre les membres de cette *blockchain*. Dans l'hypothèse où une future loi en France permettrait le recours à la *blockchain* en droit de la preuve (outre les minibons et titres financiers non cotés), les parties pourraient placer leurs relations sous ladite loi.

Paragraphe 2 : Les règles de rattachement s'agissant de l'objet et de la charge d'une preuve *blockchain*

171. L'objet de preuve n'est pas un instrument conçu par les systèmes juridiques nationaux, *a contrario* des actes notariés français établis par les notaires en France, par exemple. La *Lex causae* est applicable de façon principielle à l'objet des preuves *blockchains* (A) et la loi du contrat, voire la loi applicable en matière de responsabilité civile extracontractuelle ou de propriété intellectuelle, couvrent quant à elles, la charge de la preuve *blockchain* (B).

A. L'application de principe de la *lex causae* pour l'objet de la preuve

172. La détermination de l'objet de la preuve à trait étroitement à la substance, au fond du droit et relève ainsi de la *lex causae*[434]. C'est la loi applicable au fond du droit qui tend à s'appliquer, conformément à l'idée selon laquelle c'est elle qui détermine les conditions d'existence de ces éléments de preuve[435]. Par exemple, si l'objet relève d'une inscription d'un jeton financier dans une *blockchain* en Italie, la loi italienne sur l'horodatage sera applicable alors que si l'objet relève d'une entrée de transaction en bitcoins dans le registre de la *blockchain* Bitcoin dans l'État du Vermont, la loi américaine de l'État du Vermont trouvera à s'appliquer.

[434] F. Jault-Seseke, « La blockchain au prisme du droit international privé, quelques remarques », *op.cit*., p.547.
[435] Cass. civ., 25 mars 1948 : D. 1948, 357 ; JCP 1948, II, 4532, note Vasseur.

B. L'application de la *lex contractus* ou de la *lex loci protectionis* pour la charge de la preuve

173. La charge de la preuve, soit la détermination de la qualité du plaideur, c'est-à-dire celui qui porte le « *fardeau* » de la preuve sera soumis à la loi du contrat en vertu de l'article 18.1 du règlement (CE) n°593/2008 sur la loi applicable aux obligations contractuelles dit « *Rome I* » qui prévoit que **«** *la loi régissant l'obligation contractuelle en vertu du présent règlement s'applique dans la mesure où, en matière d'obligations contractuelles, elle établit des présomptions légales ou répartit la charge de la preuve* ». La problématique de la loi applicable en matière de charge de la preuve se pose essentiellement en matière de présomption. Par principe, les systèmes juridiques nationaux s'accordent en effet sur la charge de la preuve pesant sur le demandeur à l'action[436]. Une difficulté surviendrait dans l'hypothèse d'un conflit de loi interrogeant sur l'application ou non d'un régime de présomption spécifique pertinent établi dans une loi nationale d'un pays. La loi du contrat dans l'hypothèse de son existence trouverait à s'appliquer.

174. Aussi, en matière de responsabilité délictuelle, l'article 22.1 du règlement dit « *Rome II* » prévoit qu'à la présomption de preuve s'appliquera la loi régissant l'obligation non contractuelle. Par exemple, en matière de propriété intellectuelle, c'est la *lex loci protectionis*, soit la loi du pays de protection qui est applicable, ce qui correspond le plus souvent à la loi du for[437]. En revanche, la jurisprudence est confuse au sujet des œuvres numériques ou diffusées sur des réseaux numériques[438]. Ces œuvres sont justement celles pouvant faire l'objet d'une préconstitution de preuve par la technologie *blockchain*. Pour certains auteurs, il sera essentiel de trouver un point d'ancrage permettant l'application de la loi d'un pays qui offre une protection satisfaisante[439], mais la jurisprudence est encore incertaine, surtout pour ce qui est

[436] P.Mayer, V. Heuzé, *Droit international privé, op.cit.*, p.363, n°523 ; B. Audy, L. d'Avout, *Droit international privé, op.cit.*, n°504, p.445.
[437] Concernant le droit d'auteur : Cass. 1ère civ., 10 avr. 2013 : RIDA 2013, 361, obs. P.Sirinelli ; JCP 2013, 493 obs. A. Lucas-Schloetter ; *op.cit.*, 701, note E. Treppoz ; D. 2013. 2004, note T. Azzi ; Propr. intell. 2013, 306, obs. A. Lucas ; RTD com. 2013, 725, obs. F. Pollaud- Dulian. Concernant les droits voisins : Cass. 1ère civ., 19 juin 2013, n°2-18.032, Culture Press, RIDA 2013, 399, obs. P.Sirinelli ; D. 2013. 2004, note T. Azzi ; *op.cit.* 2014, 1059, obs. H. Gaudemet-Tallon et F. Jault-Seseke ; RTD com. 2013, 729, obs. F. Pollaud- Dulian ; Propr. intell. 2013, 406, obs. A. Lucas / Concernant le droit des artistes-interprètes : Cass. 1ère civ., 18 févr. 2015, n°11-11.054, Propr. intell. 2015, 302, obs. A. Lucas ; D. 2015, 487 ; *Ibid* . 1056, obs. H. Gaudemet-Tallon et F. Jault- Seseke.
[438] A. Lucas, *op.cit.*, n°39 et s.
[439] T. Azzi, *Recherche sur la loi applicable aux droits voisins du droit d'auteur en droit international privé*, thèse ss. dir. H. Gaudemet-Tallon, Paris 2, LGDJ, 2005, n°516 ; F. Jault-Seseke, « La blockchain au prisme du droit international privé, quelques remarques », *op.cit.*, p.548.

des atteintes commises au moyen d'internet[440]. Le point d'ancrage avec la *blockchain* porte bien son nom puisqu'en matière de propriété intellectuelle, l'empreinte d'une œuvre serait ancrée dans la *blockchain*. Cet ancrage peut difficilement être déterminé, seul l'identifiant de transaction pourrait donner une indication précise sur l'enchainement des transactions et la validation du bloc sur l'heure et la date. Or, aucune indication ne semble pouvoir être apportée sur le lieu de l'ancrage. Pour un auteur, il conviendrait de demander une application au regard de la localisation de la personne protégée, passant outre la localisation de l'atteinte, comme en matière de droit de la consommation ou de droit des données personnelles[441].

175. Grâce à la souplesse des règles de droit international privé, des pistes de solution peuvent être envisagées au sujet du droit applicable aux preuves *blockchains*, puisqu'au regard des évolutions législatives nationales, les preuves *blockchains* ne sont plus conçues comme des outils translégaux et, en conséquence, transjuridictionnels. Toutefois, il peut sembler vain en pratique de chercher une localisation et un droit applicable aux preuves *blockchains* associé à des *blockchains* publiques. La complexité tient au fait de trouver la localisation des acteurs et opérations dans la *blockchain* décentralisée, et ainsi transnationale. Pour l'heure, les conflits de loi ne doivent pas inquiéter à ce stade car les litiges passés relatifs à la *blockchain* n'ont pas encore soulevé de problématiques de lois applicables[442]. Ils pourront à terme susciter des questionnements mais nous pouvons présager que ces règles de droit international d'une certaine flexibilité pourront être à même de s'adapter aux preuves *blockchains*, au même titre, que pour le commerce électronique par exemple. Une fois la loi déterminée, la question des règles nationales les plus enclines à s'appliquer aux éléments de preuves de la *blockchain* interroge (section 2).

[440] Solution discutée dans le domaine des dessins et modèles : CJUE 27 sept. 2017, aff . C- 24/ 16 et C- 25/ 16, affaire dite « *Nintendo* », D. 2017, 1977 ; *op.cit.* 2018, 966, obs. S. Clavel et F. Jault- Seseke ; *Ibid* . 1566, obs. J.-C. Galloux et P.Kamina ; Dalloz IP/ IT 2018, 190, obs. A.- E. Kahn ; Propr. ind. 2018, Comm. 23, obs. J.-P.Gasnier ; CCE 2018. Chron. 1, obs. M.- E. Ancel.
[441] F. Jault-Seseke, « La blockchain au prisme du droit international privé, quelques remarques », *op.cit.*, p.548.
[442] E. Treppoz, « Quelle régulation internationale pour la *blockchain* ? Code is law v. Law will become Code » *in La blockchain : big bang de la relation contractuelle*, Dalloz, coll. Thèmes et commentaires, p.55 et s.

Section 2 : Étude comparée des systèmes juridiques européen et nord-américain de la preuve électronique

176. Pour analyser les deux systèmes de la preuve électronique européen et nord-américain, nous emprunterons à cette fin une approche de droit comparé de façon à dégager les concordances conceptuelles (paragraphe 1) et les différences structurelles (paragraphe 2), susceptibles d'avoir un impact significatif sur les différents angles de l'étude du droit de la preuve au regard de la *blockchain*. Les différences géographiques en matière de reconnaissance juridique des preuves *blockchains* n'en ressortiront qu'avec plus de saillance.

Paragraphe 1 : Les concordances substantielles entre les droits européen et nord-américain de la preuve électronique

177. En substance, les concordances entre les droits européen et nord-américain de la preuve se situent au niveau de la reconnaissance juridique et de la recevabilité en justice de l'écrit électronique (A) et de la signature électronique (B).

A. L'admissibilité et la recevabilité en justice de l'écrit électronique

178. Au sein de l'hexagone, un document électronique est admis en droit. Le Code civil prévoit que « *l'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité* »[443]. Son effet et sa recevabilité en justice ne peuvent être refusés au seul motif que ce document se présente sous une forme électronique, selon l'article 46 du règlement eIDAS.

179. Aux États-Unis, une loi d'état l'*Uniform Electronic Transactions Act* dit « *UETA Act* » de 1999[444] est adoptée par la commission d'uniformisation des droits étatiques américains (ou *National Conference of Commissioners on Uniform State Laws*) dont le champ d'application est reconnu par l'*Electronic Signatures in Global National Commerce Act* du 30 juin 2000 dit

[443] C. civ., art.1366.
[444] National Conference of Commissioners on Uniform State Laws, Uniform Electronic Transactions Act, 1999.

« *E-Sign Act* », une loi fédérale entrée en vigueur le 1er octobre 2000 (dans la majorité de ses dispositions). C'est dans un souci de cohérence entre les différentes lois étatiques aux États-Unis que cette dernière règlementation prévoit des règles relatives aux signatures électroniques et la sécurité numérique[445]. L'*UETA Act* dégage un principe spécifique de non-discrimination pour les registres qui ne peuvent se voir refuser d'effets juridiques ou de force exécutoire du seul fait qu'ils soient sous formes électroniques[446]. Il en va de même pour les contrats formés par l'utilisation de registres électroniques[447]. L'*E-sign Act* confirme qu'un contrat ou tout autre document relatif à une transaction ne peut se voir refuser d'effets juridiques, une validité ou un caractère exécutoire du seul fait qu'il soit sous forme électronique[448]. L'*UETA Act* ajoute que si une loi exige qu'un document soit établi par écrit, un document électronique satisfait aux conditions de la loi[449].

180. Le règlement eIDAS reconnait les documents électroniques comme recevables en justice[450]. L'*UETA Act* prévoit également que dans une procédure, une preuve d'un document ne peut être exclue du seul fait qu'elle est sous forme électronique[451].

181. Pour conclure, l'écrit sur support électronique est admis juridiquement et ne peut pas être un motif de refus en justice tant aux États-Unis, qu'en Europe. La loi type sur le commerce électronique de la CNUDCI entérine ces règles en accordant qui plus est une parfaite équivalence entre l'écrit électronique et tout autre écrit au sein des pays membres des Nations unies si « *l'information qu'il contient est accessible pour être consultée ultérieurement* »[452]. Les règles sont semblablement similaires pour la signature électronique de document.

B. L'admissibilité et la recevabilité en justice de la signature électronique

182. La signature électronique fait l'objet d'un même régime que l'écrit électronique. Au regard de l'article 25 et du considérant 39 du règlement eIDAS, l'effet juridique d'une signature

[445] Electronic Signatures in Global and National Commerce Act, Pub. L. No. 106-229, 114 Stat. 464, june 30, 2000.
[446] UETA Act, section 7 (a).
[447] UETA Act, section 7 (b) ; E-Sign Act, section 101 (a) (2).
[448] E-Sign Act, section 101 (a) (1).
[449] UETA Act, section 7 (c).
[450] Règl. eIDAS, art. 46
[451] UETA Act, section 13.
[452] Loi type CNUDCI sur le commerce électronique, 2001, art. 6, al. 1.

électronique ne peut être refusé au seul motif que cette signature se présente sous une forme électronique et, qu'elle doit être équivalente à celle d'une signature manuscrite. L'alinéa 2 de l'article 1367 reconnaît la signature électronique qui « *consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie (…)* ». L'*E-sign Act* et l'*UETA Act* quant à eux exposent qu'une signature ne peut se voir refuser d'effets juridiques ou un caractère exécutoire du seul fait qu'elle soit sous forme électronique[453]. L'*E-sign Act* prévoit en plus que la validité de la signature électronique ne peut pas non plus être refusée.

183. En Europe comme aux États-Unis, la signature électronique remplit les mêmes fonctions que la signature simple mais sur un support dématérialisé, autrement dit, c'est une marque électronique qui a pour but d'apparaître sur un document pour authentifier son auteur ou en établir sa légalité[454]. La signature électronique, sur ces deux continents, est considérée comme un ensemble de données électroniques jointes ou associées à un contrat ou un fichier et dont l'utilisation par un individu reflète son intention de signer[455].

184. En Europe et aux États-Unis, une signature électronique pourra être simple, consistant en un nom apposé sur un document électronique ou complexe et plus fiable, impliquant le recours à des technologies avancées et/ou des prestataires[456]. Ils disposent aussi tous deux de prestataires de service de confiance permettant d'apporter des degrés supplémentaires quant à la fiabilité d'une signature électronique[457]. Ces deux continents couvrent des mécanismes d'identification électronique, d'authentification et de certification encadrant aussi bien les niveaux de fiabilité des signatures, que les risques de fraude. Le règlement eIDAS prévoit que l'identification électronique est un « *processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale* »[458] et l'exige

[453] E-Sign Act, section 101 (a) (1).
[454] Black's Law Dictionnary 1381, 6th ed. 1990 ; C. civ., art. 1366, al.1.
[455] Aux États-Unis : E-Sign Act, Section 106 (5) ; UETA Act, Section 2 (8). En Europe et particulièrement France : Règl. eIDAS, art. 3.10 ; C. civ., art. 1366, al.1.
[456] J. Daniel Greewood and A. Ray Campbell, « Elecronic Commerce Legislation : From Written on Paper and Signed in lnk to Electronic Records and Online Authentification », 53 bus. Law. 307 (1997) ; Règl. eIDAS, art. 3.10, 3.11, 3.12 et C. civ., art. 1366, al.2.
[457] Règl. eIDAS, cons. 35, art. 22 ; E-sign Act, section 101 (g).
[458] Règl. eIDAS, art. 3.1.

dans certains cas comme condition validant une signature électronique[459]. L'authentification consiste en « *un processus électronique qui permet de confirmer l'identification électronique d'une personne physique ou morale, ou l'origine et l'intégrité d'une donnée sous forme électronique* »[460]. *E-Sign Act* n'impose pas l'identification comme une condition de validité d'une signature électronique mais adapte, quant à lui, des méthodes de vérification d'identité *a posteriori* par un tiers, comme celle de la certification conforme par un officier assermenté dite procédure de *notarization* et la confirmation de ladite procédure par l'*aknowledgment*[461]. La présence d'un officier public ou « *notary* » n'est pas requise pour la validité de la vérification[462]. En effet, *E-Sign Act* précise que dès l'instant où une disposition exige qu'une signature soit certifiée ou confirmée, cette condition est remplie lorsque la signature de l'officier assermentée est jointe ou liée logiquement à la signature ou au fichier[463]. L'authentification en France finalement proche de la certification américaine - bien que plus sectorielle -, aurait pour différence de pouvoir être effectuée par voie électronique sans la présence obligatoire d'un officier assermenté.

185. Le règlement eIDAS reconnait comme recevable en justice la signature électronique[464]. L'*UETA Act* prévoit également que dans une procédure, une signature ne peut être exclue du seul fait qu'elle est sous forme électronique[465]. La loi type de la CNUDCI sur les signatures électroniques de 2001 uniformise, pour le reste, les règles sur les signatures électroniques au sein des pays membres des Nations unies[466].

Paragraphe 2 : Les différences structurelles entre les droits européen et nord-américain de la signature électronique

186. Bien que les modèles des preuves électroniques se rapprochent en Europe et aux États-Unis dans le principe même de leurs admissibilités et de leurs recevabilités, les approches restent idéologiquement différentes. Si les États-Unis empruntent une approche permissive pour

[459] Règl. eIDAS, art. 26.
[460] Règl. eIDAS, art. 3.5.
[461] E-Sign Act, section 101 (g).
[462] Voir les développements n°241 sur les *notaries*.
[463] E-Sign Act, section 101 (g).
[464] Règl. eIDAS, art. 25.
[465] UETA Act, section 13.
[466] Loi type CNUDCI sur les signatures électroniques, 2001.

la signature électronique, tant théoriquement que dans la vie des affaires (B), l'Europe adopte une approche plus intermédiaire (A).

A. Une approche intermédiaire du Règlement eIDAS en Europe

187. Le règlement eIDAS adopte une approche intermédiaire ou hybride concernant les différents degrés de fiabilité de signature. Ce règlement permet d'utiliser les signatures électroniques mais accorde différents niveaux de fiabilité en fonction des conditions remplies par celles-ci. Il existe trois degrés de signature de la moins fiable à la plus fiable : la signature électronique simple, la signature électronique avancée et la signature électronique qualifiée[467].

188. Pour les signatures électroniques qualifiées qui requièrent un dispositif de création de signature qualifiée reposant sur un certificat qualifié de signature, des prestataires de service de confiance qualifié sont désignés par les organes de contrôle désignés par les États membres pour délivrer, notamment, ces certificats. En France, c'est l'Agence nationale de la sécurité des systèmes d'information (ANSSI) qui accorde ces agréments, dispose d'un pouvoir de contrôle *a posteriori* des prestataires, et a droit de prendre des mesures nécessaires pour les prestataires non qualifiés[468].

189. C'est ainsi que l'esprit du règlement eIDAS est d'instaurer un gage de vérification pour les degrés de fiabilité les plus élevés de signature. Certains autres pays prennent parti pour une approche totalement prescriptive contrairement à cette approche intermédiaire, comme au Brésil, Inde, Israël, et en Malaisie notamment, où les lois dictent les moyens techniques à employer pour signer électroniquement. Au total opposé, l'approche des États-Unis est permissive.

B. Une approche permissive de l'E-Sign et *UETA Act* aux États-Unis

190. L'approche américaine est la plus libérale. Les lois des États acceptent le recours aux signatures électroniques pour la presque totalité des documents et sont dites « *neutres* »

[467] Voir *infra* n°316 et s.
[468] Règl. eIDAS, art. 17. Voir *infra* n°342.

technologiquement. *E-Sign Act* met, par conséquent, en place une règle générale de validité de la signature électronique. Une signature peut, de surcroît apparaître sous différentes formes comme des sons, des symboles ou des processus électroniques dès lors que la personne qui a joint cette signature ou l'a logiquement associée à un contrat ou un registre, avait l'intention de signer le document[469]. Enfin, les prestataires de service de signatures électroniques sont le plus souvent des sociétés privées et ne sont pas soumises à un contrôle gouvernemental[470]. Cette approche permissive est la traduction plus globale d'une plus grande souplesse dans la vie des affaires aux États-Unis.

[469] E-Sign Act, Section 106 (5).
[470] Par exemple : Docusign, Verisgn, Signnow etc.

CHAPITRE 2

LES CONDITIONS D'ADMISSIBILITE ET DE RECEVABILITE DES PREUVES *BLOCKCHAINS* EN JUSTICE

191. Pour être admise et reçue par un juge, la preuve *blockchain* judiciairement discutée se voit appliquer les règles de droit de la preuve et les principes fondamentaux du procès. Le droit a en effet pour mission de protéger les individus par le respect du principe de licéité (section 2) et celui de légalité des modes de preuve issus des preuves *blockchains* (section 1).

Section 1 : Le respect de la légalité des preuves *blockchains* apprécié par les juges

192. Notre système de preuve mixte français[471] énumère un principe général de liberté de la preuve des faits et des actes juridiques[472] qui est applicable aux preuves *blockchains* (paragraphe 1). Des exceptions de preuve légale sont imposées pour certains modes de preuve (paragraphe 2). Cette présentation de la légalité de la preuve comme une exception au principe de liberté fait suite à un mouvement de libéralisation de l'admissibilité des modes de preuves civiles par la Cour de cassation[473].

Paragraphe 1 : L'application du principe de liberté aux enregistrements dans une *blockchain*

193. Le principe de liberté de la preuve des faits juridiques qui seront enregistrés dans la *blockchain* (A) et d'autres cas précis (B) admet que l'on puisse apporter des preuves par tout moyen.

[471] F. Ferrand, Preuve, *op.cit.*, n°28, 30.
[472] N. Dissaux, C. Jamin, *Réforme du droit des contrats, du régime général et de la preuve des obligations. Commentaire des articles 1100 à 1386-1 du Code civil*, Supplément au Code civil Dalloz 2017, août 2016, p.240.
[473] R. Legeais, *Les règles de preuve en droit civil. Permanences et transformations*, *op.cit.*, 260 p. ; E. Vergès, « Droit de la preuve : une réforme en trompe-l'œil », *op.cit.*, p.839.

A. Le principe de liberté de la preuve des faits juridiques enregistrés dans une *blockchain*

194. Les faits juridiques sont des conséquences de droit (création, extinction, ou modification des droits) qui n'ont pas été voulues par leur auteur[474]. Ils s'opposent aux actes juridiques qui sont toutes manifestations de volonté ayant pour but immédiat et direct de créer, éteindre, résoudre, reconnaître, confirmer, ratifier, modifier, restreindre étendre ou enfin transférer des obligations ou des droits[475]. Certains faits peuvent être enregistrés dans la *blockchain* et seront à ce titre régis par le principe de liberté de la preuve.

195. Depuis la réforme du droit des contrats par l'ordonnance n°2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations[476], l'article 1358 du Code civil présente la liberté de la preuve comme un postulat de base érigé en principe sacramentel[477], en ce qu'il dispose qu' « *hors les cas où la loi en dispose autrement, la preuve peut être apportée par tout moyen* »[478]. Le principe de liberté de la preuve désormais consacré est « *au fondement de toute vérité scientifique* »[479]. C'est pour cette raison que, par principe, tout moyen de preuve apporté devant les tribunaux est admis pour les faits et les actes. La liberté de la preuve ou la preuve libre/morale est le fait que « *la loi permet aux parties et au juge d'utiliser tous procédés de preuve* »[480]. Elle laisse alors au juge *« (…) le soin, au regard de son intime conviction fondée sur les éléments probatoires dans le débat, de décider si tel fait est ou non prouvé* »[481].

---

[474] Cass. civ., 13 juill. 1874 : DP 1875, 1, p.73 ; Cass. 1ère civ., 27 avr. 1977 : D. 1977 p.413, note Gaury.
[475] Cass. req., 1er août 1906 : DP 1909, 1, p.398 ; M. Planiol, G. Ripert, *Traité pratique de droit civil français*, t. 7, 2e éd., 1952, n°762, p.243.
[476] Ordonnance n°2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations, publié au JORF n°0035 du 11 février 2016, texte n°26.
[477] Rapport, JO 11 févr. 2016 : « *L'article 1358 pose le principe de liberté de la preuve, sauf disposition légale contraire. Ce principe n'était pas affirmé de façon aussi limpide dans le code actuel, mais se déduisait de la confrontation des dispositions des articles 1341 et 1348. Le principe est désormais posé, et concerna autant les faits juridiques que les actes juridiques, en dehors des exceptions légales* ».
[478] Désormais, le principe et l'exception sont inversés par rapport au droit antérieur, conformément aux évolutions qui se dégageaient en droit positif (E. Vergès, « Droit de la preuve : une réforme en trompe-l'œil », *op.cit.*, p.839). En somme, « *le nouveau dispositif ne fait qu'énoncer clairement ce qui était admis, mais de manière plus confuse. On n'est pas loin de le suivre : dans l'ancien système, il était dit que l'acte juridique devait être prouvé par écrit, mais uniquement au-delà d'un certain montant ; aujourd'hui on retient que la preuve de l'acte juridique est libre, mais en deçà de ce montant … Ce qui revient à dire à peu près la même chose mais sous deux angles différents* » (N. Dissaux, C. Jamin, *Réforme du droit des contrats, du régime général et de la preuve des obligations. Commentaire des articles 1100 à 1386-1 du Code civil*, *op.cit.*, p.240).
[479] X. Lagarde, *Réflexion critique sur le droit de la preuve*, *op.cit.*, p.17 : lequel critiquait l'absence de reconnaissance d'un principe général en droit français.
[480] F. Ferrand, Preuve, *op.cit.*, n°27.
[481] *Ibid.*

196. La *blockchain* pourra distinguer les faits inhérents aux opérations se déroulant dans le registre et ceux se déroulant à l'extérieur de la *blockchain* intégrés dans une transaction pour refléter cette situation extérieure. Ces derniers faits pourraient être qualifiés de « *faits constatés* » par la *blockchain*. Par exemple, une transaction datée pourra être un moyen de prouver le paiement dans les temps d'une dette d'un débiteur envers son créancier[482]. Les cahiers de laboratoire permettant aux personnes qui réalisent des travaux de recherche de consigner au jour le jour le détail et évènement de leurs travaux sont des faits extérieurs qui pourront également être intégrés dans la *blockchain*.

B. Les autres cas de liberté de la preuve dans une *blockchain*

197. **La liberté de la preuve en matière commerciale.** En matière commerciale, l'article 110-3 du Code de commerce prévoit qu' « *à l'égard des commerçants, les actes de commerce peuvent se prouver par tous moyens à moins qu'il n'en soit autrement disposé par la loi* ». Cette règle s'applique entre commerçants (personne physique ou morale[483]) ayant passé un acte de commerce. *A contrario*, elle ne s'appliquera pas dans un litige opposant deux personnes n'ayant pas le statut de commerçant et/ou n'ayant pas passé un acte de commerce[484].

198. D'une part, si l'un des deux n'est pas commerçant, ce sont les règles probatoires du Code civil qui s'appliquent[485], même si les juges pourront admettre que le commerçant était dans une impossibilité morale de se constituer une preuve écrite en raison par exemple de l'usage de la profession ou d'un type de marché spécifique[486]. D'autre part, ce principe de liberté de la preuve en matière commerciale devra s'appliquer à la preuve d'un acte de commerce ou *a minima* à un acte mixte[487]. L'étendue du principe de liberté pourrait porter sur

[482] Voir *infra* n°258 et s.
[483] Voir notamment : Cass. com. 10 mars 2004, n°0215.256, RJDA 2004, n°994 , Cass. com. 13 nov. 2007, n°0617.823, RJDA 2008, n°162.
[484] D. Guével, Fasc. 40 : Contrats et obligations. Preuve testimoniale. Liberté des preuves en matière commerciale, JCl. Civil Code, Lexis Nexis, 7 sept. 2010, n°52-81.
[485] Cass. com. 21 juin 1988, Bull. civ. IV, n°212 ; JCP 1989. II. 21 170, note Moderne ; JCP N 1990. II. 13, note P.Delebecque.
[486] Cass. 1ère civ., 17 mars 1982, Bull. civ. I, n°114 ; Cass. com. 22 mars 2011, n°09-72.426, Bull. civ. IV, n°50, RTD civ. 2011. 491, obs. P.Deumier, D. 2011. Chron. 2891, obs. P.Delebecque ; D. 2011. Chron. 2687, obs. F. Arbellot.
[487] Cass. com., 17 févr. 1976, Bull. civ. IV, n°58 ; Cass. com., 20 mai 1980, Bull. civ. IV, n°210 ; Cass. com., 12 oct. 1982, Bull. civ. IV, n°313 ; Cass. 1ère civ., 8 févr. 2000, n°98-10.107, Bull. civ. I, n°35, RTD com. 200. 327, obs. J. Derruppé, RTD com. 2000. 704, obs. B. Bouloc ; Com. 13 nov. 2001, n°97-22.153. Jurisprudence en sens contraire : Cass. 1ère civ., 2 mai 2001, n°98-23.080, Bull. civ. I, n°108, RTD com. 2001. 865, obs. B. Saintourens.

l'existence ou le contenu de l'acte, et la preuve outre et contre le contenu à l'acte[488]. La jurisprudence a déjà admis certains modes de preuve comme des documents comptables ou des factures, des enregistrements sur support informatique, voire même leur reproduction sur support informatique retraçant des transactions[489]. Par ce dernier exemple, l'intérêt concret des transactions d'une *blockchain* pourrait être mis en avant lors d'un échange précis entre deux commerçants portant sur une vente, en contrepartie de crypto-monnaies. La preuve de l'existence de cette vente grâce spécifiquement au registre retraçant la transaction litigieuse pourrait donc être apportée.

199. **La liberté de la preuve en matière pénale.** En matière pénale, l'article 427 du Code pénal prévoit que « *... les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction* ». Il sera admis que des éléments de preuve soient apportés par tous moyens, par exemple, pour des cas des *cryptojacking*, des rançongiciels moyennant des crypto-monnaies, ou encore des infractions traditionnelles adaptées à la *blockchain* comme des vols de clés privées ou encore des escroqueries à l'investissement[490].

200. Tout d'abord, le *cryptojacking* est un phénomène majeur qui s'est développé en 2018[491]. Il consiste en l'utilisation clandestine de la puissance de calcul d'un tiers de manière à miner des crypto-monnaies au bénéfice du cyberdélinquant. Par exemple, CoinHive - pionner dans cette pratique - a impliqué l'installation frauduleuse d'une extension sur des navigateurs Internet pour ensuite détourner la puissance de calcul des ordinateurs des personnes physiques ou morales[492]. La victime a le loisir dans ce cas de réunir toutes les preuves pertinentes pour

[488] CA Paris, 30 juin 1995, SA Tabbagh Travel Service c/ SA Bellamy et Martet, Juris-Data n°022780 ; Com. 29 mars 1994, n°92-12.733, Bull. civ. IV, n°129, RTD com. 1994. 697.
[489] Cass. 1ère civ., 8 nov. 1989, D. 1990. 369, note C. Gavalda ; D. 1991. Somm. 38, obs. M. Vasseur ; JCP 1990. II. 21 576, note G. Virassamy.
[490] Exemple d'une demande d'indemnisation d'une prétendue victime d'escroquerie suite à un transfert d'un montant de 1 500 euros en bitcoin : TGI de Grasse, Commission d'indemnisation des victimes d'*infra*ctions, 26 septembre 2016, n°15/02876. Pour davantage de développements sur les *infra*ctions courantes en matières de *blockchain* et d'actifs numériques et les recours adaptés voir : A. Barbet-Massin, J. Brosset, « La souscription de crypto-actifs et de jetons d'ICOs : les recours des investisseurs », RLDA n°6531, suppl. n°140, sept. 2018, p.38-39.
[491] Tracfin, Tendances et analyse des risques de blanchiment de capitaux et de financement du terrorisme 2017-2018, nov. 2018, cas n°16, p.62 ; Tracfin, Tendances et analyse des risques de blanchiment de capitaux et de financement du terrorisme en 2018-2019, dec. 2019, p.69 ; J. Martinon, « Crypto-actifs : la justice pénale à l'épreuve des crypto-monnaies », Dossier : la justice pénale à l'épreuve des crypto-monnaies, Dalloz IP/IT n°10, oct. 2019, p.531.
[492] J. Martinon, « Phénomènes criminels célèbres ou exotiques dans le champ des crypto-actifs (illustrations extraites de la présentation de Patrice Réveillac, Europol) », Dossier : la justice pénale à l'épreuve des crypto-monnaies, Dalloz IP/IT n°10, oct 2019, p.535.

démontrer l'infraction comme, des factures d'électricité anormales ou encore un constat d'huissier d'une extension ou logiciel frauduleux.

201. Les rançongiciels (ou « *ransomwares* ») sont ensuite des logiciels spécifiques prenant en otage des données moyennant une rançon et des logiciels malveillants (ou « *malware* ») ont pour but d'avoir accès au système informatique d'une victime sans son consentement. Souvent, les installations de ces logiciels pour l'accès au système informatique de la victime et les transactions litigieuses des fonds en crypto-monnaies seront constitutifs des infractions d'accès ou maintien frauduleux dans un système de traitement automatisé de données (STAD) ou d'extorsion[493]. Il est apparu, par exemple, que le rançongiciel « *WannaCry* » collectait sa rançon en bitcoins *via* l'adresse publique du cyber-délinquant[494]. Dans ces cas, les preuves des transferts litigieux de crypto-monnaies retracés dans une *blockchain* et la preuve de l'adresse publique utilisée par le cyber-délinquant peuvent être apportées au soutien des prétentions de la partie victime.

202. S'agissant du vol par intrusion dans un système informatique comme un ordinateur[495] ou un *smartphone* stockant la clé privée de la victime, il constitue l'infraction d'« *extraction* » de données et pourra être prouvé librement[496]. Il est courant que des détenteurs de portefeuilles virtuels mal protégés se voient subtiliser des crypto-actifs suite à ce type vol. Ceux-ci pourront alors prouver par un relevé de compte que les crypto-actifs ont subitement été soustraits.

203. Enfin, des escroqueries à l'investissement, incluant de l'hameçonnage (ou « *phishing* ») et des usurpations d'identité[497] ciblent régulièrement des personnes peu informées. La pratique du *phishing* vise les investisseurs de crypto-actifs, destinataires d'un courriel provenant d'un prestataire de services liés aux crypto-actifs établi, comme une plateforme d'échanges de crypto-actifs[498]. À la suite de la réception de ce « *spam* », la victime est incitée à se rediriger

[493] C. pén., art. 323-1, art. 312.
[494] « Cyberattaque, ransomware et Bitcoin », bitcoin.fr, https://bitcoin.fr/cyberattaque-ransomware-et-bitcoin/ (consulté le 31/05/2020).
[495] J. Martinon, « Crypto-actifs : la justice pénale à l'épreuve des crypto-monnaies », *op.cit.*, p.532 : « *les usagers prennent souvent le parti de « copier » ces informations et de les « coller » au lieu de les taper un à un avec le clavier, un peu comme ces clés Wifi interminables. Les informations contenues dans les presse-papiers des systèmes d'exploitation comme Windows sont généralement peu sécurisées et peuvent donc servir de vecteur d'attaque très efficace* ».
[496] C. pén., art. 323-3. Selon une jurisprudence antérieure, il était admis que le vol de données soit puni sur le fondement de l'article 311-1 du code pénal qui vise la soustraction frauduleuse de la chose d'autrui (Cass. crim., 20 mai 2015, n°14-81336 (confirmé par Cass. Crim., 28 juin 2017, n°16-81113).
[497] C. pén., art. 226-4-1.
[498] « *Entre 2017 et 2018, le groupe Lazarus, réputé proche de la Corée du Nord, serait responsable du vol de 571 millions de dollars sur un total de 882 millions de dollars de crypto-actifs dérobés sur des plateformes d'échange,*

vers une fausse version du site du prestataire lui demandant d'entrer ses identifiants, de façon à permettre au cyber-délinquant le détournement des fonds. Par exemple, en septembre 2019, les clients de CoinHouse la plateforme française d'achat et de vente en ligne et physique de crypto-actif, se sont fait escroquer à la suite d'un *phishing* [499]. Dans ces hypothèses, les personnes victimes pourront prouver par tout moyen le *phishing* soit, en avançant que l'établissement prétendument frauduleux était visé sur la liste noire de l'AMF, soit en apportant l'ensemble des échanges d'e-mails envoyés par le cyber-délinquant utilisant la même charte graphique que le véritable établissement[500].

Paragraphe 2 : L'application des exceptions de légalité aux inscriptions dans une *blockchain*

204. Cette exception de preuve légale résulte de la règle de légalité des modes de preuve dressés par le législateur (A) selon laquelle il convient d'apporter le mode de preuve exigé par la loi pour certaines preuves. Pour l'heure, en l'absence de mode de preuve spécifique, une preuve *blockchain* se voit appliquer par analogie aux modes de preuve existants, les règles prévues par le Code civil notamment mais pourrait être confrontée à une impossibilité morale ou matérielle de fournir ces preuves (B)[501].

A. Le principe de légalité des modes de preuve inscrits dans une *blockchain*

205. **Le principe.** Le principe de la preuve légale consiste à présenter le mode de preuve imposé par une disposition légale. La preuve légale selon le Professeur Frédric Ferrand est le fait qu'une « *preuve peut être conditionnée par des règles légales imposant certains modes de preuve prédéterminés et ordonnant au juge de tenir pour vrais les faits établis par certains*

soit près de 65 % de la somme totale au niveau mondial. Cinq des quatorze cyberattaques de plateformes ont été attribuées au groupe Lazarus, parmi lesquelles le piratage de la société japonaise Coincheck (NEM) re-cord de 532 millions de dollars. Un récent rapport de l'ONU tisse également un lien entre ces cyberattaques et le fi nancement du programme nucléaire de la Corée du Nord » (J. Martinon, « Phénomènes criminels célèbres ou exotiques dans le champ des crypto-actifs (illustrations extraites de la présentation de Patrice Réveillac, Europol) », *op.cit.*, p.534-535.

[499] https://www.coinhouse.com/fr/communique-suite-a-la-tentative-de-phishing-de-coinhouse-du-12-septembre/ (consulté le 31/05/2020).

[500] C. pén., art. 226-4-1.

[501] Voir *infra* n°246 et s. pour les qualifications juridiques des preuves *blockchains*.

procédés de preuve »[502]. S'agissant par exemple de l'acte juridique portant sur une somme d'un montant supérieur à 1500 euros[503], l'article 1359 du Code civil le conditionne à la preuve d'un écrit sous signature privée ou authentique. Dans l'hypothèse où l'on souhaiterait prouver un acte juridique portant sur une somme supérieure à 1500 euros échangée grâce à la *blockchain*, un acte devra être établi au préalable sous signature privée ou authentique en dehors de la *blockchain* pour se préconstituer la preuve de l'échange. Au sujet de la preuve de souscription de minibons par exemple, un acte sous seing privé est requis, mais dorénavant l'inscription sur la *blockchain* de minibons équivaut à un contrat[504]. Partant, il sera possible d'apporter le registre de transactions de la *blockchain* démontrant l'inscription des minibons en cause[505].

206. **La distinction entre mode de preuve parfait et imparfait.** Il est de tradition chez le juriste de rattacher les différentes preuves légales de droit commun à une ancienne classification : celle des preuves parfaites et imparfaites[506]. La preuve est dite parfaite lorsque les « *(…) procédés sont, à la fois, les plus hauts dans l'échelle des valeurs et ceux qui peuvent se suffire à eux-mêmes en ce qu'ils s'imposent au juge* »[507]. Ces preuves sont perçues comme incontestables et ayant une grande valeur juridique. Alors que les preuves imparfaites sont admises exceptionnellement mais ne lient pas le juge. La doctrine considère généralement que l'écrit littéral, le serment décisoire ou l'aveu judiciaire sont des preuves parfaites alors que le commencement de preuve par écrit, la preuve testimoniale, l'aveu extra-judiciaire sont imparfaites[508]. Si l'empreinte ancrée dans une *blockchain* pourra être considérée comme une preuve parfaite dans l'hypothèse où elle serait qualifiée de copie, une transaction serait une preuve imparfaite si elle s'apparente à un commencement de preuve par écrit[509]. Selon l'une ou l'autre de ces catégories, les conditions d'admissibilité de ces preuves seront alors plus ou moins strictes.

---

[502] F. Ferrand, Preuve, *op.cit.*, n°27.
[503] Décret n°2016-1278 du 29 septembre 2016 portant coordination des textes réglementaires avec l'ordonnance n°2016-131 portant réforme du droit des contrats, du régime général et de la preuve des obligations.
[504] C. mon. fin., art. L223-12.
[505] Voir *infra* n°424-441.
[506] H., L., J. Mazeaud, F. Chabas, Leçons de droit civil, t. 1, vol.1, *Introduction à l'étude du droit*, par F. Chabas, Montchrestien, 12ème éd., 2000, p.616 ; D. Guével, Fasc. unique : Contrats et obligations – Preuve par serment, JCl. Civil Code > Art. 1384 à 1386-1, Lexis Nexis, juin 2016 (maj 25 nov. 2018), n°4.
[507] D. Guével, Fasc. unique : Contrats et obligations – Preuve par serment, *op.cit.*, n°4.
[508] H., L., J. Mazeaud et F. Chabas, Leçons de droit civil, *op.cit.*, p.616, n°431 ; Guével D., Fasc. 50 : contrats et obligations, Preuve testimoniale, Commencement de preuve par écrit, JCl. Civil Code, art. 1341 à 1348, Lexis Nexis, juin 2013, n°13 ; S. Dorol, Fasc. 20 : Preuve. Modes de preuve, JCl. des Huissiers de Justice > Preuve, Lexis Nexis, févr. 2015 (maj juin 2015), n°2.
[509] Voir *infra* n°378 et s. et n°292 et s.

B. L’exception d’impossibilité morale ou matérielle de la preuve des actes juridiques inscrits dans une *blockchain*

207. Le Code civil prévoit une exception à la légalité de l’écrit. L’article 1360 du Code civil vise le cas d’une impossibilité matérielle ou morale « *…de se procurer un écrit, s'il est d'usage de ne pas établir un écrit, ou lorsque l'écrit a été perdu par force majeure* ». Précisons que l’impossibilité matérielle ou morale de se procurer un écrit ne dispense pas celui qui l'invoque d'avoir à prouver l'acte, mais elle permet uniquement de pouvoir l’apporter par tout moyen. Cela n’affecte pas la charge de la preuve mais seulement l'admissibilité des modes de preuve[510] sauf lorsqu’un tiers à l’acte doit apporter la preuve de son existence et de son contenu[511].

208. Il a déjà été admis des preuves par témoins de l’existence et du contenu d’un testament au motif d’une perte fortuite de celui-ci par un tiers. Sans même caractériser le fait constitutif d’un cas fortuit ou d’une force majeure, l’impossibilité matérielle a permis aux juges de déclarer que la disparition de ce testament était le fait d’un tiers. Une impossibilité matérielle de fournir un acte dans le cadre de la *blockchain* pourrait être le fait, par exemple, d’avoir ancré un acte sous seing privé portant sur une somme de plus de 1500 euros, dont la perte serait imputable à un prestataire qui se charge du stockage dudit document (à l’exclusion probablement des hypothèses de stockage en mode BaaS dans le cloud, qui est considéré comme particulièrement sûr). Ce pourrait être certainement le cas aussi de la perte de clés privées donnant accès à des crypto-actifs par un prestataire de services de portefeuille numérique.

[510] Cass. 1ère civ., 19 oct. 2016, n°15-27.387, D. 2016. 2169, D.2018. 259, obs. J.-D. Bretzer et A. Aynès ; AJ fam. 2016. 608, obs. P.Hilt ; RTD civ. 2017. 472, obs. B. Vareille.
[511] Cass. 1ère civ., 5 janv. 1983 : Bull. civ. 1983, I, n°10 ; Cass. 1ère civ., 18 avr. 1989 : D. 1992, somm. p.228, obs. B. Vareille ; Cass. 1ère civ., 11 juill. 1984 : Bull. civ. 1984, I, n°231 ; Cass. 1ère civ., 31 mars 1992 : Bull. civ. 1992, I, n°98 ; Cass. 1ère civ., 3 janv. 1996 : Bull. civ. 1996, I, n°7 : Defrénois 1996, p.1022, obs. Ph. Delebecque.

Section 2 : Le respect du principe de licéité des preuves *blockchains* apprécié par les juges

209. Le juge vérifie le respect de licéité des preuves *blockchains* conformément aux principes généraux qui s'imposent à lui[512]. C'est une forme de vérification « *morale* » de la preuve[513]. À cette fin, il doit mettre en jeu un contrôle de proportionnalité de l'intérêt des preuves *blockchains* licites (paragraphe 1) pour, le cas inverse, écarter les preuves *blockchains* illicites par application du principe de « *l'exclusion des preuves* »[514] (paragraphe 2).

Paragraphe 1 : Les preuves *blockchains* illicites écartées par les juges

210. Les preuves *blockchains* illicites seront écartées dans deux domaines plus particulièrement : en matière civile (A) en matière pénale (B).

A. Les preuves *blockchains* illicites en matière civile

211. La licéité s'entend du respect des principes généraux du droit de la preuve et des règles techniques propres à chaque preuve. Ce principe s'impose à toutes les preuves et de fait aux preuves *blockchains*. Une preuve civile est donc admissible dès lors qu'elle n'est pas prohibée par la loi ou un principe général de la preuve civile[515]. L'administration de la preuve civile veut que des éléments de preuves issus de la *blockchain* obtenus par des procédés déloyaux (1), qui porteraient atteintes à la confidentialité (2) ou à des droits essentiels comme la vie privée (3), soient considérés comme illicites[516]. D'autres principes spécifiques doivent être respectés comme celui de dignité de la personne ou celui de l'interdiction de se constituer de preuve à

[512] S. Guinchard, *Droit et pratique de la procédure civile. Droit interne et européen*, Dalloz Action, 9e éd., 2017/2018, n°111.21 : « *En dehors des contestations relative à la preuve littérale, celui qui entend engager un procès doit également s'interroger sur le caractère licite de la preuve dont il dispose* ».
[513] F. Terré, *Introduction générale au droit*, Dalloz coll. « Précis », 2015, n°167 cité par V. Magnier, « Enjeu de la *blockchain* en matière de propriété intellectuelle et articulation avec les principes généraux de la preuve », Dossier *Blockchain* et preuve, Dalloz IP/IT n°2, févr. 2019, p.79.
[514] E. Vergès. « Loyauté et licéité, deux apports majeurs à la théorie de la preuve pénale », D. 2014, p.623 : cet auteur décrit un double mouvement dans la constitution d'un dossier probatoire pour aboutir sur la proposition deux principes : celui de réunion des preuves et celui d'exclusion des preuves.
[515] H., L., J. Mazeaud, F. Chabas, Leçons de droit civil, t. 1, vol. 1, *Introduction à l'étude du droit*, *op. cit.*, n°371- 2.
[516] Pour Etienne Vergès, la loyauté, la protection de la vie privée et la confidentialité devraient figurés dans les principes généraux du droit de la preuve (E. Vergès. « Loyauté et licéité, deux apports majeurs à la théorie de la preuve pénale », *op.cit.*, p.623).

soi-même[517]. Ces derniers ne seront pas abordés dans l'étude par manque de pertinence avec le sujet des preuves *blockchains*.

1. La preuve *blockchain* obtenue de façon déloyale civilement

212. La déloyauté est un « *manquement à la loyauté, manque de franchise, de droiture ; dans un jeu, un débat, un combat manquement aux règles qui le gouvernent, afin de l'emporter subrepticement par ce moyen* »[518]. Le principe de loyauté est la condition d'exercice des droits de la défense et plus généralement, la condition de la conduite du procès équitable[519]. Bien que ce principe ne soit pas consacré par le législateur, il « *irrigue* » les dispositions processuelles par des règles ponctuelles[520] et s'épanouit au prix d'une effectivité sans failles[521]. Dans le Code de procédure civile, hormis l'article 1464, qui emploie la notion de loyauté à propos de la conduite de la procédure arbitrale, seul l'article 763 fait obligation au juge de la mise en état « *de veiller au déroulement loyal de la procédure* ». C'est souvent sur la base de l'article 9 de Code civil relatif à la vie privée, l'article 1104 sur la bonne foi contractuelle[522], et l'article 6 de la CESDH faisant référence à l'égalité des armes et au principe du contradictoire, qui ne mentionnent pas la loyauté, que se fonde le principe de loyauté en matière civile.

213. Le droit européen de la preuve s'est par ailleurs constitué de nombreuses décisions de la Cour européenne des droits de l'homme (CEDH). La CEDH impose que les preuves soient recueillies et exploitées de façon loyale, depuis un arrêt important du 6 décembre 1988 dit « *Barbara, Messegue et Jabardo c/ Espagne* »[523]. Par cet arrêt, la Cour consacre le principe de loyauté dans la réunion judiciaire et policière des preuves. En dépit de cela, il convient de rechercher si la procédure est considérée dans sa globalité comme loyale, à savoir si le mode de présentation des moyens de preuve à charge et à décharge a revêtu un caractère contradictoire. Ce principe de loyauté est une exigence générale si bien qu'il n'irait pas jusqu'à

[517] C. civ., art. 1363.
[518] G. Cornu, *Vocabulaire juridique*, *op.cit.*, p.323.
[519] P.Lemoine, « Loyauté de la preuve », *in* Cour de cassation, Rapport, La vérité, 2004, p.142.
[520] D. Guével, Fasc. unique : Contrats et obligations – Preuve. Charges de la preuve et règles générales, JCl. Civ., Lexis Nexis, 25 juill. 2014.
[521] M.-E. Boursier, *Le principe de loyauté en droit processuel*, thèse ss. dir. S. Guinchard, Paris 2, Dalloz coll. Nouvelle Bibliothèque des thèses, 2013, 527 p.
[522] L'article 1104 du Code civil dispose uniquement que *« les conventions doivent être négociés, formés et exécutés de bonne foi* ».
[523] CEDH, 6 déc. 1988, aff. 15590/83, Barbara, Messegue et Jabardo c/ Espagne.

imposer ou refuser des modes de preuve indépendamment d'autre considération. Le procès doit donc avoir été équitable dans son ensemble. Il revient en principe aux juridictions internes d'apprécier les l'ensemble des éléments recueillis et la pertinence des preuves. C'est l'arrêt de la CEDH du 12 juillet 1988 dit « *Schenk c/ Suisse* » qui énonce que la CESDH ne réglemente pas l'admissibilité des preuves en tant que telle, matière qui relève du droit interne[524]. Dès lors, la CEDH n'a pas compétence pour exclure l'admissibilité d'une preuve recueillie de façon illégale[525].

214. En substance, l'exigence générale de loyauté dans le cadre d'une preuve *blockchain* interdira que soient utilisés des éléments de preuve obtenus grâce à des procédés déloyaux dans la phase d'administration de la preuve. Le principe de loyauté appliqué à cette preuve se décompose en deux points. Premièrement, les preuves *blockchains* doivent être obtenues par des moyens loyaux[526]. Serait jugée déloyale la « *non-indépendance* » des huissiers de justice par rapport à la partie requérante lors de l'établissement d'un procès-verbal d'un ancrage *blockchain* par exemple[527]. Ce fut le cas dans l'affaire d'un avocat stagiaire d'un cabinet d'avocats représentant les intérêts de la société titulaire de droits qui assignait une autre en contrefaçon et parasitisme. La preuve de l'opération d'achat avait été jugée irrecevable au motif que le tiers acheteur devait être indépendant du requérant et que tel n'était pas le cas du stagiaire avocat si bien que le constat d'achat était irrecevable[528]. D'autre part, les preuves *blockchains* doivent être produites de façon loyale en justice[529]. Cette exigence interdit de retenir une preuve utile à la recherche de la vérité sur la base de l'article 11, alinéa 2 du Code de procédure civile. Le juge ne pourra pas admettre qu'une partie qui aurait accès à des données hachées dans la

[524] CEDH, 12 juill. 1988, req. n°10862/84, Schnek c/ Suisse.
[525] Voir par exemple une décision d'une ingérence dans le droit au respect de la vie privée par des écoutes téléphoniques : CEDH, 24 avr. 1990, Kruslin c/ France : D. 1990, jurispr. p.353, note J. Prade.
[526] Cass., ass. plén., 7 janv. 2011, n°09- 14.316 et 09-14.667, Sté Philips France c./ Ministre de l'économie, de l'industrie et de l'emploi, D. 2011. 562, obs. E. Chevrier, note F. Fourment ; *op.cit.* 618, chron. V. Vigneau ; *op.cit.* 2891, obs. P.Delebecque, J.- D. Bretzner et I. Gelbard- Le Dauphin ; RTD civ. 2011. 127, obs. B. Fages ; *Ibid* . 383, obs. P.Théry ; RTD eur. 2012. 526, obs. F. Zampini.
[527] Même si une partie de la doctrine juge cette position sévère : V. Magnier « Enjeu de la *blockchain* en matière de propriété intellectuelle et articulation avec les principes généraux de la preuve », *op.cit.*, p.80.
[528] Cass. 1ère civ., 25 janv. 2017 n°15-25.210 D.2017. 304 ; *Ibid* . 2018. 259, obs. J.- D. Bretzner et A. Aynès ; *op.cit.* 1566, obs. J.- C. Galloux et P.Kamina ; Dalloz IP/ IT 2017. 335, obs. A. Lecourt ; RTD civ. 2017. 489, obs. N. Cayrol ; *Ibid* . 719, obs. P.Théry ; RTD com. 2017. 92, obs. F. Pollaud- Dulian.
[529] Cass., ass. plén., 7 janv. 2011, n°09- 14.316 et 09-14.667, Sté Philips France c./ Ministre de l'économie, de l'industrie et de l'emploi, D. 2011. 562, obs. E. Chevrier, note F. Fourment ; *Ibid* . 618, chron. V. Vigneau ; *Ibid* . 2891, obs. P.Delebecque, J.- D. Bretzner et I. Gelbard- Le Dauphin ; RTD civ. 2011. 127, obs. B. Fages ; *Ibid* . 383, obs. P.Théry ; RTD eur. 2012. 526, obs. F. Zampini.

blockchain les retienne si celles-ci étaient jugées utiles à la recherche de la vérité de l'affaire en question.

2. La preuve *blockchain* attentatoire aux secrets juridiquement protégés

215. Un ensemble de secrets dans des secteurs variés sont juridiquement protégés auxquels les preuves *blockchains* ne doivent pas porter atteinte. La production d'une preuve *blockchain* ne doit pas par exemple porter atteinte au secret médical[530]. Si une *blockchain* est établie dans le domaine de la santé, les données doivent être hachées et le secret sur celles-ci gardé. Aussi, les secrets professionnels[531] pourraient être affectés dans les *blockchains* établies par des professions réglementées comme les notaires ou encore les huissiers de justice.

216. Le secret bancaire devra être aussi respecté dans les nombreux cas déployés ou envisagés dans ce secteur, bien qu'il ne semble pas de prime abord intervenir dans le cadre des *blockchains* publiques qui exclues par principe les banques[532]. Par exemple, sont ou seront soumis au respect du secret bancaire la banque de France qui a désormais sa *blockchain* de certification de données ou encore certaines banques centrales qui projettent de déployer leur propre crypto-monnaie[533].

217. Les preuves *blockchains* ne doivent pas non plus constituer une atteinte au secret des correspondances[534]. Est une atteinte au secret des correspondances, selon la Cour de cassation,

---

[530] Voir et les nombreuses jurisprudences condamnant des preuves illicites sur le fondement de la violation du secret médical : Cass. 1ère civ., 6 janv. 1998 : Bull. civ. 1998, I, n°3 ; Cass. 1ère civ., 12 janv. 1999 : Bull. civ. 1999, I, n°18, JCP G 1999, II, 10, n°6, p.333, P.Sargos ; Cass. com., 5 mai 2004 et Cass. 1ère civ., 15 juin 2004 : D. 2004, p.2682, note D. Duval-Arnould ; Cass. 1ère civ., 7 déc. 2004 : D. 2005, p.244, D. 2005, p.403, obs. J. Penneau ; Cass. com., 25 janv. 2005 : D. 2005, p.485, note V. Avena-Robardet ; Cass. 2ème civ., 2 juin 2005 : JCP G 2005, IV, 2623.

[531] Voir les nombreuses jurisprudences condamnant des preuves illicites sur le fondement de la violation du secret professionnel : Cass. 1ère civ., 15 janv. 1968 : Bull. civ. 1968, I, n°17, JCP G 1968, IV, 32 ; Cass. com., 15 nov. 1994 : Bull. civ. 1994, n°334 ; Cass. 1ère civ., 4 févr. 2003 : Bull. civ. 2003, I, n°33 ; Cass. 1ère civ., 13 nov. 2003 : Bull. civ. 2003, I, n°225 ; Cass. 1ère civ., 27 janv. 2004 : Bull. civ. 2004, I, n°25.

[532] Voir le champ du secret bancaire restreint aux établissements de crédit (C. mon. fin., L511-33) et les nombreuses jurisprudences condamnant des preuves illicites sur le fondement de la violation du secret bancaire : Cass. com., 13 juin 1995 : Bull. civ. 1995, n°172, D. 1995, inf. rap.p.166 ; Cass. com., 16 janv. 2001 : Bull. civ. 2001, n°12 ; Cass. com., 18 févr. 2004 : Bull. civ. 2004, n°33 ; Cass. com., 25 janv. 2005 : Bull. civ. 2005, n°13, JCP E 2005, n°47, p.1971, Salgueiro, D. 2005, p.485, obs. Avena-Robardet, RTD com. 2005, p.395, obs. R. Legeais, RTD civ. 2005, p.384, obs. J. Mestre et B. Fages ; A. Teissier, *Le secret professionnel du banquier*, thèse, Aix-en-provence, 1998, 709 p.

[533] Voir n°66, n°491.

[534] Voir les nombreuses jurisprudences condamnant des preuves illicites sur le fondement de la violation du secret des correspondances : Cass. soc., 2 oct. 2001 : Bull. civ. 2001, n°291, JCP E 2001, 1918, C. Puigelier, D. 2001,

la production de messages électroniques issus de la messagerie personnelle d'un salarié, quand bien même ce dernier utilisait un ordinateur mis à disposition de son employeur[535]. À considérer que la constitution d'une adresse publique dans la *blockchain* soit assimilée à une messagerie personnelle, la violation du secret des correspondances semble tout de même difficilement constituée puisque la lecture par un employeur d'une transaction de son salarié nécessiterait concrètement d'avoir accès à sa clé privée. Il pourra aussi être exclu la piste de la production d'un SMS issu du téléphone d'un salarié mis à disposition par son employeur qui n'est pas désigné comme personnel[536]. Effectivement, les preuves issues d'un portefeuille virtuel installé sur un téléphone d'un salarié mis à disposition par son employeur pourraient être admises mais l'impossibilité d'échanger des correspondances sur un portefeuille, outre la transaction financière, nous conduit à exclure la piste d'une possible transgression du secret des correspondances.

3. La preuve *blockchain* attentatoire à la vie privée

218. Les preuves constitutives d'une atteinte à la vie privée sont illicites[537]. Les procédés qui portent atteinte à la vie privée constituent une violation des articles 8 de la CESDH, 9 du Code civil. Ces atteintes s'ancrent aussi dans un ensemble de solutions jurisprudentielles envisagées en matière de vie privée[538]. Classiquement, la production d'un document portant atteinte à la vie privée ne serait pas admise par les juges du fond comme, des correspondances en clair dans une transaction *blockchain* portant sur la vie privée ou des documents liés à un dossier médical ancrés dans la *blockchain*.

---

p.3148, note P.-Y. Gautier, Gaz. Pal. 2002, 377, note Bridenne, Defrénois 2002, 1407, obs. A. Raynouard, RTD civ. 2002, p.72, obs. J. Hauser ; Cass. ch. mixte, 18 mai 2007 : Bull. civ. 2007, ch. mixte, n°3, D. 2007, p.2137, note J. Mouly, JCP G 2007, II, 10129, Loiseau ; JCP E 2007, 1884, C. Puigelier.

[535] Cass. soc., 26 janv. 2016 n°14-15.630 : D. actualité 9 févr. 2016, note Kebir.

[536] Cass. com., 10 févr. 2015, n°13-14.779 : D.2015. 959, note Lasserre Capdeville.

[537] J. Ghestin, G. Goubeaux, *Traité de droit civil. Introduction générale*, avec le concours de M. Fabre-Magnan, LGDJ, 4e éd., 1994, p. 631, n°656 et s.

[538] Voir les arrêts : « *eDate Advertising* » en matière de compétence juridictionnelle en cas d'atteinte aux droits de la personnalité sur Internet (CJUE, gr. ch., 25 oct. 2011, aff. C- 509/ 09 et C-161/ 10, D. 2011. 2662 ; *op.cit.* 2012. 1228, obs. H. Gaudemet- Tallon et F. Jault- Seseke ; *op.cit.* 1279, chron. T. Azzi ; *op.cit.* 1285, chron. S. Bollée et B. Haftel ; *op.cit.* 2331, obs. L. d'Avout et S. Bollée ; Rev. crit. DIP 2012. 389, note H. Muir Watt ; RTD com. 2012. 423, obs. A. Marmisse-d'Abbadie d'Arrast ; *op.cit.* 554, obs. F. Pollaud- Dulian ; RTD eur. 2011. 847, obs. É. Treppoz) et « *Bo-lagsupplysningen OÜ* » en matière de compétence en cas d'atteinte aux droits de la personnalité de la personne morale sur Internet (CJUE 17 oct. 2017, aff. C-194/ 16, D. 2018. 276, note F. Jault-Seseke ; *op.cit.* 966, obs. S. Clavel et F. Jault-Seseke ; Rev. crit. DIP 2018. 290, note S. Corneloup et H. Muir Watt ; RTD com. 2018. 520, obs. A. Marmisse-d'Abbadie d'Arrast ; JDI 2018. 602, note C. Latil ; JCP 2017. 2222, note M. Laazouzi).

219. Peu importe les techniques de captations utilisées (caméra, photographie, photos prises par drone[539]) du moment que les preuves fixent la parole ou l'image d'une personne sans son consentement, elles sont considérées comme portant atteinte à la vie privée des individus[540]. Il peut être conçu qu'une empreinte d'une image soit ancrée dans la *blockchain* et soit conséquemment considérée comme attentatoire à la vie privée. Le procédé utilisé dans la surveillance clandestine pourra[541], de surcroît, être pris en compte par les juges.

220. Par exemple, la cour de cassation prohibe les filatures effectuées par un détective privé à la demande d'un employeur à l'insu de son salarié[542]. Pourraient être assimilés à des détectives ou comme réalisant de la surveillance clandestine, les explorateurs de *blockchains* qui se chargent de tracer les transactions d'un même compte et remonter à l'identité d'un émetteur par recoupement. La CEDH veille dans ces cas à ce que l'affaire dite « *Schenk c/ Suisse* », qui laisse aux États-membres le soin de fixer les règles probatoires, n'ait pas pour conséquence une négation des autres droits fondamentaux protégés par la CESDH. Par conséquent, il n'est pas rare que certains éléments de preuve soient sanctionnés par la Cour aux motifs d'une atteinte à la vie privée protégée par l'article 8 de la CESDH. La CEDH a, par exemple, jugé dans un arrêt dit « *Kruslin et Huvig c/ France* » du 24 avril 1990 que des écoutes téléphoniques clandestines étaient une violation de l'article 8 de la CESDH[543].

221. Pour autant, notons qu'un tempérament au principe du respect de la vie privée a récemment été admis par la CEDH dans un arrêt du 17 octobre 2019 qui a validé la preuve par vidéosurveillance de salariés lorsque des éléments de fait préalables le justifiaient[544]. Dans le cas d'espèce, la CEDH réunie en Grande chambre a approuvé la possibilité de recourir à la vidéosurveillance de caissier de supermarchés sans qu'une information préalable leur soit portée. Précisément, elle a jugé que l'existence de soupçons raisonnables d'irrégularités graves et l'ampleur des manques constatés pouvaient justifier l'absence d'information préalable au placement sous vidéosurveillance de ces caissiers, et ne contrevenait pas à l'article 8 de la

[539] CA Paris, pôle 01, ch. 03, 15 mai 2019, n°18/26775.
[540] S. Guinchard, *Droit et pratique de la procédure civile. Droit interne et européen*, *op.cit.*, n°111.24.
[541] Cass. soc., 18 mars 2008, n°06-40.852, n°06-45.093, D. 2008. 2306, obs. M.-C. Amauger-Lattes, I. Desbarats, C. Dupouey-Dehan, B. Lardy-Pélissier, A. Pélissier et B. Reynès, D. 2008. 2820, obs. Delebecque, Bretzner et Vasseur, Procédures mai 2008. Comm. 137, p.14, note Perrot.
[542] Cass. soc., 22 mai 1995, n°93-44.078, Bull. civ. V, n°164, RTD civ. 1995. 862, obs. Hauser, RTD civ. 1996. 166, obs. Mestre, RTD civ. 1996. 197, obs. Gautier, BICC 1er juill. 1995, no 700, RJS 1995. 489, note Chauvy.
[543] CEDH, 24 avr. 1990, Série A, Kruslin et Huvig c/ France, Série A et B, n°176.
[544] CEDH, Grande chambre, 17 oct. 2019, aff. 1874/13 et 8567/13, Lopez Ribalda et autres c. Espagne.

CESDH. Cette décision qui interpelle pourrait très bien être étendue à des cas impliquant d'autres supports technologiques comme la *blockchain*, ce qui mettrait nécessairement à mal le principe de respect de la vie privée et par la même de loyauté dans le cadre de la constitution et de la production de preuve[545].

B. Les preuves *blockchains* illicites en matière pénale

222. Le contrôle de licéité de la preuve pénale passe par la conformité, d'une part, aux règles du Code pénal et d'autre part, aux principes généraux de la preuve pénale[546]. Pour être licite, la preuve ne doit pas être obtenue illégalement (1) et doit être loyale (2). D'autres preuves illicites comme celles obtenues au prix d'une auto-incrimination, celles qui violent le principe d'égalité des armes[547] ou des droits de la défense n'ayant pas nécessairement de lien avec les preuves *blockchains* ne seront pas ici traitées.

1. La preuve *blockchain* obtenue au prix d'une infraction pénale

223. En principe, une preuve obtenue au prix d'une infraction est illicite car elle est logiquement « *recevable dans le procès criminel qu'à la condition d'avoir été obtenue légalement* »[548]. La chambre commerciale a déclaré irrecevables les fichiers achetés par l'administration fiscale permettant d'identifier des fraudeurs alors qu'un vol de fichier de données clients d'une banque, dans le même temps, avait été déclaré suite à un accès dans un STAD[549]. Notons toutefois que la chambre criminelle a déjà considéré que le juge n'a pas le pouvoir de rejeter une preuve apportée par une partie au seul motif qu'elle aurait été illégalement obtenue[550].

[545] L. Costes, **«** Pas de violation du droit à la vie privée de caissières de supermarché espagnoles filmées à leur insu par des caméras de sécurité », Actualités du droit, oct. 2019.
[546] Confirmé par la décision : Crim. 8 janv. 2014, n°12- 88.326, D. 2014. 87. Voir aussi le concept de « *licéité de la preuve* » se divisant en théorie générale de la preuve et droit des preuves spéciales soutenu par E. Verges (E. Vergès, « Loyauté et licéité, deux apports majeurs à la théorie de la preuve pénale », *op.cit.*, p.408).
[547] C. pr. civ., art. 16.
[548] S. Guinchard, *Droit et pratique de la procédure civile. Droit interne et européen*, *op.cit.*, n°111.22.
[549] Cass. com., 31 janv. 2012, n°11-13097, Lexbase proc. fiscale fevr. 2012, com.
[550] Cass. crim. 15 juin 1993 : bull. crim., n°210 ; 6 avr. 1993, JCP 1993, II, 22144, note M.-L. Rassat.

224. À titre d'illustration, ne serait pas admise, la preuve d'une transaction obtenue par un individu issue de la mise en place d'un *malware* en vue de remplacer l'adresse publique utilisée par la partie à une transaction, par sa propre adresse afin de recevoir les crypto-actifs à transférer. Cette transaction serait ainsi obtenue au prix d'une infraction pénalement condamnée d'accès ou maintien frauduleux dans un STAD[551], suivi d'une modification de données contenues dans ce STAD[552]. Par exemple, le logiciel « *CryptoSchuffler* » a déjà permis à des cyber-délinquants ce genre de manipulation[553]. Dans le même sens, serait illicite la preuve d'une transaction en crypto-actifs qui tomberait sous le coup d'une infraction de blanchiment[554].

2. La preuve *blockchain* déloyale pénalement

225. Tout comme la loyauté en matière civile, le Code de procédure pénale n'emploie pas explicitement le terme de « *loyauté* ». L'article préliminaire du Code de procédure pénale précise que la « *procédure pénale doit être équitable et contradictoire et préserver l'équilibre des droits des parties* ». Seule la formule de serment du médiateur ou du délégué du procureur de la République fixée à l'article R.15-33-36 et R.53-38 indique, à propos de l'usage des moyens de télécommunication dans la procédure, qu'ils doivent « *assurer une retransmission fidèle, loyale et confidentielle à l'égard des tiers* ». Le principe de loyauté de la preuve est aussi retenu par la jurisprudence criminelle depuis les années 1990[555]. Ce principe général en matière pénale est donc un principe jurisprudentiel consacré par la chambre criminelle de manière informelle par les arrêts dit « *Wilson* » et « *Imber* » le 31 janvier 1888[556] et réellement né d'une décision de la chambre criminelle du 27 février 1996 relative à des provocations policières[557]. Depuis lors, il est reconnu comme « *standard classique* » de contrôle des preuves pénales

[551] C. pén., art. 323-1.
[552] C. pén., art. 311-1.
[553] B. Eschapasse, « Attention aux voleurs de crypto-monnaies », Le Point, 16 dec. 2017, http://www.lepoint.fr/economie/attention-aux-voleurs-de-crypto-monnaies-16-12-2017-2180508_28.php# (consulté le 31/05/2020).
[554] C. pén., art. 324-1.
[555] Cass. Crim., 27 févr. 1996 : *Bull. crim.* 1996, n°93 ; Cass. 2e civ., 7 oct. 2004 : *Bull. civ.* 2004, II, n°447 ; Cass. ass. plén., 7 janv. 2001, n°09-14.316, PBRI.
[556] Cass., ch. réun., 31 janv. 1888, S. 1889. 1. 241 : « *le juge V. a employé un procédé s'écartant des règles de la loyauté que doit observer toute information judiciaire* » ; Cass. crim. 12 juin 1952, S. 1954. 1. 69 : JCP 1952. II. 7241 : les stratagèmes avaient « *pour but et pour résultat d'éluder les dispositions légales et les règles générales de procédure* ».
[557] Crim. 27 févr. 1996, n °95- 81.366, Bull. crim. 93 ; D. 1996. 346, note C. Guéry ; RSC 1996. 689, obs. J.-P.Dintilhac : il était porté atteinte au « *principe de la loyauté des preuves* » lorsque les autorités publiques utilisaient un « *stratagème* », autrement dit, la « *machination de nature à déterminer les agissements délictueux* » qui avait eu pour effet de « *vicier la recherche et l'établissement de la vérité* ».

conduisant la doctrine à différencier au sein de ce standard la provocation à la preuve et la provocation à l'infraction[558].

226. S'agissant de la provocation à la preuve, la Cour de cassation a retenu que les preuves obtenues par un policier qui s'était fait passer pour un adolescent âgé de quatorze ans incitant le prétendu délinquant à transmettre des images pédopornographiques, avaient été acquises de façon déloyale et étaient par conséquent irrecevables[559]. Dans le cadre de la *blockchain*, si un agent de police incitait sur le *darknet* un individu à payer des produits stupéfiants illicites en crypto-actifs, cette preuve serait acquise de façon déloyale. Toujours est-il que, la mise en œuvre d'une provocation à la preuve ou à l'infraction pourrait se révéler laborieuse au sein du réseau *blockchain* en lui-même, lequel ne formant pas un réseau de messagerie. Elle pourrait toutefois être observée par alternance, à l'extérieur du réseau pour la phase de prise de contact avec un individu et, à l'intérieur du réseau pour la transaction.

Paragraphe 2 : La proportionnalité et nécessité de l'intérêt des preuves *blockchains* licites

227. La preuve *blockchain* est supposée revêtir un caractère proportionné si une atteinte est portée à un droit fondamental (A). Ce contrôle de proportionnalité est le plus généralement appliqué par la jurisprudence pour l'atteinte à la vie privée (B).

A. Une proportionnalité et nécessité au regard du droit à la preuve *blockchain*

228. Le droit « *à* » la preuve est retenu depuis 2006 par la CEDH[560] et entériné en 2012 par la Cour de cassation[561]. Ce droit n'autorise pas pour autant la production de preuves qui seraient attentatoires à un droit fondamental, sauf si elles s'avèrent proportionnées et nécessaires au but poursuivi et/ou aux intérêts en présence. La Cour de cassation adopte une méthode selon laquelle elle mesure la proportionnalité de l'atteinte à un droit par rapport à l'intérêt que pourrait

[558] E. Vergès, *Procédure pénale*, Lexis Nexis, 2011, n°111.
[559] Cass. crim., 11 mai 2006, n°05-84.837 : Gaz. Pal. n°23 2009, com. M. Prud'homme ; *op.cit.* n°363 2007, com. Y Monnet ; JCP E n°3 2007, com. M. Vivant, N. Mallet-Poujol, J.-M. Bruguière ; CCE n°1 2007, com. A. Lepage ; LJ n°299 2008 proc. prud'homale, obs. C. Radé ; Hebdo ed. privée proc. pén. n°710 2017, obs. P.Le Monnier.
[560] CEDH 10 oct. 2006, n°7508/02, L. L. c/ France, D. 2006. 2692 ; RTD civ. 2007. 95, obs. J. Hauser.
[561] Cass. 1re civ., 5 avr. 2012, n°11-14.177, Bull. civ. I, n°85, D. 2012. 1596, note G. Lardeux, 2826, obs. J.-D. Bretzner, 2013. 269, obs. N. Fricero, et 457, obs. E. Dreyer ; RTD civ. 2012. 506, obs. J. Hauser.

constituer la production d'une preuve[562]. Ce contrôle des juges de cassation, considéré comme casuel et factuel, est critiqué par une partie de la doctrine, jugé à la limite de son rôle de juge du droit[563]. Alors qu'un autre versant de la doctrine considère que le contrôle de proportionnalité devrait être étendu à tous les principes relatifs à la licéité de la preuve[564].

229. Une décision récente au fond avait écarté des débats des documents (informations relatives à la clientèle personnelle d'un collaborateur en l'espèce), sur le fondement de l'article 145 du Code de procédure civile, considérant que des mesures d'instructions devaient être ordonnées à la demande de l'intéressé pour obtenir des pièces qui ne lui appartenaient pas. Cependant, c'est au visa de l'article 6 de la CESDH que la Cour de cassation a reproché à la Cour d'appel de ne pas avoir recherché « *comme elle y était invitée, si la production litigieuse n'était pas indispensable à l'exercice du droit à la preuve et proportionnée aux intérêts antinomiques en présence* »[565].

230. Dans le cadre de la *blockchain*, les preuves obtenues par une partie issue du déchiffrement d'une adresse publique permettant d'obtenir l'identité de son titulaire (conservée par un prestataire, comme une plateforme d'échange de crypto-actifs soumis à l'obligation d'identification de ses clients), devront être soumises à un contrôle de proportionnalité systématique par les juges du fonds au regard de l'atteinte.

B. Une proportionnalité et nécessité appliquées pour arbitrer les conflits entre droit à la preuve et vie privée

231. Fréquentes sont les décisions contrôlant le droit au respect de la vie privée et sa difficile balance avec le droit à la preuve. Depuis une jurisprudence de principe de la première chambre civile de la Cour de cassation du 5 avril 2012, deux règles sont consacrées[566]. La première,

[562] Cass. 1ère civ., 16 oct. 2008 n°07-15.778 : RLDC n°144 2017, com. L. Rousvoal ; D.2009, obs. P.Delebecque, J.-D. Bretzner, T. Vasseur ; JCP G n°19 2009, obs. L. Cadier, S. Amrani-Mekki, T. Clay ; RTD Civ n°1 2009, com. R. Perrot ; CCE n°7 2009, com. A. Lepage ; LJ n°591 2014, obs. E. Vegès ; chr. proc. civ. n°506 2012 obs. E. Vegès ; *op.cit.* n°586 2014, obs. E. Vergès : « *caractériser la nécessité de la production litigieuse quant aux besoins de la défense et de proportionnalité au but recherché* ».
[563] A. Aynès, J.-D. Bretzner, « Droit de la preuve septembre 2016 – janvier 2017 », D.2017, p.263.
[564] E. Vergès. « Loyauté et licéité, deux apports majeurs à la théorie de la preuve pénale », *op.cit.*, p.623.
[565] Cass. 1ère civ., 5 juill. 2017, n°16-22.183, D. 2017.1479, D. avocats 2017. 321, obs. F. Naftalski et M. Mohajri.
[566] Cass. 1ère civ, 5 avr. 2012, n°11-14.177, D. 2012. 1596, note G. Lardeux, 2826, obs. J.-D. Bretzner, 2013. 269, obs. N. Fricero, et 457, obs. E. Dreyer ; RTD civ. 2012. 506, obs. J. Hauser. Cette solution est réaffirmée par un

devenue un principe, énnonce que le droit au respect de la vie privée ne tient pas en échec le droit à la preuve. La seconde exige, d'un côté, que l'accès à une pièce soit « *indispensable* » à l'exercice du droit à la preuve, et de l'autre, que la mesure prescrite soit « *proportionnée* » aux intérêts en présence.

232. La chambre civile de la Cour de cassation a déjà admis, entre autres, la preuve tirée des constatations d'un huissier ayant filmé une partie qui, victime d'un accident de la circulation, invoquait sa perte d'autonomie pour réclamer une provision. En l'espèce, la Cour a retenu que l'atteinte à la vie privée n'était pas disproportionnée par rapport aux droits et intérêts des parties et notamment de l'assureur[567]. Au contraire, un arrêt récent de la Cour d'Appel de Paris rappelle sur le fondement de l'article 9 du Code civil que « *le droit à la preuve ne peut justifier la production d'éléments portant atteinte à la vie privée d'une personne qu'à la condition que cette production soit indispensable à l'exercice de ce droit et que l'atteinte soit proportionnée au but poursuivi* ». Elle indique qu'en l'espèce la production de preuves portant sur des photos prises par drone avec une prise de vue aérienne d'une propriété privée sans l'accord des propriétaires « *constitue à l'évidence une atteinte à leur vie privée et ce même si elle n'en montre pas ses occupants* »[568]. De surcroît, elle ajoute que ces « *photographies ne sont nullement indispensables à l'exercice du droit de la preuve* ». Dans ce cas, l'atteinte issue de supports technologiques nouveaux était en conséquence disproportionnée par rapport à l'objectif poursuivi. Les preuves inhérentes à la *blockchain* ou résultant de celle-ci mettant en place des procédés de cryptographie très protecteurs de la vie privée, semblent justement être « *couvertes* » de ce type d'atteintes. En effet, le pseudonymat règne dans les *blockchains* publiques grâce à la signature qui ne dévoile pas l'identité directe d'un émetteur participant à la transaction mais uniquement sa clé publique[569]. Partant, ce cas de figure ne doit pas être exclu mais semble difficilement pouvoir se présenter.

233. Une décision précise l'appréciation du respect du principe de proportionnalité, indiquant que seule une analyse globale des moyens mis en œuvre par un plaideur pour accéder à un élément de preuve permet d'apprécier avec pertinence si le principe de proportionnalité a été

arrêt récent : Cass. 1ère civ, 25 févr. 2016, n°15-12.403, D. 2016. 884, note J.-C. Saint-Pau ; AJ pénal 2016. 326, obs. D. Aubert ; RTD civ. 2016. 320, obs. J. Hauser, et 371, obs. H. Barbier.

[567] Cass. 1ère civ., 31 oct. 2012, n°11-17.476, Bull. civ. I, n°224, JCP 2012. Actu. 1229, note Sabine Abravanel-Jolly.

[568] CA Paris, pôle 01, ch. 03, 15 mai 2019, n°18/26775.

[569] Voir *supra* n°133-134.

observé ou non. Cette appréciation doit prendre appui sur deux critères : l'ampleur et la durée des actions qui portent atteinte à la sphère de la vie privée. Le risque de violation de l'exigence de proportionnalité s'accroit si des moyens importants sont mobilisés dans l'atteinte à la vie privée et qu'elle subsiste dans le temps[570].

234. Il pourrait être admis qu'un explorateur de *blockchain*, prestataire qui trace des transactions dans les *blockchains* publiques de manière continue, soit considéré comme portant atteinte à la vie privée. A supposer que cet outil permette d'aboutir à l'extraction des comportements d'achat d'un participant à la *blockchain* qui paye en crypto-monnaies, cette atteinte pourrait être qualifiée. Néanmoins, elle serait proportionnée à l'objectif poursuivi de droit à la preuve, ne portant pas sur des éléments particulièrement intimes. Par exemple, le rapport d'un détective privé qui rendait compte de l'activité d'une personne au balcon de son domicile a été considéré comme une atteinte proportionnée à la vie privée. Ce sont précisément les photos de ce rapport, pièces destinées à démontrer que la personne observée ne souffrait d'aucun trouble de la vision, contrairement à ce qu'elle affirmait, qui ont permis de déterminer le caractère proportionné[571]. Les juges de cassation ont estimé que l'atteinte portée au droit au respect de la vie privée, si elle était bien réelle, n'en était pas moins proportionnée eu égard au droit à la preuve. En effet, il était seulement rapporté que la personne ne portait pas de lunettes pour conduire, faire le ménage, et conséquemment, cela ne concernait pas des éléments particulièrement intimes.

[570] Cass. 1ère civ, 25 févr. 2016, n°15-12.403, D. 2016. 2535, obs. Bretzer et A. Aynès.
[571] Cass. 1re civ., 10 sept. 2014, n°13-22.612, D. 2014. 1824, D.2014. 167, obs. J.-D. Bretzner et A. Aynès, 2015. 342, obs. E. Dreyer ; RTD civ. 2014. 856, obs. J. Hauser.

CONCLUSION DE LA PARTIE PRELIMINAIRE

235. Cette partie préliminaire visait à proposer des bases techniques et juridiques nécessaires aux développements à venir de l'étude.

236. **Préalables techniques.** Par un cheminement intellectuel de conceptualisation[572], plusieurs classifications techniques des preuves *blockchains* ont été proposées en fonction du support des preuves étudiées (signature *blockchain*, horodatage *blockchain* et empreinte *blockchain*) et de leur objet (selon la nature des données : transactionnelles ou complémentaires ; la provenance des données : ajoutées volontairement par un sujet de droit ou générées par la *blockchain*, et les modalités d'ajout des données : ancrées, inscrites ou enregistrées).

237. **Préalables juridiques.** Si l'application des règles de droit international privé aux preuves *blockchains* est flexible, elle trouve difficilement des réponses tranchées et reste encore au stade de la réflexion embryonnaire. Par ailleurs, les préalables juridiques d'admissibilité et de recevabilité se voient quant à eux ajustés aisément aux spécificités des preuves numériques distribuées.

238. **Droit international privé applicable aux preuves *blockchains*.** Dans l'hypothèse d'un conflit de loi des preuves *blockchains*, des règles de rattachement peuvent être retenues pour connaître le droit applicable. S'agissant de l'administration de la preuve, la *lex fori* ou loi du tribunal s'appliquerait et pourront être envisagées alternativement la loi du lieu de l'acte et celle applicable au fond d'un acte. L'application de la loi du for pour les conditions matérielles pourra poser des difficultés particulières, avec le langage informatique, le hachage et le chiffrement. Seul un rapport d'expert pourrait à ce stade permettre d'expliciter les preuves *blockchains*. Pour les cas où certaines preuves *blockchains* seront qualifiées d'écrits électroniques, il conviendra de vérifier au cas par cas si la loi du *for* ou la loi qui en régit la forme trouve à s'appliquer. En

[572] Pour E. Verges : la conceptualisation est une « (…) *tâche ardue et généralement vouée à la critique. Mais elle est indispensable, dans la mesure où les concepts permettent de définir des catégories juridiques et les régimes juridiques qui y sont associés* » (E. Verges, « Eléments pour un renouvellement de la théorie de la preuve en droit privé », *op.cit.*, p.853).

matière de fait, l'application à la fois de la loi du for comme de la loi du fond apparaissent couvrir cette situation ; étant précisé que les lois concordent souvent vers le régime de la liberté de la preuve. Puis, la force probante d'un acte constaté ou constitué par la *blockchain* se verra aussi appliquer la loi du *for* mais la jurisprudence pourrait accepter l'application de la loi du lieu de l'acte. Alternativement enfin, la loi du fond de l'acte dans une *blockchain* privée ou publique permissionnée pourra être déterminée par contrat.

S'agissant par ailleurs de l'objet de la preuve, le fond du droit déterminera les conditions d'existence des preuves *blockchains* (lorsqu'il est établi) ; ce pourquoi la *lex causa* trouvera à s'appliquer.

S'agissant enfin de la charge de la preuve, l'acteur qui portera le fardeau de la preuve *blockchain* sera déterminé par la *lex contractus* ou loi du contrat ou la *lex loci protectionis*, soit la loi du pays de protection d'un droit de propriété intellectuelle.

239. **Légalité des preuves *blockchains*.** Pour que les preuves *blockchains* soient admises, des règles de droit de la preuve devront être respectées par les preuves *blockchains*. En matière de faits enregistrés dans la *blockchain*, pénale (précisément pour le *crypto-jacking*, le *ransomware* de crypto-actifs, l'installation de *malware*, le vol de clés, le *phishing* ou encore l'escroquerie à l'investissement) et commerciale, les preuves pourront être apportées par tous moyens. Pour les preuves légales, soit certaines inscriptions dans la *blockchain*, le respect des exigences des modes de preuve sera nécessaire.

240. **Licéité des preuves *blockchains*.** Aussi, le respect par les preuves *blockchains* des principes fondamentaux du procès seront indispensables sous peine de se voir écartées par le juge. En matière civile, les preuves *blockchains* obtenues de façon déloyale, comme celles apportées par un huissier de justice non-indépendant, les atteintes à la confidentialité (violation du secret par des notaires ou encore bancaire au regard des nombreuses *blockchains* déployées dans ces secteurs), et à la vie privée avec des données publiées en clair dans la *blockchain* (même si le hachage devrait minimiser ces risques) seront irrecevables. En matière pénale, sous peine également d'irrecevabilité, les preuves *blockchains* ne devront pas être obtenues au prix de l'une des infractions pénales précitées ou d'une provocation à la preuve et à l'infraction sur le *darkweb* (pour la phase de prise de contact avec un individu) et, à l'intérieur du réseau de la *blockchain* (pour la phase de transaction).

241. Les preuves *blockchains* feront l'objet d'un contrôle de proportionnalité de l'atteinte portée par la preuve à un droit fondamental, notamment à la vie privée, somme toute limité par le chiffrement prévu dans le cadre des *blockchains*.

242. L'ensemble de ces préalables techniques et juridiques sera utile tantôt à l'assimilation ou à la consécration de notions, catégories et régimes juridiques pour les preuves *blockchains*, tantôt à l'appréhension de ces preuves par le juge.

PARTIE 1

LE CADRE JURIDIQUE REQUIS AU SOUTIEN DE LA TRADUCTION DE LA « *VERITE CRYPTOGRAPHIQUE* » DES DONNEES ENREGISTREES DANS LA *BLOCKCHAIN*

243. La *blockchain* et ses preuves ne sont pas « *a-légales* » ou des « *forces de la nature* » bâtissant une « *forteresse technique* »[573] impénétrable par le droit, comme des technophiles ont pu le formuler[574]. Il est régulièrement avancé que les transactions effectuées grâce à une *blockchain* n'ont de valeur que celle que les acteurs, parties prenantes à cette *blockchain*, souhaitent leur donner mais qu'elles n'auraient pas pour autant de valeur juridique[575]. Si l'existence même du droit est idéologiquement remise en cause dans le cadre de cette technologie, il semble que la « *zone grise blockchain* » puisse et doive faire l'objet d'application de normes, à la fois pour servir utilement le droit de la preuve dans l'objectif de révéler la vérité cryptographique, et pour rendre efficace ces preuves en pratique au bénéfice des acteurs de celles-ci.

244. Avant d'envisager toute loi spécifique pour cette zone juridiquement incertaine induisant un cadre nouveau, il convient dès lors de déterminer avec rationalité si nos mécanismes et règles existants sont adaptés à ce nouveau sujet technologique. Comme l'a souligné le Ministère de la Justice dans une réponse à une question écrite posée par le député Daniel Fasquelle « *en matière probatoire, si aucun texte juridique ne mentionne spécifiquement la blockchain, il n'en résulte pour autant aucun vide juridique* »[576]. La *blockchain* doit alors se « *mouler* » aux contraintes imposées par l'ordre public[577]. Au prisme du droit commun existant, une étape de qualification juridique de la preuve des données enregistrées dans la *blockchain* devra être réalisée (titre 1) puisque tout cheminement juridique en vue de l'appréhension d'un sujet nouveau amène à cette opération intellectuelle de qualification. Elle constituera un préalable à la déduction et l'établissement de régimes juridiques adaptés (titre 2). L'objectif poursuivi par ce titre n'est pas tant d'étayer toutes les potentialités offertes par la technologie au soutien de la preuve juridique mais d'appréhender les preuves cryptographiques de la *blockchain* pour en éprouver un cadre juridique généralisé. Les linéaments projetés de ces preuves cryptographiques en droit impliqueront de polariser cette partie sur les *blockchains* publiques. Celles-ci, remises dans leurs environnements pratiques, peuvent faire l'objet d'observations généralisées, contrairement aux blockchains privées qui changent davantage en

[573] T. Schrepel, « Anarchy, State, and *Blockchain* Utopia: Rule of Law Versus Lex Cryptographia », *in* General Principles and Digitalisation (chapitre 15), Libraire SSRN, 12 nov. 2019, p.353.
[574] G. Wood (co-founder and chief technologic officer of Ethereum), CoinScrum and Proof of Work : Tools for the future, Youtube, dec. 2014, https://www.youtube.com/watch?v=WdgQI6CA4-E (consulté le 31/05/2020).
[575] B. Barraud, « Les *blockchains* et le droit », RLDI n°147, avr. 2018, p.48-62.
[576] Question écrite n°22103 de D. Fasquelle, publiée au JO le 30/07/2019, réponse du Ministère de la Justice publiée au JO le 10/12/2019, p.10774. Voir annexe n°10.
[577] V. Magnier, « Enjeux de la *blockchain* en matière de propriété intellectuelle et articulation avec les principes généraux de la preuve », Dossier *Blockchain* et preuve, Dalloz IP/IT n°2, févr. 2019, p.78.

fonction des règles que l'on souhaite appliquer à chaque projet informatique et qui sont souvent solutionnées en droit par des conventions.

TITRE 1

LES QUALIFICATIONS JURIDIQUES APPLICABLES AUX PREUVES DE DONNEES ENREGISTREES DANS LA *BLOCKCHAIN*

246. Si l'essentiel de la démarche de ce titre ne consistera pas à remettre en cause l'ensemble de l'ordonnancement actuel de la preuve, celle-ci aura pour but de déceler les catégories auxquelles les preuves *blockchains* peuvent prétendre en l'état du droit positif[578]. Cette approche d'équivalence fonctionnelle de la preuve reposera sur l'absence de distinction du support de la preuve (tangible ou numérique). Elle consistera avant tout à s'attacher à la fonctionnalité de la preuve et non à sa matérialité. Si les preuves *blockchains* remplissent les mêmes fonctions que certaines preuves actuellement encadrées par le droit commun, alors elles pourront disposer de la même valeur. Par analogie et assimilation aux catégories juridiques de droit commun, il est possible de décomposer les preuves existantes dans la *blockchain* pour en trouver des qualifications. Les qualifications juridiques de droit commun peuvent dans ce cas tenter de régler les instruments probatoires de la *blockchain* selon deux angles : concernant les preuves de données sur les transactions elles-mêmes, c'est-à-dire sur leur apparence et concernant les preuves de données dans les transactions, c'est-à-dire dans leur substance. En ce sens, ces angles de vue seront développés par des qualifications juridiques de droit commun de la preuve envisagées pour les preuves de données transactionnelles d'une part (chapitre 1), et pour les données complémentaires d'autre part (chapitre 2).

[578] Cette démarche est préconisée par le législateur qui recommande de « *dresser un état des (...) sur la capacité du droit national à appréhender pleinement les enjeux qui entourent les usages possibles de cette technologie » avant d'envisager de légiférer* » (Assemblée nationale, Rapport d'information n°1501, *op.cit.*, p.66).

CHAPITRE 1

LES QUALIFICATIONS JURIDIQUES DE DROIT COMMUN ENVISAGEES POUR LES PREUVES DE DONNEES TRANSACTIONNELLES ENREGISTREES DANS LA *BLOCKCHAIN*

247. Un registre *blockchain* quelconque regroupe des transactions générant un ensemble de données relatives à ces transactions[579]. Ce sont les transactions elles-mêmes du registre qui seront précisément étudiées pour en trouver des qualifications juridiques de droit commun (section 1), puis les données signées dans le registre de la *blockchain* (section 2) et enfin celles horodatées (section 3).

Section 1 : Les qualifications juridiques de droit commun envisagées pour les transactions du registre de la *blockchain*

248. Deux approches du registre de transactions d'une *blockchain* peuvent être affichées, une conception substantielle du registre de la *blockchain* consistant à qualifier le contenu du registre en la représentation de ses transactions ou une conception structurelle qui implique la qualification du contenant même du registre, son squelette. Les développements de cette section vont essentiellement se concentrer sur la conception substantielle du registre de transactions, lesquelles pourraient être concrètement apportées comme preuve lors d'un litige au succès des prétentions d'une partie. Cette approche utilitariste a pour ambition de déduire la valeur probatoire effective des transactions du registre d'une *blockchain*. *In limine,* la qualification des transactions en tant que telle nécessite une qualification générale comme un ensemble de documents (paragraphe préalable) et des qualifications en détail des différentes transactions observées : simples ou complexes.

[579] Voir *supra* n°39-40.

249. Ces dernières qualifications impliquent un rattachement déterminant à la catégorie des actes ou des faits juridiques[580]. La faculté de se ménager une preuve écrite des actes juridiques explique la rigueur dans l'interdiction par la loi de prouver les actes par un procédé imparfait jugé comme dangereux. *A contrario*, il ne pourrait être exigé de celui qui invoque un fait juridique qu'il apporte la preuve écrite de ce dernier, évènement qui survient soudainement échappant à toutes prévisions[581]. La loi accepte donc, dans ces cas, les procédés de preuve parfaits, admissibles dans toutes matières ainsi que les procédés de preuve imparfaits[582].

250. Une transaction enregistrée dans la *blockchain* est plus ou moins technique intervenant manuellement ou automatiquement (par un *smart contract*). Partant, elle peut être qualifiée différemment selon qu'elle représente une « *transaction simple* » ou une « *transaction complexe* », rattachée à des catégories dissemblables et ainsi se voir appliquer des règles de preuve différentes. La « *transaction simple* » suppose un échange de crypto-monnaies (achat et vente). Elle pourrait être qualifiée de simple paiement (paragraphe 1) emportant logiquement la constatation d'un fait juridique par la *blockchain*. Cette transaction d'un émetteur à un destinataire a pour finalité un unique transfert de crypto-monnaies. Traditionnellement, cette transaction implique simplement l'achat et la vente de crypto-monnaies, elle se complexifie dès lors que l'on y opère une action supplémentaire. La « *transaction complexe* », quant à elle, est une transaction n'impliquant pas qu'un simple flux financier mais l'ajout de l'exécution d'une condition préalablement établie par un *smart contract* ou l'inscription d'un jeton entrainant le transfert de ce bien incorporel. Cette dernière inscription pourrait s'apparenter à un enregistrement dans la blockchain d'un acte établi à l'éxtérieur de cette technologie produisant des conséquences juridiques, c'est-à-dire un acte juridique. Elle nécessite alors de retenir une qualification différente : celle du commencement de preuve (paragraphe 2).

Paragraphe préalable : Les transactions du registre d'une *blockchain* : une reconnaissance internationale et européenne

[580] Voir *supra* n°192-208 en partie préliminaire.
[581] H., L., J. Mazeaud, F. Chabas, Leçons de droit civil, *Introduction à l'étude du droit*, *op.cit.*, n°390.
[582] Cass. civ. 3e, 2 oct. 1996 : JCP G 1996, IV, 2238 : au sujet d'une dégradation imputable à un locataire ; Cass. 1ère civ., 20 déc., 1993 : Bul. Civ. I, 377 : au sujet de la preuve d'une possession d'état.

251. **Les transactions du registre comme informations et documents électroniques au sens du droit européen ou international.** Les transactions du registre de la *blockchain* peuvent substantiellement constituer un ensemble d'informations et de documents électroniques reconnus par le droit européen ou international[583].

252. **L'information sous forme de message de données.** En droit commercial international, le message de données désigne une « *information créée, envoyée, reçue ou conservée par des moyens électroniques ou optiques ou des moyens analogues, notamment, mais non exclusivement, l'échange de données informatisées (EDI), la messagerie électronique, le télégraphe, le télex et la télécopie* »[584]. L'article 5 de la loi type de la CNUDCI sur le commerce électronique de 1996[585] précise que « *l'effet juridique, la validité ou la force exécutoire d'une information ne sont pas déniés au seul motif que cette information est sous forme de message de données* ». L'emploi généraliste de la notion d'« *information* » au soutien de la reconnaissance juridique de messages de données s'applique à une multitude de cas et pourrait faire référence au contenu échangé entre deux protagonistes. La transmission d'information est symptomatique des transactions de la *blockchain* qui visent à échanger de la valeur et d'autres données par un message, une transaction entre deux participants.

253. **Les documents électroniques.** La loi type de la CNUDCI sur les documents transférables électroniques de 2018[586] offre un résultat plus large en faisant référence aux documents électroniques en son article 7, 1 qui indique que « *le document transférable électronique n'est pas privé de ses effets juridiques, de sa validité ou de sa force exécutoire au seul motif qu'il se présente sous une forme électronique* ». Le document renvoie à un écrit, un ensemble formé par un support et à l'information, le contenu correspondant[587]. Le règlement eIDAS, dans son article 3.35 définit, quant à lui, le document électronique uniquement sous le prisme du contenu, à savoir comme un « *contenu conservé sous forme électronique* ».

254. Le contenu en sa représentation des transactions et données répertoriées et agencées logiquement par ordre chronologique dans le registre de la *blockchain* est un contenu et non un

[583] Avis partagé par : T. Douville, « *blockchains* et preuve », D.2018, 22 nov. 2018, p.219 ; T. Douville, « *Blockchains* et droit international privé : état sommaire des questions », *op.cit.*, p.385.
[584] Loi type CNUDCI sur le commerce électronique, 1996, art. 2 ; Voir aussi la définition similaire de message de données dans : CNUDCI, Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux, 2005, art. 4, c.
[585] Loi type CNUDCI sur le commerce électronique, 1996.
[586] Loi type CNUDCI sur les documents transférables électroniques, 2017.
[587] G. Cornu, *Vocabulaire juridique*, *op.cit.*, Voir document sens n°1, p.365.

simple contenant. Notons pour rappel que seul le contenu suivant des données dites transactionnelles seront disponibles dans un registre de *blockchain* publique : identifiants de transaction, crypto-monnaies échangées, adresses publiques à l'initiative de transaction, dates et heures de ces transactions, voire d'autres données complémentaires (développées ci-après). Les transactions sont donc des informations au contenu modeste et limité contrairement à une grande base de données centralisée agrégeant des documents et autres contenus. Le registre lui est le support de ces transactions. L'ensemble du registre et de ses transactions ne résistent donc pas à la qualification de document électronique. Au sens de la loi type de la CNUDCI et du règlement eIDAS, les transactions du registre de la *blockchain* peuvent ainsi correspondre aux qualifications plus précises de documents électroniques.

255. Si elles sont qualifiées comme telles, les transactions ne pourront être refusées au simple motif qu'elles sont de nature électronique en vertu du principe de non-discrimination de la loi type de la CNUDCI sur les documents électroniques et du règlement eIDAS. Selon ce principe, l'admissibilité des effets et la recevabilité d'un document électronique comme preuve en justice ne peuvent être refusés au seul motif que ce document se présente sous une forme électronique[588]. Cette qualification conforte le rayonnement international et européen de la portée (plein effet juridique, validité, force exécutoire et recevabilité en justice) des documents électroniques constitués par l'ensemble des transactions du registre de la *blockchain*. L'*European Blockchain Observatory and Forum* est enclin à accueillir favorablement cette qualification de document électronique confirmant « *la possible qualité juridique des données contenues dans un registre blockchain* »[589].

256. **Les interrogations des transactions du registre comme des écrits électroniques au sens du droit français.** En droit français, l'écrit est *« une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quel que soit leur support* » selon son article 1365 du Code civil. Souvent critiquée, la définition retenue pour « *la reine des preuves* » laisse planer le doute sur la nature de documents qui ne présenteraient pas les garanties de l'acte sous signature privée papier ou électronique[590], par exemple les

[588] Règl. eIDAS, art. 46.
[589] EU Blockchain Observatory and Forum, Legal and regulatory framework of *blockchains* and smart contracts, *op.cit.*, p.12. Voir aussi : EU blockchain Observatory and Forum, Blockchain and digital identity, le 2 mai 2019, p.21.
[590] E. Vergès, « La réforme du droit de la preuve civile : enjeux et écueils d'une occasion à ne pas manquer *op.cit.*, p.623.

courriels[591], télécopies[592], documents faisant apparaître une signature scannée[593]. La question se pose tout autant pour la transaction d'une *blockchain* qui ne semble pas être dotée d'une signification intelligible, de prime abord, alors même qu'elle est représentée d'un identifiant de transaction correspondant à une suite de lettres et de chiffres. Lorsqu'il est électronique, l'écrit doit répondre à des conditions particulières d'identification de la personne dont il émane et d'établissement et de conservation de nature à en garantir l'intégrité[594]. La problématique de l'identification dans la *blockchain* est latente, ce qui a tendance à compromettre la qualification d'écrit électronique pour les transactions de la *blockchain*[595]. L'intégrité des données garantie par l'immuabilité du registre qui trouve sa justification technique par l'empreinte numérique des blocs de transactions est néanmoins satisfaite[596]. En définitive, le droit français ne semble pas pouvoir trouver d'issue favorable à la qualification des transactions comme des écrits électroniques.

257. Faute de réponse satisfaisante en droit interne, le droit international et européen prendront naturellement leur place dans la reconnaissance des transactions du registre d'une *blockchain* comme des flux juridiquement identifiés.

Paragraphe 1 : La qualification appropriée de paiement pour les « *transactions simples* »

258. La qualification de paiement des transactions simples est la plus vraisemblable (A) et celle-ci aura pour conséquence l'application du principe de liberté de la preuve (B). Si l'on en juge cette proposition, toute preuve pourra ainsi être apportée.

[591] L'e-mail ne serait pas un écrit selon la jurisprudence : Cass. 1ère civ. 30 sept. 2010, n°09-68-555, D.2010. 2362 ; AJDI 2011, 73, obs. F. de la Vaissière ; RTD civ. 2010, 785, obs. B. Fages. Il ne serait qu'un simple commencement de preuve par écrit : Cass. 1ère civ., 20 mai 2010, 09-65.854 ; CA Versailles, 16e ch., 8 nov. 2012, n°12/00118 ; CA Lyon, 1e ch. civ. b, 6 févr. 2018, n°16-09379 ; CA Riom, 1e ch., 19 nov. 2018, n°17/00837.
[592] La télécopie serait assimilée à un écrit selon la jurisprudence : Cass. com. 2 dec. 1997, n°95-14. 251, D. 1998. 192, note. D. R. Martin ; RTD. com. 1998. 187, obs. M. Cabrillac ; JCP 1998. II. 10097, note L. Grynbaum.
[593] L'acte de prêt dont la signature est scannée est valide. La signature scannée peut ici en principe conférer à l'écrit la qualité de preuve littérale : CA Aix-en-Provence, ch. 8 B, 27 avr. 2017, n°2017/96 : Com. com. élec. 2017, com. E. Caprioli. Ce postulat est remis en question pour les actes de procédure judiciaire et administrative : CA Besançon, ch. soc., 20 oct. 2000, n°99/0834 : JCP G 2001, II, 10606 ; Defrénois 2002, 1394, obs. A. Raynouard ; Cass. 3e civ., 30 avr. 2003, n°00-46.467 : Bull. civ. III, n°118.
[594] C. civ., art. 1366.
[595] Voir les développements n°291-295 et s. sur l'identification consacrée à la signature.
[596] Voir *supra* n°137.

A. La qualification opportune de paiement des transactions simples

259. **La notion juridique large de paiement.** Dans le langage courant, le paiement est entendu restrictivement dans le sens où il est défini comme le versement d'une somme d'argent en exécution d'une obligation de somme d'argent[597]. Alors que juridiquement, il est conçu d'une façon large, comme toute prestation éteignant une dette, c'est une exécution d'une obligation quel que soit l'objet de celle-ci[598]. C'est le premier alinéa de l'article 1342 du Code civil qui prévoit le paiement comme « *l'exécution volontaire de la prestation due* ». Le paiement se déroule entre deux acteurs : un *solvens* et un *accipiens*. Le *solvens* représente la personne effectuant le paiement (souvent le débiteur lui-même, ou son représentant). Il est toutefois admis que le paiement puisse même être réalisé par une personne qui n'y est pas tenue, sauf refus légitime du créancier[599]. L'*accipiens* quant à lui est la personne qui reçoit le paiement. Le paiement est effectivement adressé au créancier ou à toute personne désignée pour le recevoir[600]. Cependant, le paiement fait de bonne foi à un créancier apparent est valable[601].

260. **Le paiement d'une transaction simple.** La transaction simple *blockchain*, autrement dit, l'achat ou la vente de jetons ou crypto-monnaies répondant aux notions visées par l'article L54-10-1, 1° et 2° du Code monétaire et financier susmentionnées, correspond à l'exécution d'une obligation de payer des jetons ou crypto-monnaies qui est de nature, pour ce débiteur, à éteindre sa dette envers le créancier à qui il a commandé ces jetons ou crypto-monnaies. L'émetteur et le destinataire d'une transaction sur la *blockchain* seront de fait considérés comme respectivement un *solvens*, le débiteur d'une obligation de payer la souscription des jetons et crypto-monnaies, et un *accipiens*, le créancier qui reçoit ce paiement. Force est de conclure qu'il n'est pas déraisonnable de retenir la qualification de paiement pour la transaction simple, ce qui a une incidence directe sur la façon de le prouver.

[597] G. Cornu, *Vocabulaire juridique*, *op.cit.*, Voir paiement sens n°1, p.730.
[598] G. Cornu, *Vocabulaire juridique*, *op.cit.*, Voir paiement sens n°2, p.730.
[599] C. civ., art. 1342-1.
[600] Fiches d'orientation, Paiement, Dalloz avocats, déc. 2019.
[601] C. civ., art. 1342-3.

B. La liberté de la preuve des transactions simples

261. **La preuve du paiement apportée par tout moyen.** Le paiement réalisé par une transaction simple dans la *blockchain* est un fait juridique constaté dans le registre de la *blockchain*[602]. L'article 1342-8 du Code civil précise que la preuve du paiement peut être apportée par tout moyen. Ce nouvel article introduit par la réforme du droit des contrats confirme les jurisprudences antérieures qui indiquaient - en l'absence de disposition légale - que le paiement était un fait juridique et qu'il se prouvait par tout moyen[603]. Une transaction simple pourrait par voie de conséquence être apportée par tout moyen, particulièrement par la copie du registre constituant l'ensemble des transactions de la *blockchain* en cause. La solution mathématique peu orthodoxe développée par les cryptographes du premier protocole Bitcoin avait justement le mérite de répertorier l'ensemble des transactions effectuées en bitcoin, selon un ordonnancement chronologique et sans possibilité de les altérer. La force mathématique de l'immuabilité du registre de transactions généré et sécurisé par l'ensemble des moyens cryptographiques mentionnés sera de nature à constituer une preuve particulièrement convaincante, une preuve « *gravée cryptographiquement* ». Pour autant, elle sera conditionnée aux arguments du plaideur pour justifier de la fiabilité suffisante du protocole du cas d'espèce.

262. **Le cas de la créance constatée dans un acte sous signature privée.** La preuve de paiement d'une créance constatée dans un acte sous signature privée nécessite encore toutefois la remise de cet acte par le créancier au débiteur qui fait ainsi présumer le paiement[604]. Dans ce cas, si un contrat prévoit le paiement en bitcoin pour éteindre une créance, il conviendra que le paiement soit prouvé par ce contrat, le registre *blockchain* seul indiquant la transaction ne suffira pas.

263. **Le cas du paiement de l'indu.** Un paiement de l'indu pourra également être prouvé par tout moyen. Celui qui aura réalisé un paiement indu, par erreur, pourra obliger celui qui a reçu

---

[602] Voir *supra* n°196.

[603] Cass. civ. 3e, 23 nov. 2017, n°16-17. 764, Dalloz actualité, 19 janv. 2018, obs. Ghiglino. Cette décision est cependant le fruit de nombreuses réflexions doctrinales (P. Catala, *La nature juridique du paiement*, thèse Paris, 1961, note au JCP 1966. II. 14841) et d'un revirement jurisprudentiel récent. Décisions antérieures en sens contraire : Cass. 1ère Civ., 15 déc. 1982, Bull. civ. I, n°365 ; Cass. 3ème civ., 10 mars 1993, n°91-14.781, Bull. civ. III, n°33, JCP N 1994. II. 25, note Leveneur, RTD civ. 1993. 827, note Mestre ; Cass. 1ère civ., 19 mars 2002, n°98-23.083, D. 2002. IR 1324. Décisions récentes confirmant l'actuelle position : Cass. 1ère civ., 6 juill. 2004, n°01-14.618, Bull. civ. I, n°20 ; Cass. 3ème civ., 27 févr . 2008, n°07-10.222, Bull. civ. III, n°35, D. 2008. Chron. 2820, obs. Delebecque ; Cass. 1ère civ., 16 sept. 2010, n°09-13.947, Bull. civ. I, n°173, D. 2010. 2671, obs. Delebecque, D. 2011. 622, obs. Creton, RDC 2011/1, p.103, note Libchaber, RLDC 2010, n°3992.

[604] R. Cabrillac, *Droit des obligations*, 6e éd, Cours, Dalloz, 2004, n°445 et 446, p.299.

le paiement à le lui rembourser par l'action de répétition de l'indu[605]. L'erreur d'un versement de crypto-actifs suite à une faute dans le report de l'adresse publique du destinataire de la transaction, pourra être apportée librement par tout moyen au soutien de la preuve de la transaction. Le registre de transactions pourrait à cet effet - à l'image de la preuve du paiement dû - faire office de preuve du paiement indu.

Paragraphe 2 : La qualification appropriée de commencement de preuve par écrit pour les « *transactions complexes* »

264. Les développements sur les transactions complexes doivent exclure d'une part, certaines qualifications inopportunes, soit celles des preuves écrites parfaites d'acte authentique (A) et d'acte sous signature privée (B). Ils doivent inclure d'autre part, la qualification d'écrit imparfait à laquelle pourra prétendre le participant à une transaction complexe : le commencement de preuve par écrit (C).

A. Le rejet de la qualification d'acte authentique pour une transaction complexe

265. Si la terminologie des notions d'« *authentique* », d' « *authenticité* » et d'« *authentification* », - souvent source de confusion dans le cadre de la technologie *blockchain* - a une importance capitale pour les développements sur les transactions complexes, elle sera aussi majeure dans le titre 2 sur les régimes des données enregistrées dans la *blockchain*. Revenons sans plus tarder sur ces fondamentaux terminologiques formants une base indispensable à l'étude.

266. La notion d'« *authentique* » peut recouvrir deux réalités et ainsi avoir deux sens. La notion d'authentique au sens de celui qui a véritablement l'auteur ou l'origine qu'on lui attribue[606] et authentique - réservée aux développements ci-dessous quant aux transactions complexes - qui « *se dit techniquement, par opposition à l'acte sous seing privé, de l'acte qui, étant reçu ou dressé par un officier public compétent, selon les formalités requises (sur papier ou support électronique), fait foi par lui-même jusqu'à inscription de faux* »[607]. Ce second sens

[605] C. civ., art. 1302.
[606] G. Cornu, *Vocabulaire juridique*, *op.cit.*, Voir authentique sens n°1, p.106.
[607] G. Cornu, *Vocabulaire juridique*, *op.cit.*, Voir authentique sens n°2, p.106.

d'authentique renvoie au support de l'acte authentique qui est « *celui qui a été reçu, avec les solennités requises, par un officier public ayant compétence et qualité pour instrumenter* »[608] et peut désormais être dressé électroniquement[609], s'il est établi et conservé sous certaines conditions fixées par deux décrets du 10 août 2005[610]. Résultat de nombreuses réflexions doctrinales[611], l'authentification d'acte notarié (voir la définition ci-après de cette action de rendre authentique) sur support papier ou électronique est depuis lors indifférente.

267. Cette notion d'« *authentique* » est proche de l'« *authenticité* » qui elle, relève de la qualité de l'objet ou du document dont l'auteur ou l'origine sont attestés, notamment sur la foi d'un certificat. Selon une deuxième conception, l'authenticité vise la qualité dont est revêtue un acte du fait qu'il soit reçu ou, au moins, dressé par un officier public compétent, suivant les solennités requises. Cette dernière conception, qui fera l'objet des analyses ci-après sur les transactions complexes, est une définition substantielle de l'authenticité[612]. Des actes authentiques de deux types peuvent être établis : des actes authentiques de droit public par certains fonctionnaires (préfets, sous-préfets, maires et adjoints, agents de police judiciaire) dans l'exercice de leurs fonctions pour conférer authenticité aux actes qu'ils élaborent et des actes authentiques de droit privé comme les décisions judiciaires, les rapports d'expertises, les actes d'huissiers, les sentences arbitrales[613]. Les actes authentiques les plus nombreux et importants sont les actes notariés dont la rédaction résulte d'un monopole conféré aux notaires

[608] C. civ., art. 1369, al. 1.
[609] C. civ., art. 1369, al. 2. Voir une critique du régime de l'acte authentique électronique introduit par la loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique et le décret n°2005-973 du 10 août 2005 : L. Grynbaum, « Loi du 13 mars 2000 : la consécration de l'écrit et de la preuve électroniques au prix de la chute de l'acte authentique », Commun. Comm. Elec., avr. 2000, p.12.
[610] Décret n°2005-973 du 10 août 2005 modifiant le décret n°71-941 du 26 novembre 1971 relatif aux actes établis par les notaires ; Décret n°2005-972 du 10 août 2005 modifiant le décret n°56-222 du 29 février 1956 pris pour l'application de l'ordonnance du 2 novembre 1945 relative au statut des huissiers de justice.
[611] Rapport l'authenticité. Droit, histoire, philosophie, ss. Dir. L. Aynès, la documentation française, 2e ed., janv. 2014 : « *l'absence d'influence du support électronique sur le concept d'authenticité. Qu'il instrumente sur une feuille de papier ou sur son ordinateur, le notaire procède toujours de la même manière. Il est tenu aux mêmes exigences de rédaction, au respect des mêmes solennités et aux mêmes vérifications de droit et de fait. Il n'y a aucune concession par rapport aux contraintes classiques de l'authenticité* » ; F. Perrotin, « l'authenticité à l'heure du numérique », LPA, 30 avr. 2015, p.9-11 ; M. Mekki, « retour vers le futur de l'acte authentique !. - à propos du rapport de la commission de réflexion sur l'authenticité », JCP G n°42, 14 oct. 2013, p.1876-1878 ; M. Mekki, « Voyage au pays de l'authenticité. - quelques réflexions à partir du rapport de la commission présidée par le professeur laurent aynès », JCP N n°41, 11 oct. 2013, p.33-40 ; L. Aynès, « Avons-nous besoin de l'acte authentique ? », Defrénois, n°20, 30 oct. 2013, n°113z1, p.1019-1021 ; B. Reynis, « l'acte authentique électronique », Defrénois, 15 avr. 2005, p.100 ; J.-D. Mathias, « l'authenticité électronique », LPA, 2 avr. 2001, p.25. ; F. Mathieu, « L'acte authentique électronique : état des lieux et perspectives », RLDC n°175, nov. 2019, p.32-34.
[612] Rapport L'authenticité. Droit, histoire, philosophie, *op.cit.*, p.104, n°76 et s.
[613] J.-L. Mouralis, « Preuve : modes de preuve », Répertoire civil, Dalloz, janv. 2011, n°25-31, p.19-20.

par la loi pour la constatation de conventions conclues entre personnes physiques[614]. Il sera question de centrer cette démonstration sur les raisons qui poussent à rejeter la qualification d'acte notarié - « *acte authentique par nature* »[615] - pour les transactions complexes, particulièrement celles qui pourraient porter sur des transactions immobilières, en ce qu'elles concentrent le plus d'enjeux pour la *blockchain*. Nous reviendrons sur les réflexions déjà largement amorcées sur cette problématique par les praticiens, comme les théoriciens, la technologie *blockchain* susceptible de constituer pour la profession notariale, une menace à sa survie[616]. Les transactions même complexes de la *blockchain* ne peuvent pas constituer des actes authentiques et ce pour deux raisons. La première est de l'ordre de la fonction des notaires : l'authentification des actes notariés relève du ressort du notaire puisqu'il est le seul habilité et compétent (1) et la seconde relève des fonctionnalités techniques réduites de la *blockchain*, qui ne peuvent pas accorder la preuve du *negotium* d'un acte (2).

1. L'authentification des actes notariés : l'habilitation et les compétences attribuées aux notaires

268. L'« *authentification* » est une opération définie de deux manières distinctes rejoignant à cet égard les dichotomies précédemment relevées pour les notions d'« *authentique* » et d'« *authenticité* ». Tout d'abord, elle peut être une opération consistant à vérifier l'authenticité d'un objet ou d'un document *a posteriori*[617]. Ou alors, elle peut être considérée comme

[614] *Ibid.*, n°25, p.19.
[615] Ce dernier opère une distinction entre les actes authentiques par nature (actes dressés par les notaires, les huissiers de justice, les commissaires-priseurs judiciaires et les officiers d'état civil) et les actes authentiques fonctionnelles actes administratifs, les sentences arbitrales et les actes du juge dans ses attributions contentieuses (Rapport L'authenticité. Droit, histoire, philosophie, *op.cit.*, p.69 et s., n°44 et s et p.83, n°81).
[616] V. Streiff, « Blockchain et propriété immobilière : une technologie qui prétend casser les codes », Droit & Patrimoine n°262, oct. 2016, p.24-29 ; D. Coiffard, « Didier Coiffard, président du Conseil supérieur du notariat : "La blockchain a un sens pour répartir une partie de la confiance en rendant une information infalsifiable mais cette confiance est très en deçà de celle conférée par le notaire" », RLDC n°147, 1er avr. 2017, p.37-38 ; M. Fontaine, S. Juillet et D. Froger, « La blockchain : mythe ou réalité ? », JCP N n°25, etude n°1214, juin 2017, p.31-36 ; M. Mekki, « Les mystères de la blockchain », *op.cit.*, p.2165, n°17-n°19 ; M. Mekki, « Notaire - Congrès MJN 2017-2018 : rapport de synthèse », JCP N n°47, 24 nov. 2017, p.1319, n°24 ; F. Dempuré, « Où en est la révolution Blockchain ? », JCP N n°18-19, 4 mai 2018, p.1182-1183 ; F. G'Sell, « Preuve et signature numérique », *in* France Stratégie, Rapport, Les enjeux des *blockchains*, *op.cit.*, p.105-106 ; M. Mekki, « Blockchain, smart contracts et notariat : servir ou asservir », ibid., act. 599, p.8, 9, 11 ; Table ronde « L'officier public ministériel est-il soluble dans la blockchain ? », organisée par Le Club du Droit & le Conseil supérieur du Notariat, Intervention de M.-A. Frison-Roche, le 14 mai 2019, à Paris ; M.-A. Frison-Roche, « Analyse des *blockchains* au regard des usages qu'elles peuvent remplir et des fonctions que les officiers ministériels doivent assurer », Defrénois n°25, juin 2019, p.23.
[617] G. Cornu, *Vocabulaire juridique*, *op.cit.*, Voir authentification sens n°2, p.106.

opération *a priori* consistant à conférer l'authenticité des actes authentiques[618]. Ce dernier sens sera retenu pour les développements suivants relatifs aux transactions complexes. L'habilitation et la compétence à authentifier les actes notariés n'ont de sens que si elles sont remises dans leur contexte géographique influant nécessairement sur les conceptions juridiques de l'authentification. La *blockchain* ayant d'importants développements aux États-Unis, de nombreuses confusions ont induit la possibilité d'authentifier par la *blockchain*. Or, en fonction du droit civiliste (a) ou du droit continental (b), c'est une aptitude qui est, soit d'ores et déjà attribuée à une profession réglementée pour l'un, soit qui n'est pas encadrée pour l'autre.

a. Une tradition ancrée dans les pays de droit romano-germanique

269. **L'authentification des actes par le notariat public au Moyen Âge.** La vieille opposition moyenâgeuse entre le seing privé et le seing public permettrait de justifier l'intervention du notariat public et la valeur supérieure de l'acte authentique à celle de l'acte sous signature privée[619]. Des origines anciennes rattachaient l'acte notarié à la catégorie d'acte public[620]. L'institution judiciaire en Italie du Nord au XI^{e} siècle établissait initialement ces actes. En France dans le Midi, et dans les régions septentrionales au XIII^{ème} siècle, c'est le juge non contentieux sous sa fonction de magistrat de l'amiable qui rédigeait ces actes, rôle qui sera ensuite confié au notariat public[621]. La décrétale d'Alexandre III a ainsi posé les bases de l'authenticité d'un écrit, en l'attachant soit à l'intervention d'une « *main publique* », soit à l'apposition d'un sceau authentique[622]. En somme, la qualité d'officier public et ministériel confère depuis de nombreux siècles une telle force à l'acte authentifié, laquelle ne peut pas être remplacée aussi simplement par une *blockchain* qui ne confère quelconque force probante aux transactions immobilières. Pour autant, la *blockchain* a déjà accordé en France une valeur à des parts de Société détenues par un immeuble en permettant leurs enregistrements et leurs ventes dans la *blockchain via* des inscriptions de *tokens*[623].

---

[618] G. Cornu, *Vocabulaire juridique*, *op.cit.*, Voir authentification sens n°1, p.106.
[619] L. Aynès, « Avous-nous besoin de l'acte authentique ? », *op.cit.*, p.1.
[620] Rapport L'authenticité. Droit, histoire, philosophie, *op.cit.*, p.41, n°20.
[621] C. Jallamion, « L'apport des notaires dans l'émergence et la formulation des contrats innomés », Defrénois n°20, n°113z6, 30 oct. 2013, p.1-2 ; Rapport L'authenticité. Droit, histoire, philosophie, *op.cit.*, p.35, n°17.
[622] L. Aynès, « Avous-nous besoin de l'acte authentique ? », *op.cit.*, p.1.
[623] G. Raymond, « Première vente immobilière via blockchain en France », Capital, 24 juin 2019, https://www.capital.fr/immobilier/premiere-vente-immobiliere-via-blockchain-en-france-1342764 (consulté le 31/05/2020).

270. **Les compétences du notaire pour authentifier les actes.** « *Seul un officier public est à même de dispenser l'authenticité* » car c'est « *un service public qu'il incombe dans nos systèmes de droit, à l'État d'organiser et de contrôler* » tels étaient les propos du Professeur Laurent Aynès accompagnant le retour de son rapport sur l'authenticité en octobre 2013[624]. L'utilité des pouvoirs du notaire a déjà été largement étudiée par la doctrine interrogée sur sa légitimité à instrumenter des actes authentiques au regard des développements technologiques et de la libéralisation des métiers du droit[625]. Rappelons que le notaire a reçu en France une habilitation de la loi lui reconnaissant un monopole pour conférer authenticité aux actes juridiques établis par des particuliers[626]. Cette habilitation est ainsi la condition essentielle de l'authenticité d'un acte[627]. Le notaire dispose, en outre, de compétences spécifiques pour exercer ce droit d'instrumenter[628]. C'est une compétence territoriale fixée en fonction de la localisation géographique de l'office notarial et matérielle pour tous les actes dont la loi ne confie pas exclusivement l'authenticité à un autre officier public. Seul le notaire dispose donc d'une délégation de puissance publique pour authentifier les actes.

271. Ses compétences, pour délivrer des actes notariés consistent en trois actions « *dresser, vérifier, et conserver* » l'acte notarié[629]. En effet, le notaire dresse l'acte notarié et n'est pas un « *guichet* » d'enregistrement pur et simple d'une transaction immobilière à la différence de la technologie *blockchain* qui, dans son registre distribué, effectue froidement les opérations. Contrairement à un enregistrement électronique des transactions complexes dans la *blockchain*,

[624] L. Aynès, « Avous-nous besoin de l'acte authentique ? », *op.cit.*, p.1.
[625] Rapport sur les obstacles à l'expansion économique, ss. dir. J. Rueff et L. Armand, présenté par le comité institué par le décret n°59-1284 du 13 nov. 1959, 94 p. ; Rapport de la Commission sur la libération de la croissance française, ss. dir. J. Attali, XO Editions, La Documentation Française, 2008, p.155-170 ; Rapport sur les professions du droit, ss. dir. J.-M. Darrois, mars 2009 ; Rapport L'authenticité. Droit, histoire, philosophie *op.cit.*, p.83, n°56 ; Avis Commission européenne : Recommandation du Conseil, COM (2013), 360 Final (point 13) ; *CJUE, 24 mai 2011* affaire C-47/08, C-50/08, C-51/08, C-52/08, C-53/08, C-54/08, C-61/08 : JCP G 2011, 661, com. F. Picod.
[626] Ordonnance n°45-2590 du 2 novembre 1945 relative au statut du notariat, art. 1 : « *Les notaires sont les officiers publics, établis pour recevoir tous les actes et contrats auxquels les parties doivent ou veulent faire donner le caractère d'authenticité attaché aux actes de l'autorité publique, et pour en assurer la date, en conserver le dépôt, en délivrer des grosses et expéditions* ».
[627] J.-L. Mouralis, « Preuve : modes de preuve », *op. cit.*, n°32, p.20.
[628] Décret n°71-942 du 26 novembre 1971 relatif aux créations, transferts et suppressions d'office de notaire, à la compétence d'instrumentation et à la résidence des notaires, à la garde et à la transmission des minutes et registres professionnels des notaires ; Décret n°86-728 du 29 avril 1986 ; Décret n°97-1002 du 29 octobre 1997 relatif au notariat dans les collectivités territoriales de Mayotte et Saint-Pierre-et-Miquelon ; Décret n°2005-311 du 25 mars 2005 relatif aux professions de notaire et d'huissier de justice.
[629] Rapport L'authenticité. Droit, histoire, philosophie, *op.cit.*, p.103, n°73.

le notaire « *fabrique* »[630] l'acte avec un « *supplément d'âme* »[631]. La *blockchain* serait une forme de sous-traitance immatérielle et technique qui, de façon autonome, ne peut assurément être admise par le Conseil Supérieur du Notariat. Cette organisation professionnelle a eu l'occasion de rappeler que la rédaction des actes, en elle-même, est ce qui constitue l'authenticité, ce qui interdit la mutualisation et la sous-traitance[632].

272. Le notaire vérifie, en outre, les faits et la légalité de l'acte[633]. Il vérifie dans ce cas la conformité des faits aux textes de loi et autres normes, c'est-à-dire la capacité, le consentement éclairé, la pleine validité de l'acte ainsi que l'opportunité de l'acte (le notaire a un devoir de conseil impartial et désintéressé). Si cet officier commet une faute, comme l'absence de contrôle de l'identité des parties, sa responsabilité peut être engagée[634]. Il a aussi un devoir de conseil et de mise en garde quant aux mentions manuscrites imposées par le législateur. Les actes authentiques sont soumis à des conditions de forme *ad validitatem*, variables selon le type d'acte considéré[635]. La *blockchain* implique une logique au mécanisme primaire ne permettant ni d'accorder un conseil éclairé, ni de vérifier des conditions de validité d'un acte. Elle ne pourrait sans nul doute se substituer aux pouvoirs du notaire. La doctrine majoritaire est ainsi unanime sur l'impossibilité pour la *blockchain* d'endosser les compétences du notaire[636].

---

[630] Rapport L'authenticité. Droit, histoire, philosophie, *op.cit.*, p.83, n°56.
[631] V. Streiff, « Blockchain et authenticité : pour une copie non certifiée conforme », Dossier *blockchain* et métiers du droit : une force vive ou subversive, Dalloz IP/IT n°95, févr. 2020, p.97.
[632] Voir notamment les conditions dans lesquelles la sous-traitance est limitativement admise : CSN, AG des 2-3 juill. 2019, résolution relative à la sous-traitance des activités notariales. Voir aussi *infra* les développements sur l'impossible preuve du négocium par la *blockchain* n°280-282.
[633] Rapport L'authenticité. Droit, histoire, philosophie, ss. dir. *op.cit.*, p.84 et s., n°57 et s.
[634] Cass. 1ère civ, 25 nov. 1969, Bull. civ. I, n°364 ; Cass. 1ère civ., 3 avr. 2007, n°06-13.304, D.2007. 1271; AJDI 2007. 498.
[635] Loi du 25 ventôse en XI ; Décret n°71-942 du 26 novembre 1971 relatif aux créations, transferts et suppressions d'office de notaire, à la compétence d'instrumentation et à la résidence des notaires, à la garde et à la transmission des minutes et registres professionnels des notaires ; Décret n°73-1202 du 28 décembre 1973 relatif à la discipline et au statut des officiers publics ou ministériels.
[636] 112ème Congrès des notaires de France, Nantes, juin 2016, n°1249 : propos de la garde des Sceaux qui a indiqué que « *(…) l'acte authentique (n'est) pas qu'une procédure, la blockchain ne pourra pas se substituer à lui* » ; V. Streiff, « Blockchain et propriété immobilière : une technologie qui prétend casser les codes », *op.cit.*, p.24-29 ; M. Mekki, « Notaire - Congrès MJN 2017-2018 : rapport de synthèse », JCP N n°47, 24 nov. 2017, p.1319, n°24 ; M. Mekki, « Les mystères de la blockchain », *op.cit.*, p.2165, n°17-n°19 ; D. Coiffard, « Didier Coiffard, président du Conseil supérieur du notariat : "La blockchain a un sens pour répartir une partie de la confiance en rendant une information infalsifiable mais cette confiance est très en deçà de celle conférée par le notaire" », RLDC n°147, avr. 2017, p.37-38 ; F. Dempuré, « Où en est la révolution Blockchain ? », JCP N n°18-19, 4 mai 2018, p.1182-1183.

273. Le notaire doit enfin assurer la conservation[637] des actes authentiques originaux pendant soixante-quinze ans, après quoi les documents sont versés aux archives[638]. Cette obligation de conservation est rappelée à l'article 1317, alinéa 2 du Code civil pour les actes authentiques établis sur support électronique. L'ancien garde des Sceaux Dominique Perben soutenait lors d'un congrès de notaire qu' « *(...) un aspect essentiel de l'acte notarié, (est) sa conservation ; la minute de l'acte authentique conservé (...) dans l'office notarial, confère aux parties une sécurité et un confort irremplaçables* »[639]. Pour autant, la conservation d'empreintes est une fonction que peut aussi endosser la technologie *blockchain* dans un registre sécurisé, preuve en est que le Conseil supérieur du notariat travaille à l'emploi de cette technologie pour la conservation et le traçage des copies exécutoires électroniques[640].

274. **Les conséquences sur la force probante des actes authentiques.** Cette parcelle d'autorité publique conférée aux notaires par l'État pour authentifier les actes permet de donner pleine foi au contenu desdits actes. La « *foi publique* »[641] accordée à ces actes leur décerne une force probante exceptionnelle. La valeur des faits accomplis ou constatés par le notaire est, par voie de conséquence, considérée comme ayant valeur exceptionnelle. Selon le premier alinéa de l'article 1371 du Code civil, l'acte fait foi jusqu'à inscription de faux pour les énonciations relatives à des faits que le notaire a accompli, ou constaté. De cela, un acte est présumé authentique quand il a une apparence de régularité[642], c'est celui qui conteste qui doit en démontrer la fausseté par la procédure de l'inscription de faux. Par exemple, sont présumées sincères la signature et la date de l'attestation que les parties ont fait ou payé « *en la vue du notaire* »[643]. L'acte notarié donne aussi force exécutoire. En d'autres termes, sans avoir à obtenir un jugement de condamnation, le créancier peut prendre une mesure d'exécution forcée (saisie-attribution, saisie-revendication, saisie-vente) grâce à la « *copie exécutoire* » délivrée

[637] Ordonnance du 2 novembre 1945 relative au statut du notariat, art. 1 ; Décret n°71-941 du 26 novembre 1971 relatif aux actes établis par les notaires, art. 26-28.
[638] Loi n°2008-696 du 15 juillet 2008 relative aux archives, art. 4°, d.
[639] T. Blanchet, « La réalisation du minutier central des notaires de France (la conservation des actes authentiques électroniques) », LPA n° PA20051941729, sept. 2005, p.54.
[640] https://www.affiches-parisiennes.com/stephane-adler-la-*blockchain*-des-notaires-apportera-la-tracabilite-et-la-securisation-a-nos-clients-9393.html (consulté le 31/05/2020).
[641] L. Aynès, « Avous-nous besoin de l'acte authentique ? », *op.cit.*, p.1.
[642] M. Planiol, G. Ripert, *Traité pratique de droit civil français*, *op.cit.*, p.886, n°1451 ; G. Ripert, J. Boulanger, *Traité de droit civil*, t.2, LGDJ, 1957, p.155, n°392.
[643] Cass. 1ère civ. , 26 mai 1964, *Bull. civ.* I, nº 274 ; D. 1964.627 ; *JCP* G, 1964.II.13758, n. R. C. ; en l'espèce, l'acte notarié de vente précisait que le « *prix (...) a été versé par un mandataire de l'acquéreur, porteur des deniers, en la vue du notaire* » ; la cour d'appel avait décidé « *que la preuve pouvait être faite par tous moyens que le prix avait été payé à l'aide de fonds que le notaire détenait déjà pour le compte de l'acquéreur* ».

par le notaire[644]. De plus, il est à même de prendre une mesure conservatoire, sans se munir d'une autorisation du juge de l'exécution[645]. L'acte notarié dispose enfin d'une « *date certaine* »[646].

275. **Le refus de l'authentification des actes par la *blockchain*.** Selon la Professeure Florence G'Sell, dans l'hypothèse où nous souhaiterions complètement substituer l'obligation d'établir des actes notariés par des transactions réalisées dans la *blockchain*, il conviendrait « (…) *de renoncer simplement à l'exigence d'acte authentique. Par exemple, pour que les transactions immobilières soient, dans le futur, réalisées sur la blockchain, il suffirait simplement de renoncer à exiger l'établissement d'un acte notarié pour pouvoir procéder à la publicité foncière. Conférer l'authenticité à l'acte intervenu sur une blockchain n'apparaît donc pas, pour l'heure, indispensable* »[647]. Si nous poursuivions une logique ultra-libéralisante dans l'établissement et l'enregistrement des transactions immobilières, il n'est pas exclu qu'à terme il soit techniquement possible d'enregistrer ces transactions complexes dans une *blockchain* mais elle impliquerait - avec tous les risques que cela comporte - de se dispenser de l'accompagnement du notaire et de l'acte notarié dressé par ses soins.

276. Une proposition venue interpeller sur ces « *dérives technologicides* » a été votée au 113e Congrès des notaires de France pour constater la distinction entre *blockchain* et authenticité. Celle-ci est plutôt axée sur l'impossibilité d'enregistrer un acte dans la *blockchain* plutôt que d'y établir de bout en bout une transaction immobilière. Elle précise en substance que l'authenticité requiert la vérification de l'identité, de la capacité et des pouvoirs, éléments non vérifiés lors du dépôt d'un document dans la *blockchain* ; que le temps de validation d'une opération dans une *blockchain* serait inconciliable avec la date certaine de l'acte authentique ; que la seule empreinte d'un document déposé dans une *blockchain* ne saurait être constitutive de la force probante ; que la force exécutoire, qui découle par essence d'une délégation de la puissance publique, ne pouvait en conséquence être associée à la technologie de la *blockchain* ; et que l'absence de conservation des documents dans la *blockchain* ne satisfait pas à l'obligation faite aux notaires de représenter un acte authentique pendant soixante-quinze ans. Le congrès retient dès lors « *qu'en aucun cas la technologie de la blockchain ne peut se substituer à l'authenticité, comme n'ayant aucun rapport avec la pleine foi de ce que l'officier public à*

[644] Loi du 15 juin 1976, art. 1.
[645] Loi du 9 juill. 1991, art. 68.
[646] C. civ, art. 1377. Sur la notion de date certaine voir *infra* n°532-534.
[647] F. G'Sell, « Preuve et signature numérique », *op.cit.*, p.105-106.

personnellement accompli ou constaté ; et propose de déterminer des cas d'usage pertinents pour utiliser cette technologie dans le notariat »[648]. Cette position du Congrès des notaires, résolument tranchée et prévenante, a pour mérite d'afficher avec clarté le rejet catégorique de l'usage de la technologie *blockchain* en lieu et place des missions des notaires. Elle ne dispose toutefois d'aucune valeur législative ou réglementaire et ne lie en aucun cas le législateur et le pouvoir exécutif.

277. Pour autant, le rejet d'un amendement à la loi relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique n°3623 permet d'anticiper la tendance du législateur au refus de la possibilité d'endosser la fonction « *authentifiante* » par nature à la technologie *blockchain*. C'est dans le secteur des règlements-livraisons dans la finance que des discussions parlementaires ont en effet abouti au rejet de cet amendement n°CF2 qui proposait de reconnaître l'opération de règlement-livraison dans la *blockchain* comme un acte authentique[649].

b. Une tradition absente dans les pays de *common law*

278. **Confusion entre notaires et *notaries public*.** Dans les pays de *common law* l'existence du notaire authentifiant les actes n'est pas requise en matière immobilière. Certains pays comme l'Angleterre ou les États-Unis n'ont en effet pas de notaire qui joue ce rôle d'intermédiaire pour authentifier un acte. L'assimilation entre les notaires de nos systèmes latins et les « *notaries public* » de *common law* est souvent réalisée à tort. Aux États-Unis, la profession de *notary* ne vise pas une profession juridique, c'est une charge accessoire[650]. La « *notarization* » permet seulement la légalisation des signatures mais n'apporte pas de garantie quant au contenu d'un acte. Le « *notaries public* » ne vérifient pas les faits et ne dressent pas les actes[651]. En France, le juge est l'organe de l'application de la loi et les officiers publics en sont aussi garant au même titre. Or le système anglo-saxon n'a pas pour volonté de mêler l'autorité publique aux rapports privés, la souveraineté du juge s'oppose à la préconstitution d'une preuve péremptoire.

[648] Actualité : 113e congrès des notaires de France : le notaire au cœur des mutations de la société, Defrénois, n°def129c3, 28 sept. 2017, p.11.
[649] Amendement n°CF2 présenté par L. de la Raudière, article additionnel après l'article 27 de la loi relatif à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique n°3623. Voir : annexe n°1.
[650] A. Garde, Les activités notariales aux États-Unis et au Canada, Centre Notarial de droit européen, avr. 2014.
[651] Table ronde « L'officier public ministériel est-il soluble dans la blockchain ? », *op.cit.*

Il n'y a pas de vérification du droit de propriété par un officier, le juge se contente de vérifier l'accord sur la transaction entre les parties, voire uniquement l'identité des parties. En pratique, l'acquéreur fait d'ailleurs appel à des assurances pour se garantir contre un risque de contestation du droit de sa propriété. L'exécution forcée est aussi dispensée par le juge[652]. C'est un choix de politique économique lié à la culture des pays. Certains pays préfèrent assumer le risque de l'inexactitude des mentions (parties, réalité du consentement, objet, étendu des obligations, etc.) et s'assurer ainsi d'un marché plus liquide[653].

279. **Conséquences de l'absence de notaires.** Ces deux philosophies, latine et de *common law*, ont des fonctions sociales très différentes. Le réajustement des actes par rapport à la réalité se ferait lors de crises, à l'image de celle des *subprimes*[654]. Il s'agit donc d'un choix entre la liquidité ou la sécurité établie par un notaire. La sécurité technologique apportée par la *blockchain* ne permet pas pour autant de pouvoir dresser des actes dits authentiques puisqu'il n'est pas possible d'établir la preuve d'un *négocium* de l'acte requis en France.

2. L'impossible preuve du *negotium* d'un acte par la *blockchain*

280. **La preuve de l'*instrumentum* par la *blockchain* et non du *negotium*.** En droit français, l'expression de *negotium* est utilisée pour désigner dans l'acte juridique l'opération en laquelle il consiste, par opposition à l'*instrumentum*, qui est l'écrit qui le constate. Ce dernier signifie, en effet, le « *document* », la « *pièce* », utilisé pour désigner l'écrit qui constate l'acte juridique[655]. L'*instrumentum* est en effet le support matériel, la forme de l'acte. Ce support peut être constitué par un écrit sur support dématérialisé, comme ici avec la *blockchain*. L'*instrumentum* peut être endossé par la *blockchain* en ce qu'elle est déjà le support de transactions entre différents participants. Prouver l'existence d'un acte qui transfert de propriété immobilière ancré dans une *blockchain* serait aisé mais c'est le *negotium*, la preuve du contenu de l'acte qui fait défaut et se révèle impossible à établir pour la *blockchain*. L'officier public, précisément le notaire ne se borne pas à enregistrer et restituer des déclarations faites, l'acte notarié « *est le produit de l'activité d'une autorité investie par la puissance publique qui*

[652] L. Aynès, « Avous-nous besoin de l'acte authentique ? », *op.cit.*, p.2.
[653] Table ronde « L'officier public ministériel est-il soluble dans la blockchain ? », *op.cit.*
[654] *Ibid*.
[655] G. Cornu, *Vocabulaire juridique*, *op.cit.*, Voir *negotium*, p.683.

garantit le negotium qu'il constate, ou le fait dont il dresse le constat, (*il*) *s'insère dans l'ordonnancement juridique* »[656]. L'autorité de l'auteur de l'acte, le notaire permet ainsi de s'assurer de la pénétration de la règle de droit dans les rapports sociaux[657].

281. La Professeure Anne Frison-Roche est plus catégorique. Selon elle, la *blockchain* ne peut même pas assumer l'*instrumentum* qui est élaboré par « *des officiers ministériels auxquels l'État demande de vérifier la correspondance entre les mentions des instrumentums et la réalité des négotiums, ce que seuls des êtres humains peuvent mener et ce qu'aucune machine ne peut faire* »[658]. Si l'on en juge ses réflexions, la technologie n'est pas apte à « *dresser* » un acte, c'est-à-dire à en vérifier son exactitude par rapport à la réalité. Ce qui ne permet pas à la technologie d'endosser ce rôle c'est qu'elle ne garantit pas la correspondance entre le *negotium* et l'*instrumentum.* Il semblerait toutefois que la possible duplication des *instrumentum* par une empreinte ensuite ancrée dans la *blockchain* ferait ainsi sens, sans contredire l'office des officiers ministériels. C'est donc la preuve de l'existence de l'*instrumentum* qu'il serait possible d'envisager grâce à l'empreinte d'un document authentique. *In fine*, le formalisme de l'acte est soluble dans la transaction complexe d'une *blockchain* alors que le fond de l'acte ne l'est pas[659].

282. **La problématique de la preuve de la propriété originaire par la *blockchain***. Plus spécifiquement sur le *négocium*, l'acquisition de la propriété ne dérive pas inéluctablement et systématiquement d'un titre constatable dans la *blockchain*[660]. La propriété originaire s'acquiert par la possession prolongée et utile s'expliquant volontiers par l'origine étymologique de l'expression *négocium* qui signifierait notamment « *occupation* ». Force est d'admettre que l'outil technologique *blockchain*, aussi puissant soit-il, établit une césure avec son incapacité à prouver l'acquisition originaire de propriété (l'accession, l'incorporation, ou la prescription)[661]. Le caractère élémentaire du registre de la *blockchain* ne prouve pas la possession mais

[656] L. Aynès, « Avous-nous besoin de l'acte authentique ? », *op.cit.*, p.1. Voir aussi pour plus de détail : Rapport L'authenticité. Droit, histoire, philosophie, *op.cit.*, p.98, n°66.
[657] Rapport L'authenticité. Droit, histoire, philosophie, *op.cit.*, p.96, n°64.
[658] M.-A. Frison-Roche, « Analyse des *blockchains* au regard des usages qu'elles peuvent remplir et des fonctions que les officiers ministériels doivent assurer », *op.cit.*, p.23.
[659] Le formalisme de l'acte authentique est de façon large soluble dans la *blockchain* selon les conclusions du modérateur R. Boffa *in* Cour de cassation, Cycle de conférences « Entre mystère et fantasme : quel avenir pour les *blockchains* ? », ss. dir. scientifique de M. Mekki, N. Blanc, B. Haftel, conférence n°3 « Blockchain et droit immobilier », 28 nov. 2019.
[660] Voir en ce sens : V. Streiff, « Blockchain et propriété immobilière : une technologie qui prétend casser les codes », *op.cit.*, p.26.
[661] C. civ., art. 712.

l'existence à un instant donné. Cette difficulté de l'acquisition originaire ne se résout donc pas par un registre distribué puisque la preuve de l'existence d'un droit et la preuve du droit que ce titre doit transférer ne concordent pas systématiquement[662]. Bien qu'aucune hiérarchie entre les modes de preuve ne soit établie en théorie pour le droit de propriété qui est un fait à prouver, la possession prolongée et utile assortie d'un effet acquisitif est une preuve irréfutable de la propriété par prescription acquisitive ou « *usucapion* », placée au sommet des preuves[663]. De surcroît, le conflit entre acquéreurs successifs d'un même bien immobilier ne peut pas non plus être résolu dans le contexte de la technologie *blockchain* car elle ne saurait apprécier la bonne foi, notion inconstante et circonstanciée[664].

B. Le rejet de la qualification d'acte sous signature privée pour les transactions complexes

283. **Notion et portée de l'acte sous signature privée.** L'acte sous signature privée est un acte établi sur papier ou électroniquement par les parties elles-mêmes sous leur seule signature. Il n'est assujetti qu'à un minimum de formalités laissées à la libre rédaction des parties, à peine de nullité de l'*instrumentum*. Ces actes sont ainsi des actes plus « *simples* » que les actes authentiques car ils sont rédigés sans l'intervention d'un officier public qui aurait agi *ès qualité*[665]. En tant que preuve littérale préconstituée, cet acte est doté d'une force probante inférieure à l'acte authentique. Partant, celui-ci offre moins de garanties mais a toutefois pleine force probante. L'acte sous signature privée fait en effet foi entre ceux qui l'ont souscrit et à l'égard de leurs héritiers et ayants cause[666]. Pour Demolombe, il ne s'agit donc pas seulement d'écritures privées, mais d'actes volontairement rédigés en vue de produire un effet probatoire[667].

284. **Les conditions générales et spéciales de l'acte sous signature privée partiellement remplies par la transaction complexe.** L'acte sous signature privée doit satisfaire une

[662] V. Streiff, « Blockchain et authenticité : pour une copie non certifiée conforme », *op.cit.*, p.97-98.
[663] C. civ., art. 2272.
[664] C. civ., art. 1198, al. 2. Voir : V. Streiff, « Blockchain et propriété immobilière : une technologie qui prétend casser les codes », *op.cit.*, p.28-29.
[665] J.-L. Mouralis, « Preuve : modes de preuve », *op.cit.*, n°162.
[666] C. Civ., art 1372. Voir aussi la possibilité pour cet acte d'acquérir date certaine à l'égard des tiers le jour d'un enregistrement, de la mort d'un signataire, ou lorsque sa substance est constaté dans un acte authentique : C. civ. art. 1377.
[667] C. Demolombe, *Traité des contrats ou des obligations conventionnelles*, t. 6, Paris, 1876, n°350.

exigence générale de signature apposée à l'acte, laquelle lui donne toute sa valeur[668]. Il arrive que des textes spéciaux exigent la rédaction d'un acte sous signature privée *ad validatem* mais pour l'application des articles 1322 à 1325 du Code civil, les signatures ne constituent qu'une exigence *ad probationem*[669]. Cette exigence générale semble d'ores et déjà difficilement remplie avec une transaction complexe de la *blockchain* qui comporte une signature de transaction mais qui n'est pas pour l'instant reconnue par le législateur[670]. En principe, les écrits non signés ne peuvent faire pleine preuve d'un acte juridique car ils ne seront pas considérés comme des écrits sous seings privés[671]. Même si l'absence de signature ne correspond pas exactement à l'hypothèse de la signature *blockchain* apposée mais non reconnue, le fait est qu'il n'est pas possible de tenir une position inflexible sur l'acte sous signature privée dans le contexte de la transaction complexe de la *blockchain* en l'absence de loi formelle ou de jurisprudence de principe. La jurisprudence a cependant tendance à considérer que ces écrits constituent des commencements de preuve s'ils émanent de celui qui les conteste[672]. Ces transactions complexes ont donc, pour l'heure, la valeur de commencement de preuve par écrit sans la reconnaissance catégorique de la signature *blockchain*[673]. Dans ce contexte incertain, nous appelons de nos vœux à un éclaircissement par le législateur de la force probante accordée aux signatures *blockchains*. Nous proposerons ci-dessous des pistes de réflexion à ce sujet[674].

285. S'ajoute une exigence pour les conventions synallagmatiques : la formalité du double original[675]. Cette formalité consiste en la rédaction d'un original pour chaque partie ainsi qu'une mention du nombre d'originaux sur chaque exemplaire. Cette exigence est réputée satisfaite pour les contrats sous forme électronique lorsque l'acte est établi et conservé et que le procédé permet aux parties de disposer d'un exemplaire sur un support durable ou d'y avoir accès[676]. Le fonctionnement intrinsèque de la *blockchain*, indépendamment de sa nature, suppose que chaque nœud dispose d'une « *copie* » du registre de transactions. Cette notion de copie peut

[668] F. Laurent, *Principes de droit civil français*, t. XIX : Durand et Pedone, 1878, n°196 s. : F. Terré, P.Simler et Y. Lequette, *Droit civil, Les obligations*, coll. Précis Dalloz, 10e éd. 2009, n°162.
[669] F. Terré, *Introduction générale au droit,* coll. Précis Dalloz, 8e éd. 2009, n°630.
[670] Voir *infra* n°313 et s. la signature qui pourrait être admise.
[671] Cass. com., 23 févr. 1983 : JCP G 1983, IV, 149 ; Cass., 2e civ., 2 juill. 1996, RTD civ. 1996. 663, obs. Bandrac.
[672] Cass. req., 9 nov. 1869 : DP 1870, I, p.215 ; Cass. req., 22 déc. 1874 : DP 1874, I, p.104 ; Cass. req., 8 juill. 1903 : DP 1903, I, p.507; Cass. 1ère civ., 17 janv. 1961 : Bull. civ. 1961, I, n°41 ; Cass. 2e civ., 2 juill. 1996 : RTD civ. 1996. 663, obs. M. Bandrac.
[673] Voir *supra* n°317-325 sur la proposition de reconnaissance d'une signature électronique simple pour la signature *blockchain*.
[674] Voir *infra* n°374.
[675] C. civ., art. 1375, al.1.
[676] C. civ., art. 1375, al.3.

parfois sembler impropre puisque ce registre est un original dupliqué sur le nombre de nœuds existants. En revanche, ce n'est pas le procédé par lequel le document a été obtenu qui fait l'original[677]. Peu importe alors que le double ait été obtenu par duplication. L'écrit revêtira la qualité d'original dès lors qu'il aura été signé par les parties à la transaction de la *blockchain*[678]. Pour autant, les originaux établis doivent aussi être identiques[679]. L'identité requise concerne le fond, le contenu de l'acte, et non sa forme[680]. Un exemplaire pourrait parfaitement être manuscrit et les autres ancrés dans la transaction être dupliqués dans la *blockchain*, voire directement établis par la transaction complexe, puisque le fond de l'accord conclu sera identique et reproduit sur tous les nœuds. S'agissant de la signature, il est exigé que les différents exemplaires aient été signés simultanément[681]. La transaction complexe de la *blockchain* est signée indépendamment par chaque partie à la transaction grâce à sa propre clé privée, et ce à deux moments distincts, ce qui ne permet pas de satisfaire ces exigences jurisprudentielles. Des solutions techniques existent à l'instar des multisignatures (ou *multisig*) qui permettent de faire signer simultanément un seul élément à un groupe de signataires par le partage d'une adresse publique entre ceux-ci[682]. Ce mécanisme technique est déjà établi pour la conservation des actifs numériques collectés dans le cadre d'une ICO sous visa de l'AMF[683]. Pour la mention, tout participant a la capacité de l'ajouter en clair dans la transaction complexe (sous réserve de la place disponible en fonction de la *blockchain*).

286. Pour les actes synallagmatiques dont l'engagement qui en résulte a pour objet une somme d'argent ou un bien fongible auprès d'une seule partie, une formalité supplémentaire s'impose : la mention du débiteur de la somme ou de la quantité en toutes lettres et en chiffres[684]. Dans ce cas, la mention électronique semble admise grâce à la nouvelle rédaction de l'article 1376 du Code civil, qui n'exige plus de mention « *de sa main* » mais « *par lui-même* »[685]. Cette

[677] I. Pétel-Teyssié, Fasc. unique : preuve des obligations, Modes de preuve, Actes sous seing privé synallagmatiques, formalité du double original, JCl. Civil Code art. 1375, Lexis Nexis, juill. 2017, n°8.
[678] Les signatures ne sauraient résulter d'un procédé de reproduction (Cass. 1ère civ., 17 juill. 1980 : Bull. civ. I, n°225 ; CA Toulouse, 4 déc. 1968 : D. 1969, p.673) contrairement à l'original lui-même dont les duplications au carbone ou par photocopie ont déjà été admises (CA Paris, 6e ch. B, 8 janv. 2004, n°2002/12691).
[679] CA Paris, 2e ch., sect. A, 7 févr. 2007, n°05/03874.
[680] I. Pétel-Teyssié, Fasc. unique : preuve des obligations, Modes de preuve, Actes sous seing privé synallagmatiques, formalité du double original, JCl. Civil Code art. 1375, Lexis Nexis, juill. 2017, n°11.
[681] M. Planiol, G. Ripert, *Traité pratique de droit civil français*, *op.cit.*, n°1458.
[682] Conférence Scaling Bitcoin Université Keio de Tokyo, 6-7 oct. 2018, Voir les présentations « Scriptless Scripts and Multi-party Channels » et « Scaling Security », https://tokyo2018.scalingbitcoin.org/transcripts (consulté le 31/05/2020)).
[683] RGAMF, art. 712-1, II.
[684] C. civ., art. 1376.
[685] I. Pétel-Teyssié, L. Dauxerre, Fasc. unique : preuve des obligations, Modes de preuve, Actes sous seing privé unilatéraux, Mention de la somme ou de la quantité, JCl. Civil Code, art. 1376, Lexis Nexis, juill. 2017.

exigence reformulée et modernisée concorde avec l'anatomie de la technologie *blockchain* mais elle posera tout de même des difficultés. Dans l'échange de valeur des transactions complexes, le registre fait apparaître un montant de crypto-monnaies en chiffres mais pas en lettres. Le strict respect de la mention de la somme d'argent en toutes lettres fait donc défaut.

287. **L'admission de la transaction complexe dans un langage conventionnel ?** L'acte pourrait être rédigé en quelque langue que ce soit[686], sous la seule réserve que chaque partie soit en mesure d'en comprendre le sens[687]. Planiol et Ripert ont même admis l'éventualité « *d'un langage conventionnel dont (les partie) possèd(erai)ent la clef* »[688]. Cet avis doctrinal est indéfectiblement transposable au temps de la *blockchain*. Les parties à la transaction pourraient comprendre le langage utilisé en Français si un acte sous-jacent à l'ancrage dans la *blockchain* est lui-même en Français. Mais en allant plus loin dans cette logique, si la transaction complexe est elle-même considérée comme un acte sous signature privée, il est loisible d'admettre une forme de langage conventionnel informatique entre les parties qu'elles ne comprendraient qu'entre elles.

288. **L'acte sous signature privée irrégulier uniquement entre les parties.** Même si la transaction complexe est irrégulière et ne remplit pas toutes les exigences requises par l'acte sous signature privée, comme la signature électronique, l'irrégularité de l'inobservation des formalités pourra être invoquée par les parties mais non par les tiers. C'est ainsi que, contre le tiers, l'acte sous signature privée irrégulier aura une entière force probante[689]. Pour les tiers, l'acte n'aura plus de force probante uniquement lorsque la discussion porte sur l'existence du contrat ou d'une de ses mentions[690] ; *a contrario*, lorsqu'elle porte sur le sens ou la portée de l'accord, le document irrégulier s'impose à la conviction du juge[691].

---

[686] R. Beudant, P. Lerebourg Pigeonnière, *Cours de droit civil français : Les Contrats et les obligations*, t. 9, 2e ed., 1953, n°1457 ; C. Aubry, C. Rau, *Cours de droit civil français*, t. 12, par P. Esmein, 6e ed., 1958, §756, p.153 ; C. Demolombe, *op.cit.*, n°367 ; F. Terré, *Introduction générale au droit*, *op.cit.*, n°630.
[687] Cass. 3e civ., 15 déc. 1998, n°97-17.673 : Defrénois 1999, I, 1038, obs. D. Talon.
[688] M. Planiol, G. Ripert, *Traité pratique de droit civil français*, t. 7, Obligations, 2e partie, LGDJ, 1931, n°1457.
[689] Cass. civ., 22 oct. 1900 : DP 1901, 1, p.69 ; S. 1902, 1, p.129, note A. Wahl ; Tribunal civ. Grenoble, 9 mars 1937 : S. 1937, 2, p.158 ; Gaz. Pal. 1937, 2, p.172.
[690] CA Aix-en-Provence, 1ère ch., sect. A, 27 févr. 2007, n°06/02166.
[691] Cass. req., 21 juill. 1925 : DH 1925, p.555 ; Cass. civ., 15 janv. 1946 : D. 1946, p.131 ; S. 1946, 1, p.29, note G. L ; Cass. 1ère civ., 24 nov. 1959 : Bull. civ. I, n°494 ; Cass. 1ère civ., 9 janv. 1961 : Bull. civ. I, n°21 ; Cass. 1ère civ., 12 oct. 1964 : D. 1964, p.710 ; Cass. 1ère civ., 22 janv. 1968 : Gaz. Pal. 1968, 1, p.258 ; Cass. 3e civ., 16 juin 1971 : Bull. civ. III, n°387.

289. **L'opposabilité de la date.** La date - si elle est mentionnée - fait foi entre les parties jusqu'à preuve du contraire[692]. Dans l'écrit sous signature privée la date est inopposable à toute personne n'ayant pas été partie à l'acte[693]. Ainsi, l'horodatage par la *blockchain* permettant de dater la transaction complexe ne serait en principe opposable qu'entre les parties à la transaction et non aux tiers[694].

290. **La controverse de la qualification d'acte sous signature privée quant à la nature même de la transaction complexe.** L'illustration phare d'une transaction complexe *via* la *blockchain* est l'ajout d'une condition par un *smart contract*. La doctrine majoritaire refuse de donner au *smart contract* une valeur de contrat et ainsi d'écrit sous-seing privé[695]. Une première difficulté surgit directement de la qualification du *smart contract*. Il semble compliqué d'admettre que la transaction qui inclut une condition par un smart contrat puisse être qualifiée d'écrit sous signature privée alors que ce dernier n'est pas lui-même qualifié de contrat dans l'opinion doctrinale majoritaire.

291. **La reconnaissance spéciale de qualification d'acte sous signature privée pour la transaction complexe de minibons.** Une seconde remarque remettant en cause cette démonstration vient pourtant à l'esprit. Le législateur admet, par le texte spécial de l'ordonnance du 28 avril 2016, qu'une transaction complexe de cession de minibons puisse avoir la valeur d'un contrat écrit[696]. La reconnaissance spéciale de la qualification d'acte sous signature privée pour une transaction complexe ouvre ainsi la voie à cette possibilité. En l'absence de satisfaction totale des exigences de l'acte sous signature privée pour les transactions complexes dans leur ensemble, il convient malgré tout d'envisager dans le temps présent la qualification du commencement de preuve par écrit applicable aux cas généraux.

---

[692] J.-L. Mouralis, « Preuve : modes de preuve », *op.cit.*, n°181.
[693] A. Colin, H. Capitant, *Cours élémentaire de droit civil français*, t. 1, Dalloz, Paris 1914, p.99 ; C. Demolombe, *Traité des contrats ou des obligations conventionnelles*, *op.cit.*, n°365 ; M. Planiol, G. Ripert, *Traité pratique de droit civil français*, t. 6, 1952, p.921 et s, n°1483 ; D. Guével, Fasc. unique : contrats et obligation, Force probante de la date d'un acte sous seing(s) privé(s), Date certaine.
[694] Voir *infra* n°529 et s. les réflexions sur l'opposabilité aux tiers de l'horodatage *blockchain*.
[695] Voir *infra* n°412 et s.
[696] Voir *infra* n°429 et s.

C. L’assimilation souhaitable des transactions complexes à un commencement de preuve par écrit

292. De son rôle initial de modérateur de la rigueur de l'exigence de l'écrit, le commencement de preuve par écrit évolue vers un « *laboratoire d'essai de la preuve moderne* » permettant de tester « *les nouveautés et anticipant les évolutions* »[697], que constitue la *blockchain*, une des dernières évolutions technologiques en date. Le commencement de preuve joue alors un rôle contemporain de véritable « *fabrique* » à preuve numérique. Favorable à la réception de cette qualification, une partie de la doctrine en sa représentation du Professeur Thibaud Douville avance que l’enregistrement d’une transaction qui sert de support à l’acte est un commencement de preuve par écrit, sous réserve de son imputabilité à la partie à laquelle on l’oppose[698].

293. L’académie française définit largement le commencement de preuve comme « *ce qui fait présumer la vérité d'un fait ou d'une promesse, sans néanmoins fournir une preuve suffisante* »[699]. Le commencement de preuve serait donc simplement un indice qui commence une preuve mais la définition juridique semble plus complète pour cerner la notion. Elle est définie comme un écrit n’apportant pas de preuve complète, n’étant pas un acte instrumentaire (valeur de preuve littérale préconstituée) mais une simple lettre missive ou autre document comparable. Il a cependant pour vertu spécifique, comme adminicule préalable, de rendre admissible la preuve testimoniale et indiciaire concernant la preuve des actes juridiques et des faits soumis à des restrictions probatoires. Cette valeur apéritrice est attachée au fait que l’écrit doit en principe émaner de la personne à laquelle on l’oppose et rendre vraisemblable le fait allégué[700].

294. Une définition plus succincte pourrait permettre de retenir en substance qu'il s'agit d'un « *document écrit quelconque (...) dépourvu de la valeur d'acte écrit (authentique ou sous seing(s) privé(s))* »[701] qui, « *n'est pas rédigé spécialement pour constater un acte juridique* »[702] et qui, émanant de celui qui conteste la réalité de l'acte, le rend vraisemblable et permet de le

[697] D. Guével, Fasc. 50 : contrats et obligations, Preuve testimoniale, Commencement de preuve par écrit, *op.cit.*, n°4.
[698] T. Douville, « *blockchains* et preuve », *op. cit.*, p.2194.
[699] Dictionnaire de l'Académie française, t. 1, Firmin Didot, 6e éd. 1835, Voir commencement, p.348.
[700] G. Cornu, *Vocabulaire juridique*, *op.cit.*, Voir commencement de preuve par écrit sens n°1, p.198.
[701] J.-L. Aubert, *Introduction au droit et thèmes fondamentaux du droit civil*, coll. U, Armand Colin, 10e éd. Paris 2004, n°222.
[702] C. Larroumet, *Droit civil. Introduction à l'étude du droit privé*, t. 1, Economica, Paris, 4e éd. 2004, n°573.

prouver par témoins et/ou indices. Le commencement de preuve par écrit est ainsi une dérogation à l'obligation de préconstitution de preuve par écrit et à celle de production d'un écrit pour prouver contre un autre écrit[703]. Pour se voir qualifier de commencement de preuve par écrit, la transaction complexe doit néanmoins remplir systématiquement les conditions requises par ce commencement (1) afin de bénéficier de ses effets probatoires qui restent de moindre valeur (2).

1. Les conditions du commencement de preuve par écrit à satisfaire invariablement par les transactions complexes enregistrées dans la *blockchain*

295. **La condition large de l'écrit.** Selon le premier alinéa de l'article 1362 du Code civil, « *constitue un commencement de preuve par écrit tout écrit qui, émanant de celui qui conteste un acte ou de celui qu'il représente, rend vraisemblable ce qui est allégué* ». Pour être admis, ce commencement de preuve doit premièrement, constituer logiquement un écrit. C'est un écrit selon l'acception classique du terme. Il peut s'agir de n'importe quel type d'écrit n'ayant pas la valeur d'un acte authentique ou sous signature privée[704]. Ne pourront être considérés comme commencements de preuve par écrit, des agissements auxquels s'est livrée une partie[705], ou encore le silence[706]. La jurisprudence entend tout de même assez largement cette exigence de l'écrit. Sont considérés comme des écrits constituant des commencements de preuve de simples notes[707], des lettres[708], des registres domestiques[709], la reconnaissance d'une dette[710], des

[703] Cass. 3e civ., 7 mai 1969 : Bull. civ. 1969 III, n°356 : en l'espèce, il s'agissait de prouver outre et contre le contenu d'un acte authentique.
[704] D. Guével, Fasc. 50 : contrats et obligations, Preuve testimoniale, Commencement de preuve par écrit, *op.cit.*, n°9.
[705] Cass. civ., 17 déc. 1867 : DP 1867, 1, p.486 Aubry et Rau, *Cours de droit civil français*, Litec, t. 7, 6e éd. par P. Esmein, n°754, p.272.
[706] Cass. 3e civ., 23 janv. 1969 : Bull. civ. III, n°66.
[707] Cass. civ., 30 juill. 1855 : DP 1855, 1, p.332 ; Cass. crim., 27 mars 1934 : DH 1934, p.238.
[708] Cass. 1ère civ., 20 avr. 1983, Bull. civ. I, n°126 ; Com. 10 mai 1994, n°92-16.120, Bull. civ. IV, n°172 ; JCP 1994. IV. 1740
[709] Cass. civ., 4 août 1854 : DP 1854, 1, p.597.
[710] CA Lyon, 1ère ch. civile b, 6 févr. 2018, n°16/09379.

documents électroniques[711], des courriers électroniques entre deux adresses de messagerie ou des messages téléphoniques[712], ou plus généralement des écrits numériques irréguliers[713].

296. Les transactions complexes en elles-mêmes et les éléments les composant peuvent constituer des écrits numériques irréguliers en ce qu'elles contiennent une empreinte, un *smart contract* mais font généralement référence à un acte extérieur (le document dont l'empreinte est calculée ou le déclenchement de la condition requise, par exemple). Les éléments traditionnels générés par une transaction de la *blockchain*, tels que les adresses publiques des participants, l'identifiant de transaction, la date et l'heure de l'entrée de la transaction, la date et l'heure de la validation du bloc, font aussi partie prenante de ces écrits numériques.

297. **La condition de la provenance de l'écrit de la personne qui le conteste ou de celui qu'il représente.** Deuxièmement, l'écrit doit provenir de la personne qui le conteste ou de celui qu'il représente[714]. Le commencement ne peut émaner d'un tiers[715]. La représentation par un mandataire est cependant possible[716]. Dans le cadre d'une transaction complexe, il se pourrait que l'auteur d'une transaction soit représenté par un PSAN ayant obtenu mandat d'agir en nom et pour son compte. Le commencement de preuve par écrit serait ainsi le fait du mandataire représentant de la personne à qui on l'oppose. Les juges du fond doivent vérifier si l'acte peut être considéré comme émanant du défendeur lorsqu'une personne conteste avoir signé un document[717].

298. **L'identification de l'auteur de l'écrit : les frictions avec la *blockchain*.** Afin de vérifier la provenance de l'écrit de la personne qui le conteste, l'auteur de l'écrit doit être clairement identifié. Cette identification de l'auteur de l'écrit renvoie à deux facteurs essentiels à considérer dans les *blockchains* qui changent en fonction de leurs typologies et protocoles. Le

[711] TGI Évry, 1ère ch. a, 21 nov. 2016, n°15/08820 : concernant un document intégralement dactylographie et signé par les parties mais dont rien ne permettait de s'assurer sur ce document que les signataires et les scripteurs des mentions dactylographiées étaient bien authentifiés.
[712] Cass. 1ère civ., 20 mai 2010, n°09-65.854, Inédit ; CA Versailles, 16e ch., 8 nov. 2012, n°12/00118 ; CA Colmar, ch. 1 a, 14 nov. 2018, n°17/03926.
[713] O. Audic, *Les fonctions du document en droit privé*, bibliothèque de l'Institut André Tunc, t. 3, LGDJ, 2004, n°236, note 177.
[714] C. civ., art. 1362.
[715] Cass. 1ère civ., 13 juill. 1955 : Bull. civ. 1955, I, n°304 : concernant un extrait du registre d'un enregistrement qui ne pouvait « *émaner* » du vendeur du bien concerné ou de ses héritiers.
[716] Cass. 1ère civ., 24 juin 1969 : D. 1970, p.155 ; Cass. req., 16 juin 1890 : DP 1891, I, p.97, note M. Planiol ; Cass. req., 19 déc. 1904 : DP 1906, I, p.349 ; Cass. req., 13 avr. 1908 : DP 1908, I, p.363 ; Cass. 3e civ., 29 févr. 1972 : Bull. civ. 1972, III, n°142 ; Cass. 1ère civ., 5 oct. 1976 : Gaz. Pal. 1976, II, somm. p.277
[717] Cass. 1ère civ., 13 nov. 2008, n°07-20.249.

premier facteur d'identification dans la *blockchain* considère la signature *blockchain* utilisée (notamment, l'algorithme de cryptographie déployé) que nous développerons ci-après[718]. Le second facteur d'identification dans la *blockchain* prend en compte la traçabilité des transactions : si elles sont accessibles dans un registre public ou non, si des techniques de mixage sont utilisées[719], si l'origine des connexions sont anonymisée, si la pratique de l'obfuscation de données est employée[720], ou encore celle de l'usage d'une adresse publique par transaction. Certaines *blockchains* masquent la source, la destination ou le montant des transactions grâce à ces diverses techniques[721]. Ces deux critères permettent de déterminer si une *blockchain* est plutôt identifiante, pseudonyme ou totalement anonyme[722]. Il convient de revenir pour cela sur les notions, les caractéristiques et le contexte de l'anonymat et du pseudonymat dans les *blockchains* (essentiellement publiques), qui font l'objet de nombreuses discussions tant chez les technologues[723], que chez les juristes[724].

299. **Le pseudonymat et l'anonymat sous son prisme technique.** Il y aurait deux interprétations possibles dans la manière de concevoir l'anonymat des *blockchains* publiques sous son prisme technique. Ces deux axes d'interprétations conduisent à des conclusions très différentes. La première interprétation considère que le nom n'est pas requis dans une *blockchain* publique pour devenir participant puisque seul une adresse publique sert « *d'identifiant* » aux participants pour réaliser des transactions. S'il existe un lien entre le détenteur des clés et le compte lui-même, les comptes sont connus car l'adresse publique du compte apparaît publiquement mais le lien entre le propriétaire dudit compte et les comptes

[718] Voir *infra* n°331-332.
[719] Voir *infra* n°606.
[720] Voir note de bas de page n°1593.
[721] Voir notamment les techniques employées par les « *Anonymity-Enhanced Cryptocurrency* » : FAFT, Virtual assets and virtual asset service providers, juin 2019, p.6.
[722] Voir *infra* n°339.
[723] En sciences dures : A. M. Antonopoulos, *Mastering Bitcoin : Unlocking Digital Cryptocurrencies*, *op.cit.*, p.228 ; A. Narayanan, Lecture 6 – Bitcoin and anonimity, Princeton's Bitcoin Mooc, Princeton University, https://www.youtube.com/watch?v=glyQy_e5LmM (consulté le 31/05/2020) ; G. Fuchsbauer, *Strong anonymity in cryptocurrencies*, Les sémainaires de la cryptofinance ss. dir. G. Grunspan, R. Pérez-Marco, le 8 Juin 2017 ; J.-P. Delahaye, « Crypto-monnaies décentralisées raisonnables », Blogs pour la science, janv. 2020, http://www.scilogs.fr/complexites/crypto-monnaies-decentralisees-raisonnables/ (consulté le 31/05/2020).
[724] En sciences sociales : J. Tenyson, « What is the impact of *blockchains* on privacy ? », Open Data Institute, dec. 2015, https://theodi.org/article/what-is-the-impact-of-*blockchains*-on-privacy/ (consulté le 31/05/2020) ; P. de Filippi, « The interplay between decentralization and privacy: the case of blockchain technologies, Journal of Peer Production », Alternative Internets n°7, 2016, p.11-12 ; D. Guégan, « Blockchain Publique versus Blockchain Privée : Enjeux et Limites », Documents de Travail du Centre d'Economie de la Sorbonne, 2017, p.5 ; A. Barbet-Massin, F. Chafiol, « La blockchain à l'heure de l'entrée en application du règlement général sur la protection des données », Dossier données à caractère personnel, quelle circulation de demain, Dalloz, Dalloz IP/IT n°12, dec. 2017, p.638-639 ; T. Douville, « Blockchain et protection des données à caractère personnel », AJ Contrat, dossier, juill. 2019, p.319-320, n°15 ; EU Blockchain Observatory and Forum, Blockchain and the GDPR, oct. 2018, p.19.

eux-mêmes n'apparaît pas[725]. Ainsi, selon cette première interprétation, la *blockchain* publique serait anonyme car elle n'utiliserait pas un vrai nom mais un « *identifiant* ». C'est dans le sillon de cette interprétation que s'inscrit Satoshi Nakamoto, le créateur de Bitcoin, qui faisait référence à cette *blockchain* en 2008 comme étant anonyme et protectrice de la vie privée[726]. Selon une deuxième interprétation qui emporte l'assentiment général, outre le fait que seuls des chiffres et des lettres d'une adresse publique apparaissent dans la *blockchain* publique, elle n'est pas pour autant anonyme puisque d'autres facteurs techniques permettraient l'identification. Dans le cadre de cette deuxième conception, l'adresse publique serait considérée comme un pseudonyme en sciences informatiques[727].

300. **Le pseudonymat et l'anonymat sous son prisme juridique.** Sous le prisme juridique, l'anonymat complet dans le cadre d'une *blockchain* et dans un contexte plus général est un cas de figure rare. Pour en revenir à sa définition, l'anonymat, au sens large, est l'état de quelqu'un qui veut rester inconnu, anonyme[728]. Il serait un droit dans certains cas, c'est-à-dire une possibilité de rester anonyme. Par exemple, l'article 6, III, 2 de la loi pour la confiance dans l'économie numérique permet aux éditeurs de contenu non professionnels de préserver leur anonymat[729]. Selon la lettre de l'article, ils devront toutefois tenir à la disposition du public le nom, la dénomination ou la raison sociale et l'adresse de l'hébergeur, sous réserve de lui avoir communiqué leurs éléments d'identification personnelle. Les hébergeurs sont assujettis au secret professionnel au sujet de la divulgation de ces éléments d'identification mais celui-ci n'est pas opposable à l'autorité judiciaire. En réalité, cet « *anonymat* » est un pseudonymat en pratique[730]. La Commission parlementaire de réflexion et de proposition sur le droit et les libertés à l'âge du numérique de l'Assemblée nationale défend cette nécessité de recourir au pseudonymat sur Internet[731]. Les conjonctures laissent souvent céder, pour des raisons sécuritaires ou de responsabilité, le droit à l'anonymat face à l'obligation d'identification. C'est ainsi qu'en droit l'anonymat total est très rare et penche vers un pseudonymat de fait ou une

[725] Conférence « Les mardis de l'espace des sciences », organisée avec l'Université de Rennes 2 - CREA, intervention de J.-P.Delayahe « Les mathématiques et la cryptographie réinventent la monnaie : le bitcoin », le 14/10/2014.
[726] S. Nakamoto, « Bitcoin : A Peer-to-Peer Electronic Cash System », *op.cit.*, p.6.
[727] A. Narayanan, Lecture 6 — bitcoin and anonymity, Princeton's bitcoin mooc, Princeton university, (consulté le 31/05/2020).
[728] https://www.universalis.fr/dictionnaire/anonymat/ (consulté le 31/05/2020).
[729] Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
[730] Assemblée nationale, Commission de réflexion et de propositions sur le droit et les libertés à l'âge numérique, Numérique et libertés : Un nouvel âge démocratique, rapport n°3119, président par C. Paul et C. Féral-Schuhl, recommandation n°18, oct. 2015, p.69.
[731] *Ibid*., p.70.

identification pure et simple. Le Parlement européen confirme d'ailleurs dans une résolution du 3 octobre 2018 sur les technologies des registres distribués et les chaînes de blocs dans son point D que la *blockchain* « *favorise la pseudonymisation des utilisateurs mais non leur anonymisation* »[732].

301. Le pseudonymat et l'anonymat sont également envisagés d'une façon bien singulière en matière de protection des données à caractère personnel. Notons que les avis du G29 (groupe de travail « Article 29 »), de la CNIL et la jurisprudence actuelle sont très stricts sur le processus d'anonymisation lorsqu'un ensemble de données contient des données qui pourraient être identifiantes directement ou indirectement[733]. Leurs positions tendent à conclure à la quasi-inexistence d'une anonymisation totale[734], seule la pseudonymisation pourrait être une garantie technique de réussite. Les données pseudonymisées seraient celles pour lesquelles il existerait un lien avec au moins une identité de la personne concernée[735]. Cette correspondance peut être effectuée dans les deux sens, s'il existe un identifiant et une table de correspondance entre le jeu pseudonyme et les données d'identité et en amont, si une fonction de hachage est utilisée dans un sens unique[736]. Dans une *blockchain* publique la donnée pseudonymisées peut se situer d'une part avec l'adresse publique et une table de correspondance des données à caractère personnel détenue par des prestataires, et d'autre part, dans le cadre de la clé publique hachée ou d'un autre ensemble de données quelconques dont l'empreinte est calculée.

302. **L'interprétation du pseudonymat et de l'anonymat dans une *blockchain*.** Deux interprétations du pseudonymat sous un angle juridique peuvent être retenues à l'heure de la *blockchain*. L'une concerne le processus de pseudonymisation réalisé en amont par la signature *blockchain* (voir ci-après), ou encore par le mécanisme de l'empreinte *blockchain* (voir ci-

[732] Parlement européen, Résolution du 3 oct. 2018 sur les technologies des registres distribués et les chaînes de blocs: renforcer la confiance par la désintermédiation (2017/2772(RSP)), P8_TA(2018)0373. Voir la première résolution dans le secteur des crypto-monnaies qui l'évoquait : Parlement européen, Résolution du 26 mai 2016 sur les monnaies virtuelles, (2016/2007(INI)), P8_TA(2016)0228, 1.d).

[733] RGPD, art. 4, 1.

[734] Groupe de travail « article 29 » sur la protection des données, Avis 05/2014 sur les Techniques d'anonymisation, adopté le 10 avr. 2014, p.13 : « (…) *les recherches en matière de techniques d'anonymisation se poursuivent et font apparaître invariablement qu'aucune technique n'est, en soi, infaillible. En termes généraux, on distingue deux grandes approches de l'anonymisation: la première repose sur la randomisation tandis que la seconde se fonde sur la généralisation. D'autres notions sont aussi abordées dans le présent avis, comme la pseudonymisation, la confidentialité différentielle, la l-diversité et la t-proximité* » ; Voir aussi en ce sens les décisions : CNIL, délib. n°2015-255, 16 juill. 2015 ; CE, 10ème et 9ème ch. réunies, 8 déc. 2017, n°393714 : Comm. com. électr. 2017, comm. 55, note N. Metallinos ; AJDA 2017, 325 ; TGI de Paris, 17ème ch., 14 févr. 2018.

[735] Voir les conditions du processus de pseudonymisation exigé par le RGPD : RGPD, art. 4,5.

[736] Voir pseudonymisation des données à caractère personnel : https://www.cnil.fr/fr/identifier-les-donnees-personnelles (consulté le 31/05/2020).

avant), et l'autre fait référence à la possible ré-identification d'un individu notamment par une ou un ensemble de données à caractère personnel.

303. Selon la première interprétation, l'ensemble des *blockchains* qui utilisent du chiffrement asymétrique visé par les autorités de protection des données seraient pseudonymes et pourraient tendre vers des *blockchains* identifiantes. En ce sens, a été considérée comme une donnée indirectement identifiante l'adresse IP dynamique[737] et récemment l'adresse publique des *blockchains* depuis un avis de la CNIL du 24 septembre 2018[738].

304. Selon sa deuxième interprétation, l'ensemble des *blockchains* seraient aussi pseudonymes puisqu'il existe une identification massive par des services tiers permettant une ré-identification des participants. Soit, d'un côté, ces derniers sont soumis à des obligations d'identification de leurs clients au titre des mesures de *know your customer* (KYC) visant à lutter contre le blanchiment de capitaux et le financement du terrorisme[739]. À ce titre, aux États-Unis, l'« *Internal Revenue Service* » (équivalent de l'administration fiscale française) a déposé auprès du Tribunal de district du nord de la Californie une assignation à l'encontre de la plateforme « *Coinbase* » - une plateforme d'échange d'actifs numériques - exigeant l'identité de tous les utilisateurs sur le sol américain et leurs historiques de transactions de 2013 à 2015[740]. Soit, de l'autre, des explorateurs traçant des adresses publiques permettent de reconstruire les actions d'une personne en suivant l'historique du registre *blockchain* et en croisant les transactions réalisées par une même adresse publique. L'identité d'un participant à une *blockchain* peut en conséquence être associée à une adresse publique[741].

305. Ainsi, même si de prime abord, l'identification de l'auteur d'une transaction dans la *blockchain* semble complexe, les capacités techniques de certains outils pourraient permettent de connaître son identité. Couplés aux palliatifs réglementaires mis en place pour renforcer la

[737] CJUE, 2e ch., 19-10-2016, aff. 582/14, Breyer c/ Bundesrepublik Deutschland ; Cass., 1e civ., 3 nov. 2016, n°15-22.595 FS-PBI, Sté Cabinet Peterson c/ Sté Groupe logisneuf ; WO 37 : Le respect de la vie privée sur internet – Une approche européenne intégrée sur la protection des données en ligne, adopté le 21 nov. 2000 ; WP 136 : Avis 4/2007 sur le concept de données à caractère personnel, adopté le 20 juin 2007 ; CNIL, délib. n°2006-294 du 21 dec. 2006.

[738] CNIL, Premiers éléments d'analyse de la CNIL. Blockchain, 24 sept. 2018, p.7. L'Observatoire des *blockchains* confirme cet avis indiquant que les adresses publiques sont généralement des données à caractère personnel (EU Blockchain Observatory and Forum, Blockchain and the GDPR, *op.cit.*, p.19-20).

[739] C. mon. fin., art. L561-2, 7° bis : sur l'obligation des PSAN en France d'identifier leurs clients dans le cadre d'une procédure de KYC.

[740] Tribunal de district du nord de la Californie, cas n°3:16-cv-06658-JSC, États Unis c. John Doe, 17/11/16 et la doctrine de l'IRS : https://www.irs.gov/uac/newsroom/irs-virtual-currency-guidance (consulté le 31/05/2020).

[741] Le site blockchain.info en est une illustration.

connaissance des participants à la *blockchain*, il est à présent très aisé de connaître l'auteur d'une transaction.

306. Toutefois, des *blockchains* sont encore considérées comme anonymes par le Groupe d'action financière (GAFI) comme « *ZCash* » ou « *Monero* »[742]. Par exemple, ZCash use d'un registre distribué permettant de masquer plus ou moins complètement les transactions et les participants (ne faisant ni apparaître l'adresse de l'expéditeur, ni celle du signataire) par des techniques dites de « *preuve à divulgation nulle de connaissance* » (ou *zero knowledge proof*)[743]. Ces dernières attestent la validité d'une transaction sans divulguer l'identité de la partie prenante ou le montant de la transaction.

307. **L'identification dans les *blockchains* privées.** Les *blockchains* privées forment un genre de registre d'identité pour conserver les informations d'identification de ses utilisateurs à des fins d'authentification[744]. La plupart, sinon la totalité, des données des participants sont généralement stockées en dehors de la *blockchain*, de sorte qu'elle dispose d'un référentiel de données chiffrées dont l'accès est contrôlé. Les *blockchains* privées viennent donc souvent canalyser la problématique de l'identification puisqu'elles peuvent identifier les participants, opérateurs économiques ou institutions d'un même secteur généralement au nombre limité.

308. Ainsi ce critère d'identification ne posera pas, semble-t-il, de difficultés particulières pour l'auteur d'une transaction complexe dans une *blockchain* privée mais fera parfaitement défaut pour certaines *blockchains* publiques totalement anonymes[745]. Observons toutefois que l'exigence d'identification est généralement plus souple dans un commencement de preuve par écrit. Ce qui importe en effet dans ce type de preuve imparfaite c'est de pouvoir imputer l'acte à quelqu'un, soit d'établir un lien entre l'acte et son acteur. Ce lien est alors plus ou moins distendu en fonction des éléments présentés ci-avant.

309. **La condition de la vraisemblance du point allégué.** Troisièmement, l'écrit doit rendre vraisemblable le point allégué, autrement dit, il établit une vérité qui elle-même rend

[742] FAFT, Virtual assets and virtual asset service providers, *op.cit.*, p.6.
[743] E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, M. Virza, « Zerocash: Decentralized Anonymous Payments from Bitcoin », 2014, p.459 ; Rapport France stratégie (présidé par J. Toledano), Les enjeux des *blockchains*, *op.cit.*, p.52.
[744] EU Blockchain Observatory and Forum, Scalability interoperability and sustainability of blockchains, *op.cit.*, p.15.
[745] Voir les distinctions *infra* n°384 sur les degrés d'identification en fonction des blockchains.

vraisemblables l'existence et le contenu de l'élément à prouver[746]. Est donc requise une évaluation des probabilités, et à ce titre il est nécessaire que de fortes probabilités soient constatées pour l'existence et le contenu de la transaction complexe[747]. S'il y a plusieurs possibilités crédibles de manière égale, si la solution reste ambiguë, si le contenu du document est de caractère équivoque, il n'y a pas vraisemblance[748]. Les juges du fond sont souverains pour apprécier que l'écrit rende vraisemblables les faits allégués[749].

2. Les effets probatoires de moindre valeur du commencement de preuve par écrit des transactions complexes

310. **La valeur d'adminicule à compléter.** L'usage du commencement de preuve pour des transactions complexes est subordonné en matière probatoire à un autre écrit imparfait. La transaction complexe n'a donc pour seule valeur que celle d'un adminicule[750], c'est-à-dire qu'il ne peut servir que d'aide, de secours, d'appui[751]. Il convient ainsi de complémenter la transaction complexe par un autre écrit imparfait[752], comme des témoignage, indice, présomption de fait, aveu extrajudiciaire ou encore serment supplétoire. Par exemple, pour être qualifié de commencement de preuve par écrit, un mail avait été corroboré par l'argumentation développée par le demandeur devant le premier juge[753]. Ou alors a déjà été retenu un second

[746] H. Mazeaud, *La conception jurisprudentielle du commencement de preuve par écrit de l'article 1347 du Code civil*, thèse Lyon 1921, p.105.
[747] D. Guével, Fasc. 50 : contrats et obligations, Preuve testimoniale, Commencement de preuve par écrit, *op.cit.*, n°65.
[748] Com. 4 déc. 1956, Bull. civ. III, n°322.
[749] De jurisprudence constante : Cass. req., 16 mars 1881 : DP 1882, II, p.373 ; S. 1881, I, p.311 ; Cass. req., 13 juin 1895 : DP 1895, I, p.372 ; Cass. civ., 16 juill. 1918 : DP 1918, I, p.77 ; Cass. com., 10 oct. 1955 : Bull. civ. 1955, III, n°281 ; Cass. 1ère civ., 20 mai 1957 : Bull. civ. 1957, I, n°224 ; Cass. 1ère civ., 27 févr. 1961 : Bull. civ. 1961, I, n°127 ; Cass. soc., 17 déc. 1962 : Bull. civ. 1962, IV, n°911 ; Cass. 1ère civ., 13 janv. 1964 : Bull. civ. 1964, I, n°28 ; Cass. 1ère civ., 26 nov. 1964 : Bull. civ. 1964, I, n°523 ; Cass. 1ère civ., déc. 1965 : Bull. civ. 1965, I, n°670 ; Cass. 1ère civ., 20 janv. 1970 : Bull. civ. 1970, I, n°28 ; Cass. 3e civ., 29 avr. 1970 : Bull. civ. 1970, III, n°297 ; Cass. 3e civ., 5 juin 1970 : Bull. civ. 1970, III, n°382 ; Cass. 3e civ., 1er avr. 1971 : JCP G 1972, II, 16998, obs. J. Ghestin ; Cass. 1ère civ., 4 déc. 1973 : Bull. civ. 1973, I, n°336 ; Cass. 1ère civ., 22 juin 1976 : D. 1976, inf. rap.p.254 ; Cass. 1ère civ., 22 déc. 1981 : Bull. civ. 1981, I, n°396 ; Cass. com., 3 nov. 1983 : D. 1984, inf. rap.p.67 ; Bull. civ. 1983, IV, n°290 ; Cass. 1ère civ., 21 oct. 1997 : Bull. civ. 1997, I, n°284 ; Cass. 1ère civ., 6 mai 2003, n°00-16.031 ; Cass. com., 5 mai 2004, n°02-11.574 ; Cass. 1ère civ., 18 oct. 2005, n°04-11.151 ; Cass. 1ère civ., 4 juin 2007, n°06-15.945 ; Cass. com., 3 juill. 2007, n°06-10.939 : O. Audic, *op.cit.*, n°234 ; F. Terré, *op.cit.*, n°525.
[750] L'éthymologie latine *adminiculum* de l'adminicule signifie aide, action d'aider.
[751] La valeur d'adminicule du commencement de preuve par écrit : Cass. 1ère civ., 27 févr. 1961 : Bull. civ. I, n°127.
[752] Cass. com., 30 janv. 1980 : Bull. civ. 1980, IV, n°50 ; JCP G 1980, IV, p.147 ; Cass. 1ère civ., 28 févr. 1995 ; Bull. civ. 1995, I, n°107 ; D. 1995, somm. p.228, obs. R. Libchaber ; Defrénois 1995, p.735, art. 36100, n°59, obs. Ph. Delebecque ; Cass. 1ère civ., 29 mai 1997 ; Cass. 1ère civ., 16 oct. 2008, n°0711.627 ; Cass. 1ère civ., 25 juin 2009, n°08-11.931 ; Cass. 1ère civ., 24 sept. 2009, n°08-19.752 ; Cass. 1ère civ., 20 mai 2010, n°09-65.854.
[753] CA Riom, 1e ch., 19 nov. 2018, n°17/00837.

exemplaire de l'écrit[754]. L'addition de deux preuves imparfaites équivaut à une preuve parfaite[755]. Les multiples « *copies* » sur les nœuds pourraient alors servir de complément de preuve du commencement de preuve par écrit.

311. **Les modalités du complément.** Ce complément peut être indifféremment antérieur ou postérieur par rapport au commencement de preuve par écrit lui-même[756]. Il se trouve toutefois conditionné à une unicité, il ne peut y avoir une multitude de preuves complémentaires[757]. Il devra aussi être en lien avec le commencement preuve. Le lien suffisant pourra faire l'objet d'un contrôle par la Cour de cassation[758]. Enfin, il est exigé que le complément du commencement de preuve par écrit soit extérieur à celui-ci. Autrement dit, un même document ne pourrait servir à la fois de commencement de preuve et d'indice complémentaire[759]. Une transaction complexe dispose justement de faculté technique de renvoi à un écrit ou à d'autres indices en dehors de la *blockchain* formant un lien numérique inscrit dans le registre. Par exemple, un *smart contract* fait référence à un ensemble de données fournies par un Oracle extérieur à la *blockchain* permettant de déclencher l'exécution d'une conséquence préétablie. L'Oracle est un prestataire externe ayant pour but de fournir une source de données exogène qui sert de pont entre les *smart contracts* et des données en dehors de la *blockchain*[760].

[754] Cass. 1ère civ., 3 avr. 1973 : Bull. civ. 1973, I, n°126. Contre : Cass. 1ère civ., 4 mars 1997 ; Bull. civ. 1997, I, n°80 ; JCP G 1997, II, 22954, note Cl. Gonon ; RTD civ. 1998, p.108, obs. J. Mestre ; Defrénois 1997, p.748, obs. J.-L. Aubert et p.1011, obs. Ph. Delebecque ; D. affaires 1997, p.411.
[755] D. Guével, Fasc. 50 : contrats et obligations, Preuve testimoniale, Commencement de preuve par écrit, *op.cit.*, n°66.
[756] Cass. 1ère civ., 29 oct. 2002, n°00-15.834 : peu importe que qu'un aveu extrajudiciaire ne soit pas concomitant à un cautionnement irrégulier valant commencement de preuve par écrit
[757] Cass. 1ère civ., 30 oct. 1961 : Bull. civ. 1961, I, n°492 ; Cass. 2e civ., 28 oct. 1970 : JCP G 1970, IV, p.300 ; Bull. civ. 1970, II, n°290 : concernant en l'espèce la preuve d'un fait, donc sans nécessité qu'il y ait un commencement de preuve par écrit ; Cass. 3e civ., 28 nov. 1972 : JCP G 1973, IV, p.16 ; Bull. civ. 1973, III, n°636.
[758] Cass. 1ère civ., 2 juill. 1996 : Bull. civ. 1996, I, n°282 ; D. 1997, somm. p.164 (5e arrêt), obs. L. Aynès ; RTD civ. 1996, p.665, obs. M. Bandrac.
[759] Cass. 1ère civ., 22 juill. 1975 : Bull. civ. 1975, I, n°247 ; Cass. 1ère civ., 21 nov. 1978 : D. 1979, inf. rap.p.87 ; Cass. 1ère civ., 16 janv. 1985 : Bull. civ. 1985, I, n°24 ; RTD civ. 1986, p.758, obs. J. Mestre ; RTD civ. 1987, p.767, obs. J. Mestre ; Cass. 1ère civ., 5 févr. 1991 : Bull. civ. 1991, IV, n°54 ; D. 1991, somm. p.217, obs. M. Cabrillac ; Cass. com., 31 mai 1994 (2 arrêts) : JCP G 1994, IV, 1948 ; RTD civ. 1994, p.903, obs. M. Bandrac ; Bull. civ. 1994, IV, n°191 et 193 ; Cass. 1ère civ., 4 mars 1997 : Bull. civ. 1997, I, n°80 ; JCP G 1997, II, 22954, note Cl. Gonon ; RTD civ. 1998, p.108, obs. J. Mestre ; Defrénois 1997, p.748, obs. J.-L. Aubert et p.1011, obs. Ph. Delebecque ; D. affaires 1997, p.411, préc ; Cass. 1ère civ., 29 févr. 2000, n°97-21.873 ; JCP G 2000, I, 257, n°7, obs. Ph. Simler et Ph. Delebecque ; JCP G 2000, II, 10382, note J. Casey ; Bull ; Cass. 1ère civ., 29 oct. 2002, n°01-01.897 ; Cass. 1ère civ., 5 mai 2004, n°02-17.155: ne peuvent être puisés dans les autres énonciations de l'acte, les éléments extrinsèques susceptibles de compléter un commencement de preuve par écrit (en l'espèce, un acte de cautionnement irrégulier). *Contra* : Cass. com., 31 mai 1994 (2 arrêts) : Bull. civ. 1994, IV, n°191 et 193 ; JCP G 1994, IV, 1948 ; RTD civ. 1994, p.903, obs. M. Bandrac ; Cass. com., 11 juin 2003, n°00-18.390.
[760] D. Legeais, Fasc. 2160 : Blockchain, JCl. Sociétés, Lexis Nexis, 29 mai 2018 (maj 29 janv. 2019), n°54.

312. **Une valeur restreinte en pratique.** Un commencement de preuve par écrit d'une transaction complexe serait une preuve imparfaite mais la réforme du droit des contrats permet tout de même de « *suppléer l'écrit* »[761]. Nonobstant cette place renforcée du commencement de preuve par écrit par la réforme du droit des contrats et le développement des nouvelles technologies (notamment l'essor de l'écrit numérique), l'effet du commencement de preuve par écrit est en pratique restreint. Il met en évidence un contenu limité ne permettant pas d'étayer une démonstration et d'aller jusqu'au bout d'un raisonnement probatoire. Souvent le commencement de preuve par écrit et son complément peuvent prouver un versement de fonds mais pas sa cause exacte, et la nature du contrat le justifiant non plus[762]. Par exemple, la preuve d'une remise de dette ne pourrait suffire à justifier celle d'un prêt et entraîner une obligation de restitution[763]. De cela, le cas d'une remise de dette opérée en crypto-actif pourrait constituer un commencement mais ne déterminant pas la cause de cette remise, ni l'éventuel contrat sous-jacent à cette transaction.

Section 2 : La qualification juridique de droit commun envisagée pour les données signées dans le registre de la *blockchain*

313. Dans la lignée des débats assez anciens sur la reconnaissance de la signature électronique et ses modalités d'application[764], la doctrine - avec une acuité nouvelle - soulève la problématique de la qualification de la signature établie par la *blockchain* et se penche sur la valeur des données signées grâce à cette technologie[765]. Aux fondements de la doctrine civiliste

[761] C. Civ., art. 1361.Voir : E. Vergès, « Droit de la preuve : une réforme en trompe-l'œil », *op.cit.*, p.840.
[762] Cass. 1ère civ., 19 oct. 2004, n°93-15.978 : O. Audic, *op.cit.*, n°243.
[763] Cass. 1ère civ., 28 févr. 1995 ; Bull. civ. 1995, I, n°107 ; D. 1995, somm. p.228, obs. R. Libchaber ; Defrénois 1995, p.735, art. 36100, n°59, obs. Ph. Delebecque : concernant des billets constatant la réception d'une somme.
[764] J. Huet, « Vers une consécration de la preuve et de la signature électronique », D. 2000 n°6, p.95 : P-Y. Gautier et X. Linant de Bellefonds, « De l'écrit électronique et des signatures qui s'y attachent », JCP E, août 2000, p.1273-1280 ; E. Caprioli, « La loi française sur la preuve et la signature électroniques dans la perspective européenne, Dir. 1999/93/CE du Parlement européen et du Conseil 13 décembre 1999 », JCP G n°18, 3 mai 2000 p.787 : E. Caprioli. « La loi type de la CNUDCI sur les signatures électroniques », chron. 27, Com. com. élect., déc. 2001, p.9 ; C. Charbonneau, J.-F. Pansier, « La signature électronique, signature sous surveillance (à propos du décret n°2001-272 du 30 mars 2001) », Petites affiches n°69, 6 avr. 2001, p.6 ; T. Samman, N. Neveux, « La signature électronique : mythe et réalité » Expertises, févr. 2001 p.48, juin 2001 p.213, et juin 2002 p.213 ; F. Schwerer, « Réflexions sur la preuve et la signature dans le commerce électronique », Contrats, Conc., Consom., déc. 2000, p.4 ; E. Passant, « La loi du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique : nouvelle donne pour le droit de la preuve », Cahiers Lamy droit de l'informatique et des réseaux n°125, mai 2000, p.7 ; H. Bitan. « La signature électronique : comment la technique répond-elle aux exigences de la loi », Gaz. Pal. 19/20 ; juill. 2000 p.10.
[765] M. Mekki, « Les mystères de la blockchain », *op.cit.*, p.2168, n°27 ; A. Barbet-Massin, « Le droit de la preuve des œuvres d'art », *in* Smart contract : Etudes de cas et réflexions juridiques, Open Law/Coala, mars 2018, p.16 ;

- tant pour sa preuve que pour la formation des actes -, la signature peut se définir selon deux catégories.

314. La première est la signature matérielle au sens fonctionnel générique qui est un signe par lequel le signataire s'affirme comme l'auteur de ce qu'il signe (lettre, œuvre, acte), marque personnelle intentionnelle qui manifeste son identité et concentre sur sa tête les effets attachés à son initiative[766]. Alors que la seconde est la signature immatérielle, autrement dit, celle qui a recours à des techniques de cryptographie sécurisées et fiables garantissant le lien électronique entre l'écrit électronique signé et la signature immatérielle elle-même. La signature électronique est une forme de signature immatérielle réglementée, qui est une donnée résultant de l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache[767].

315. Cette signature électronique est introduite en France de façon générale depuis la loi 13 mars 2000[768]. À l'issue d'un constat d'échec de la directive 1999/93/CE sur la signature électronique à l'échelle européenne[769] - dues aux transpositions de cette directive et choix techniques des États membres qui ne permettaient pas l'émergence d'un socle commun d'interopérabilité[770] -, l'adoption d'un règlement européen eIDAS par le Parlement européen et le Conseil de l'Union européenne a eu pour objectif d'uniformiser les pratiques et de mettre en place un cadre juridique européen harmonisé, visant à susciter la confiance dans les transactions électroniques au sein du marché intérieur[771]. Le règlement eIDAS, d'application directe dans tous les États membre, est entré en vigueur le 17 septembre 2014 et est applicable depuis le 1er juillet 2016 pour la majeure partie de ses dispositions. C'est l'ordonnance du 10 février 2016 sur la réforme du droit des contrats qui, dans le respect du cadre fixé par le règlement eIDAS, est venue modifier les articles sur la signature électronique dans le Code civil au sein du

A. Barbet-Massin, V. Dahan, « Les apports de la blockchain en matière de droits d'auteur », BRDA n°8-2018, 15 avr. 2018, Francis Lefebvre, p.23-24, n°15-16 ; A. Favreau, « L'avenir de la propriété intellectuelle sur la blockchain », Propriétés intellectuelles n°67, IRPI, avr. 2018, p.11 et s. ; F. G'Sell, « Preuve et signature numérique », *op.cit.*, p.102-104 ; T. Douville, « *blockchains* et preuve », *op.cit.*, p.2193-2194 : pour lui, « *la blockchain pourrait être intégrée au processus de signature électronique* » ; I. Ganavon, « Blockchain, PI et mode : enjeux de la *blockchain* au regard des règles relatives à la preuve électronique, Dossier Blockchain et preuve, Dalloz IP/IT n°2, févr. 2019, p.93-94.

[766] G. Cornu, *Vocabulaire juridique*, *op.cit.*, Voir signature sens n°1, p.967.

[767] G. Cornu, *Vocabulaire juridique*, *op.cit.*, Voir signature sens n°3, p.968.

[768] Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, art. 4, al.2.

[769] Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques.

[770] https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-reglement-eidas/ (31/05/2020).

[771] ANSSI, Règlement eIDAS. FAQ, VOIR Qu'est-ce que le règlement eIDAS ?, p.5, 16 janv. 2019.

deuxième alinéa de l'article 1367[772]. Le décret n°2017-1416 du 28 septembre 2017 relatif à la signature électronique[773] vient apporter des précisions sur les caractéristiques techniques du procédé permettant à une signature électronique de bénéficier d'une présomption de fiabilité, abrogeant par la même, le décret n°2001-272 du 30 mars 2001 qui précisait les modalités de validité de la signature électronique[774].

316. Cette section traitera de la manière dont les données signées dans la *blockchain via* la signature d'un participant viennent s'inscrire dans ce contexte. Les développements qui vont suivre revêtent une importance capitale puisque le Parlement européen suggère un éclaircissement quant à la validité de la signature *blockchain* soulignant que la « *(…) sécurité juridique concernant la validité d'une signature numérique cryptographique est une étape essentielle vers la facilitation de contrats intelligents* »[775]. La nature des données signées sont les transactions. C'est ainsi que par le jeu des clés publiques et clés privées des participants signent les transactions réalisées. Cette opération rejoint le procédé de signature *blockchain*[776]. Ce dernier tend à être qualifié de signature électronique par le droit commun. Trois sortes de signature sont applicables, selon un niveau graduel de fiabilité : une signature électronique simple, avancée ou qualifiée. La signature *blockchain* est de fait qualifiée de signature électronique simple (paragraphe 1) et nous constaterons et développerons qu'elle remplit difficilement les critères de la signature électronique avancée ou qualifiée (paragraphe 2).

Paragraphe 1 : L'assimilation possible de la signature *blockchain* à une signature électronique simple

317. La signature électronique simple est une donnée informatique liée à d'autres données. La signature électronique simple apparaît comme un « *sceau* » numérique qui sert à authentifier un document indépendamment de son auteur[777]. Elle est utilisée pour signer tous types de

[772] C. civ, ancien art. 1316-4 (n'a pas été modifié substantiellement).
[773] Décret n°2017-1416 du 28 septembre 2017 relatif à la signature électronique, publié au JORF n°0229 du 30 septembre 2017 texte n°8 : D. 2017, p.1976, com. T. Douville ; JCP A. n°41, oct. 2017, act. 449, obs. E. A. Caprioli ; JCP G. n°41, oct. 2017, 1047, obs. E. A. Caprioli.
[774] Décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique (abrogé).
[775] Parlement européen, Résolution du 3 oct. 2018 sur les technologies des registres distribués et les chaînes de blocs: renforcer la confiance par la désintermédiation (2017/2772(RSP)), P8_TA(2018)0373, point 37.
[776] Voir *supra* n°133-134.
[777] Contrat électronique entre professionnels, DPDA, Dalloz, n°76, janv. 2020 (mise à jour).

documents comme une facture, un bon de commande, un mandat de prélèvement SEPA ou encore des conditions générales de vente sur une plateforme de e-commerce. Les conditions de la signature électronique simple sont satisfaites par la signature établie par la *blockchain* (A), ce qui lui permettra de bénéficier d'effets simples (B).

A. Les conditions de la signature électronique simple satisfaites par la signature *blockchain*

318. **La définition européenne de la signature électronique simple conforme à la signature *blockchain*.** L'article 3, 10 du règlement eIDAS vise par la signature électronique selon sa version simple « *des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer* ». L'usage par la *blockchain* de la technique de la cryptographie asymétrique permet de générer un double jeu de clés publiques et privées pour l'émetteur de la transaction et le destinataire. Les clés publiques dans la *blockchain* sont des adresses publiques, un ensemble de données uniques sous forme de caractères électroniques de chiffres et de lettres qui sont associées à une transaction électronique de la *blockchain*. Le signataire dans la *blockchain* utilise son adresse publique pour réaliser une transaction à une autre adresse publique destinatrice qui sera signée par la clé privée du signataire[778]. Pour recevoir sa transaction, le destinataire doit lui aussi utiliser sa clé privée. Il ne fait aucun doute que la signature *blockchain* répond aux caractéristiques de la signature électronique simple visée par le règlement eIDAS puisque l'adresse publique, données sous forme électronique, sont jointes à d'autres données sous formes électroniques : la transaction en crypto-actifs. L'adresse publique et la transaction apparaissent ensuite sous forme d'un ensemble de données transactionnelles liées entre elles dans le registre d'une *blockchain*[779].

319. Cette position est confirmée de façon large par l'*European Blockchain Observatory and Forum* qui indique que le règlement « *eIDAS reconnaît trois niveaux différents de signatures électroniques : simple, avancé et qualifié et la blockchain semble répondre aux critères*

[778] Voir *supra* n°133.
[779] A. Barbet-Massin, « Le droit de la preuve des œuvres d'art », *op.cit.*, p.16.

techniques des deux premières »[780]. Si l'*European Blockchain Observatory and Forum* considère que la signature *blockchain* répond aux critères des signatures électroniques simples et avancées, elle reconnait *a fortiori* que la signature *blockchain* peut satisfaire aux conditions de la signature électronique simple et conséquemment être qualifiée comme telle.

320. **Le procédé fiable d'identification imposé par le législateur français.** Le législateur français impose dans le cadre des signatures électroniques classiques l'usage d'un procédé fiable d'identification. L'article 1367 du Code civil dans son deuxième alinéa précise que « *lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache* »[781]. Ce procédé fiable d'identification ne distingue pas selon la nature de la signature, simple, avancée ou qualifiée. Seulement, dans le contexte de la signature électronique simple, ce procédé fiable d'identification n'est pas présumé. La signature *blockchain* doit, dans le contexte d'une signature électronique simple, pouvoir justifier d'un tel procédé d'identification. Il est arrivé que la jurisprudence exige du plaideur qu'il apporte la preuve de ce procédé fiable d'identification par un fichier de preuve, un sceau d'horodatage, ou encore un document d'identité du signataire[782]. La jurisprudence admet la fiabilité du procédé pour une société qui mettait en place des pouvoirs pour les signatures qui respectaient des « *règles relatives à la souscription des contrats en ligne, l'utilisation de codes d'accès sécurisés, les accès et transmissions de pièces se faisant aussi en mode sécurisé, et les formulaires PDF imprimables* » et ainsi « *n'étant plus modifiables une fois transmis* »[783]. La *blockchain* publique n'accorde aucun de ces procédés fiables d'identification. Le seul moyen permettant au signataire d'obtenir ces éléments de preuve pour justifier auprès des tribunaux du procédé fiable d'identification utilisé pour une signature *blockchain* serait de faire appel à un prestataire externe qui pourra rassembler un ensemble de preuves sur le procédé de signature *blockchain*.

321. **L'absence d'exigence d'identification dans le règlement eIDAS pour la signature électronique simple favorable à la signature *blockchain*.** Le règlement européen, qui ne fait pas mention d'un procédé fiable d'identification, n'en exige pas tant dans sa définition de la

[780] EU Blockchain Observatory and Forum, Legal and regulatory framework of *blockchains* and smart contracts, *op.cit.*, p.12.
[781] C. civ., art. 1367, al. 2. Notons aussi que l'alinéa 1, de l'article 1367 sur la signature non électronique exige déjà cette identification, laquelle peut sembler faire doublon.
[782] CA Aix-en-Provence, Ch. 1-8, 26 sept. 2019, n°19/01866.
[783] CA Aix-en-Provence, 26 juin 2014, n°13/19600.

signature électronique simple. Elle vise par ailleurs une définition de l'« *identification électronique* » indépendamment de la signature comme « *le processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale* »[784] mais à laquelle la signature électronique simple ne fait pas de renvoi. Il ne s'agit pas à proprement parler d'une « *surtransposition* » ou « *goldplating* » de la norme européenne par le législateur français car la lettre de l'article 1367 du Code civil préexistait au règlement eIDAS[785]. Pour autant, elle est susceptible de créer les mêmes effets de distorsion concurrentielle qui porteraient préjudices aux opérateurs économiques français du secteur de la *blockchain*.

322. Du reste, force est d'admettre qu'un règlement européen a une portée générale et est de nature obligatoire dans tous ses éléments en vertu du traité sur le fonctionnement de l'Union européenne (TFUE)[786]. Il est donc permis de penser qu'une signature électronique simple accordée par la *blockchain* aurait tous les arguments pour être valide devant une juridiction nationale de l'un des États membres de l'Union européenne, sans la preuve d'un nécessaire procédé fiable d'identification. À cette signature électronique simple s'applique le principe de non-discrimination conformément à l'article 25 du règlement eIDAS. Sa recevabilité comme preuve en justice ne peut être refusée au seul motif qu'elle est électronique et, qui plus est, au motif de sa typologie de signature électronique simple. Ainsi, la signature électronique simple telle que visée par le règlement eIDAS ne peut être refusée si elle ne remplit pas les conditions de la signature électronique qualifiée. Précisons toutefois qu'une jurisprudence a récemment refusé de reconnaître la validité d'une signature électronique non qualifiée contrairement à ce que préconise le droit européen[787]. Dans ce contexte jurisprudentiel français incertain, il

[784] Règl. eIDAS, art. 3, 1

[785] La surtransposition est le fait que dans les hypothèses de négociations complexes d'un texte européen, il peut être prévu l'ouverture d'options ou la possibilité de dérogations pour les États membres, si bien que son application peut exiger l'adoption de mesures nationales, ne serait-ce que pour abroger des normes incompatibles. Elle peut donc conduire à aller au-delà des obligations européennes créant un différentiel proprement national à la règle européenne (Sénat, Rapport d´information fait au nom de la commission des affaires européennes et de la délégation aux entreprises relatif à la surtranspositions préjudiciables aux entreprises d'actes législatifs européens en droit interne, par R. Danesi, le 28 juin 2018, p.9).

[786] TFUE (versions consolidées du Traité sur l'Union européenne et du Traité sur le fonctionnement de l'Union européenne 2016/c 202/01), art. 288, al. 2.

[787] CA Rouen, ch. prox., 31 mai 2018, n°17/03404 : Com. com. élec. oct. 2018 com. E. A. Caprioli.

conviendra d'étayer la preuve de la signature *blockchain* par un ensemble d'autres preuves concordantes à cette validité comme un fichier de preuve[788].

B. Les effets probatoires simples accordés à la signature *blockchain*

323. **Le principe de non-discrimination appliqué aux effets de la signature *blockchain*.** L'assimilation vraisemblable de la signature générée par la *blockchain* à une signature électronique simple permet d'accorder à cette signature les bénéfices d'effets uniquement simples. À défaut de présomption de fiabilité du procédé d'identification attachée à la signature électronique qualifiée, la signature électronique simple n'apporte aucune garantie sur l'identité du signataire mais le lien entre une adresse publique et la transaction, à l'inverse, est assuré. Le principe de non-discrimination s'applique aussi aux effets juridiques de la signature électronique simple[789]. Ces effets ne peuvent être annihilés. Par principe, ils ne peuvent pas être refusés au motif que la signature n'est pas électronique ou qu'elle n'est pas qualifiée.

324. **La signature *blockchain* d'une transaction constituant une signature originale.** Une partie peut prouver par tous moyens que la signature est originale contre la partie qui contesterait une transaction. Le juge tranchera en effet le titre le plus vraisemblable[790]. La signature simple aura donc les mêmes effets de validité que la signature qualifiée, charge à celui qui a signé de prouver la fiabilité de son procédé de signature. En cas de dénégation de signature, le juge sera aussi dans l'obligation de vérifier si les conditions de l'article 1367 du Code civil relatif à la validité de la signature sont satisfaites[791]. La jurisprudence confirme que les juges du fond doivent vérifier les conditions de fiabilité de la signature avant d'être en mesure de refuser une signature électronique non qualifiée[792], ce qui pourra être difficilement étayé pour la signature *blockchain*. Le doute ci-avant éprouvé sur le procédé fiable d'identification subsiste donc[793].

---

[788] Un courant jurisprudentiel récent consacre le fichier de preuve comme une preuve capitale d'une signature électronique valide (CA Aix-en-Provence, ch. 1-8, 26 sept. 2019, n°19/01866 ; TI Nîmes, 18 sept. 2018). Pour certains auteurs un fichier de preuve est donc d'une importance fondamentale dans la démonstration de l'existence d'une signature (I. renard, « signature électronique. Vers une meilleure reconnaissance par les tribunaux de fond ? », Expertises des Systèmes d'information, dec. 2018, p.426).
[789] Règl. eIDAS, art. 25.
[790] C. civ., art. 1368.
[791] C. proc. civ., art. 287, al. 2.
[792] Cass. 1ère civ., 6 avril 2016 n°15-10732.
[793] Voir *supra* n°320.

325. **Limite technique des effets de la signature *blockchain*.** Relevons cependant que les effets de la signature *blockchain* pourraient dépendre de la durée de vie des algorithmes utilisés, à l'instar de l'algorithme ECDSA pour Bitcoin. Comme pour d'autres solutions de signatures électroniques traditionnelles, il se pourrait qu'un individu trouve une façon de casser l'algorithme. Cette hypothèse ne remettrait pas en cause le pseudonymat du participant faisant usage de son compte dans une *blockchain* mais un individu malveillant pourrait tout à fait signer à la place de ce signataire originel. Cela rendrait ainsi le compte fragile[794].

Paragraphe 2 : L'analogie discutée de la signature *blockchain* avec une signature électronique avancée et qualifiée

326. La possibilité d'assimiler la signature *blockchain* à la signature électronique avancée et qualifiée est largement remise en question par la difficile satisfaction aux conditions prévues par ces signatures (A)[795]. Par voie de conséquence, des effets probatoires renforcés ne sauraient être accordés à la signature *blockchain* (B).

A. Les conditions de la signature électronique avancée et qualifiée à satisfaire par la signature *blockchain*

327. Les conditions des signatures électroniques avancées et qualifiées n'étant pas remplies pour les *blockchains* publiques, il convient de rejeter la qualification de signature électronique avancée et qualifiée pour la signature *blockchain* (1). Ce postulat pourrait être nuancé si tant est que la signature *blockchain* soit aménagée dans le contexte d'une *blockchain* privée, ce qui n'est pas une conjecture à généraliser (2).

[794] Entretien avec J. P.Delahaye, laboratoire CRYStAL (UMR 9189), Univ. Lille, le 20 janv. 2020.
[795] Voir un autre avis sur la qualification de la signature *blockchain* de signature électronique avancée : F. G'sell, « Preuve et signature numérique », *op.cit.*, p.103, 104, 108.

1. Le rejet de la signature électronique avancée et qualifiée pour les signatures par *blockchain* publique

328. Les signatures électroniques avancées et qualifiées ne peuvent pas être retenues pour deux raisons, tenant au critère d'identification (a) et à l'intervention d'un tiers de confiance qualifié exigée par la signature électronique qualifiée (b).

a. Le critère de l'identification comme obstacle à la qualification de signature électronique avancée

329. **La fonction de la signature électronique avancée.** La signature électronique avancée assure l'identité du signataire et l'adhésion de celui-ci à l'acte[796]. Cette signature est souvent adoptée dans le cadre de contrats de crédits ou compromis de ventes immobilières par exemple. Elle doit permettre d'identifier, être liée aux données auxquelles elle se rapporte, de telle sorte que toute modification ultérieure des données soit détectable, et être créée à l'aide de données de création de signature[797], pour que le signataire puisse avec un niveau de confiance élevé, l'utiliser sous son contrôle exclusif. Précisément, la signature générée par la *blockchain* doit répondre aux exigences visées à l'article 26 du règlement eIDAS pour être considérée comme une signature électronique avancée.

330. **Le lien univoque de l'adresse publique au signataire.** La signature par la *blockchain* doit, tout d'abord, être liée au signataire de manière univoque[798]. Une signature *blockchain* est liée de la transaction au signataire de manière univoque par son adresse publique, la clé publique du signataire, identifiant unique lui étant réservé. Cette mention est inscrite de manière inaltérable dans le registre de la *blockchain* lorsqu'elle est publique. S'il est question de transactions complexes intégrant une empreinte numérique de données ou de documents par exemple, il est techniquement possible d'intégrer un lien hypertexte pointant vers ces données/ces documents hébergés en dehors de la *blockchain*[799], avec potentiellement une faculté de limiter l'accès lorsque l'acte est confidentiel.

[796] Contrat électronique entre professionnels, DPDA, Dalloz, n°77, janv. 2020 (mise à jour).
[797] Règl. eIDAS, art. 3, 13.
[798] Règl. eIDAS, art. 26, a).
[799] Voir en ce sens : R. Matzutt, J. Hiller, M. Henze, J.-H. Ziegeldorf, « A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin », *op.cit.*, p.1 et s. ; T. Douville, « *blockchains* et preuve », *op.cit.*, p.2193.

331. **Le pseudonymat des *blockchains* : le point d'achoppement avec la condition d'identification du règlement eIDAS.** La signature *blockchain* doit ensuite permettre d'identifier le signataire[800]. Cette condition d'identification des signataires est l'un des points d'achoppement de la *blockchain* avec le règlement eIDAS[801]. Il fait référence à la problématique plus générale de l'identification dans les blockchains développée ci-avant[802]. Les signatures *blockchains* n'identifient pas les participants à une transaction car elles utilisent la cryptographie asymétrique laissant seulement apparaître dans le registre l'adresse publique du participant, signataire à la transaction[803]. C'est donc un pseudonymat qui est instauré par ce procédé cryptographique.

332. Dans certaines *blockchains* anonymes les algorithmes de signature utilisés permettent de rendre intraçables les adresse publiques. Par exemple Monero utilise des « *signatures de cercle* » ou « *signatures d'anneau* » (ou *ring signatures*) par lesquelles plusieurs adresses sont inscrites, formant un cercle ou un anneau de clés lorsqu'une transaction est effectuée, et seule une sera utilisée de manière effective[804]. Cela étant dit, outre le pseudonymat, voire l'anonymat de certaines signatures *blockchains*, la notion même d'identification *via* la signature peut être remise en question.

333. **Critique de la notion d'identification dans la signature.** Rappelons que dans l'ancien droit, il n'était pas d'usage de signer[805] mais les parties se contentaient d'une marque quelconque, un cachet d'abord ou un sceau, puis un seing manuel[806]. Le principe de la preuve par écrit fut alors fixé par ordonnance en avril 1667 et c'est à ce moment que l'usage de la signature s'installa[807]. Il n'est pas sans nier le seuil qualitatif franchi par le passage du signe à la signature. Aujourd'hui, le verbe « *signer* » a pour sens commun, non plus de faire un signe (par exemple, une croix)[808], mais d'apposer sa signature, c'est-à-dire un nom, personnalisé par l'ajout d'un paraphe, un petit signe distinctif (trait, point, queue, arabesque), une empreinte digitale, une

[800] Règl. eIDAS, art. 26, b).
[801] Voir l'autre point d'acchopement *infra* n°339-346 (sur l'intervention d'un PSCQ).
[802] Voir *supra* n°298 et s.
[803] Voir *supra* n°133 et s.
[804] OPECST, Les enjeux technologiques des *blockchains* (chaînes de blocs), *op.cit.*, p.182.
[805] C. Demolombe, *Traité des contrats ou des obligations conventionnelles*, *op.cit.*, n°355.
[806] Le seing privé était un « *dessin utilisant les lettres du nom du signataire* » (J.-P.Lévy et A. Castaldo, *Histoire du droit civil*, coll. Précis, Dalloz, 1ère éd. 2002, n°584).
[807] V. D. Jousse, Nouveau commentaire sur l'ordonnance civile du mois d'avril 1667, t. 2 : Debure, Paris 1769.
[808] G. Baudry-Lacantinerie, *Précis de droit civil*, t. 2 : Larose et Forcel, Paris, 2e éd. 1886, n°1191 ; M. Planiol et G. Ripert, *Traité pratique de droit civil français*, t. 7, *op.cit.*, n°1458 ; Cass. 1ère civ., 12 juill. 1956 : Bull. civ. 1956, I, n°302 ; Cass. civ., 20 janv. 1897 : DP 1897, I, p.128 ; Cass. req., 8 juill. 1903 : DP 1903, I, p.507 ; Cass. 1ère civ., 15 juill. 1957 : Bull. civ. 1957, I, n°331.

signature à main assistée sous certaines conditions, ou encore une signature électronique. Mais tout compte fait, une signature ne permet « *ni de prouver ni même de présumer l'identité de son auteur* »[809]. La majorité des signatures matérielles sont illisibles, au graphisme indéchiffrable. La définition de signature introduirait une « *rigidité nocive* » avec cette exigence d'identification de l'auteur[810].

334. La signature, en réalité, identifie un signataire en présence physique du destinataire d'un acte mais elle ne donne aucune garantie et assurance sur un état civil donné. D'ailleurs, l'état civil n'est pas requis pour valider un acte, cette manifestation de l'identité n'est pas exigée par le Code civil[811]. Les actes juridiques effectués par des personnes qui ne permettent pas de les identifier (cas d'un pseudonyme par exemple), ne sont pas nécessairement invalides, illicites ou viciés du reste, sauf si la loi en dispose autrement. Autrement dit, ils donnent une indication sur l'auteur de l'acte mais n'indiquent pas précisément son identité. La jurisprudence a déjà admis qu'il soit possible de signer un acte authentique par un faux nom (ou un surnom), si celui-ci est celui que l'on porte effectivement[812].

335. Somme toute, l'identification du signataire dans le cadre de cette signature est fortement remise en cause, apparaissant comme une aporie, bien qu'il soit possible d'émettre de sérieuses critiques sur le critère d'identification du signataire dans la signature *blockchain*, non déterminante de la qualification même de signature.

336. **Les données de création de signature électronique sous le contrôle du signataire.** Troisièmement, la signature *blockchain* doit avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif[813]. Rappelons que les données de création de signature électronique sont des données uniques qui sont utilisées par le signataire pour créer une signature électronique[814]. Nous pouvons considérer que ces données renvoient à celles liées à la clé privée d'une signature *blockchain*. En effet, l'ancien décret n°2001-272 du 30 mars 2001 désormais abrogé indiquait

[809] I. Dauriac, *La signature*, *op.cit.*, n°209.
[810] A. Raynouard, « Adaptation du droit de la preuve aux technologies de l'information et à la signature électronique », Defrénois, 30 mai 2000, p.593.
[811] C. civ., art. 1128 : seul le consentement des parties, la capacité à contracter et le contenu licite et certain sont exigés en tant que conditions de validité du contrat.
[812] Cass. req., 20 oct. 1908 : DP 1910, I, p.291. Cette décision serait applicable *a fortiori* à un acte sous signature privée (D. Guével, D., Fasc. unique : contrats et obligations – Actes sous seing(s) privé(s) – Règles générales, JCl. Civil Code, art. 1322 à 1324, Lexis Nexis, mars 2012 (maj dec. 2018), p.9, n°23).
[813] Règl. eIDAS, art. 26, c.
[814] Règl. eIDAS, art. 3,13.

que ces données de création de signature étaient des « *éléments propres au signataire, tels que des clés cryptographiques privées, utilisés par lui pour créer une signature électronique*»[815]. Les données de la clé privée des participants à la *blockchain* devront ainsi être sous le seul contrôle du signataire. Il semblerait que l'interprétation stricte de cette condition ne permette pas de déléguer la gestion de la conservation d'une clé privée et les données associées à un PSAN chargé de réaliser une prestation de conservation de clés cryptographiques privées permettant l'accès à des actifs numériques[816], alors qu'elle est usuelle en pratique. Cette condition pourrait apparaître comme bloquante à moins de stipuler expressément dans une convention que le signataire autorise ce prestataire à gérer sa clé privée et les données associées en son nom et pour son compte, en dehors des moments où il signe. En effet, la condition du contrôle des clés privées du signataire du règlement eIDAS semble faire référence au moment où celui-ci en a l'usage mais non aux autres moments annexes de sécurisation de cette clé.

337. **Le lien entre les données associées à la signature *blockchain* garantissant l'intégrité.** Quatrièmement et dernièrement, la signature générée par la *blockchain* devra être liée aux données associées à cette signature de telle sorte que toute modification ultérieure de ces données soit détectable[817]. Cette condition sous-tend une garantie d'intégrité des données signées, si bien que les données signées ne sont pas modifiées ou détectables à tout le moins si elles le sont. Si cette garantie d'intégrité sera assurée par le registre de la *blockchain* grâce aux empreintes successives des blocs liés entre eux, elle le sera moins par la signature elle-même.

338. Ajoutons que la signature électronique qualifiée se satisfait des critères mentionnés ci-avant de la signature électronique avancée et ajoute une condition supplémentaire de certificat qualifié de signature électronique exigeant l'intervention d'un tiers de confiance qualifié[818], second obstacle à la possible qualification de signature électronique qualifiée pour la signature *blockchain*.

[815] Décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique, art. 1,4 (abrogé).
[816] C. mon. fin, art. 54-10-20, 1°.
[817] Règl. eIDAS, art. 26, d.
[818] Règl. eIDAS, art. 3, 12.

b. L'intervention d'un tiers de confiance qualifié comme obstacle à la qualification de signature électronique qualifiée

339. **La fonction de la signature électronique qualifiée.** La signature électronique qualifiée est selon l'article 3.12 du règlement eIDAS « *une signature électronique avancée qui est créée à l'aide d'un dispositif de création de signature électronique qualifié, et qui repose sur un certificat qualifié de signature électronique* »[819]. La signature électronique qualifiée assure davantage de sécurité technique et juridique en offrant un certificat - accordé par un prestataire de services de confiance qualifié (PSCQ) - qui lie les données concernant la vérification de signature au signataire, et donne ainsi des informations du porteur de la clé privée et clé publique[820]. Cette signature est utilisée généralement pour des actes authentiques, des actes d'avocats, d'huissiers de justice, des greffes des tribunaux ou encore des contrats de la commande publique.

340. Pour être qualifiée, la signature électronique doit répondre à trois conditions. Elle doit satisfaire premièrement aux mêmes conditions que celles de la signature avancée. La condition de l'identification pose, comme nous l'avons relevé, des difficultés et empêche ainsi la reconnaissance du caractère qualifié de la signature *blockchain*. La *blockchain* publique fait classiquement obstacle à ce critère, rendant irréductible le critère d'identification.

341. **Le dispositif de création de signature électronique qualifié.** Deuxièmement, le dispositif de création de signature électronique, c'est-à-dire, un dispositif logiciel ou matériel configuré servant à créer une signature électronique, doit être qualifié[821]. Le dispositif de création de signature électronique qualifié doit respecter un ensemble d'exigences précises visées à l'annexe II du règlement eIDAS. Une décision d'exécution de la Commission du 25 avril 2016 indique les normes techniques applicables[822], et ce dispositif doit être certifié par les organismes désignés par les États membres[823]. Un prestataire, comme un prestataire de

[819] Règl. eIDAS, art. 3, 12.
[820] Contrat électronique entre professionnels, DPDA, Dalloz, n°78, janv. 2020 (mise à jour).
[821] Définition du dispositif de création de signature électronique issue du règlement eIDAS (Règl. eIDAS, art. 3, 22).
[822] Règl. eIDAS, annexe II et Décision d'exécution (UE) 2016/650 de la Commission du 25 avril 2016 établissant des normes relatives à l'évaluation de la sécurité des dispositifs qualifiés de création de signature électronique et de cachet électronique conformément à l'article 30, paragraphe 3, et à l'article 39, paragraphe 2, du règlement (UE) n°910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, publié au JOUE n°L.109, 26 avr. 2016.
[823] Règl. eIDAS, art. 30.

portefeuille, ou le participant lui-même, génère des clés attachées à un compte mais ce dispositif de création de signature n'est pas qualifié puisqu'il ne remplit pas les exigences complètes de l'annexe II s'agissant spécifiquement de l'obligation de confier à un PSCQ la génération ou la gestion de données de création de signature électronique pour le compte du signataire.

342. **La vérification par le certificat électronique qualifié.** Troisièmement, la signature électronique qualifiée doit être vérifiée par l'utilisation d'un certificat électronique qualifié délivré par un PSCQ[824]. La fourniture de services de confiance qualifiés est soumise à une autorisation préalable. Les prestataires de service de confiance (PSC) sont des personnes physiques ou morales qui, pour devenir PSCQ doivent joindre à leur demande un rapport d'évaluation de la conformité[825] délivré par un organisme d'évaluation de la conformité accrédité[826]. Un organe de contrôle s'assurera alors du respect des exigences posées par le règlement, lui délivrera le cas échéant le statut de PSC « *qualifié* »[827] pour enfin, l'inscrire sur la liste de confiance des PSCQ[828]. Leur contrôle est assuré par un organe désigné par l'État membre du lieu de leur d'établissement[829]. En France, l'organe compétent pour exercer ce contrôle est l'Agence Nationale des Systèmes d'Information (ANSSI), l'autorité nationale en matière de sécurité des systèmes d'information chargée d'assister le Secrétaire général de la défense et de la sécurité nationale (SGDSN)[830].

343. En pratique, il conviendra que le PSCQ vérifie l'identité du signataire de manière fiable à l'occasion de la délivrance du certificat par le PSCQ[831]. Cette vérification d'identité pourra intervenir en physique ou par l'utilisation d'un moyen d'identification électronique à distance[832], par un certificat de signature électronique qualifié ou un cachet électronique qualifié[833], mais la vérification pourra également se faire « *à l'aide d'autres méthodes d'identification reconnues*

[824] Règl. eIDAS, art. 28 et 3, 15.
[825] Règl. eIDAS, art. 21, 1.
[826] Règl. eIDAS, art. 3.18 : envoie aux organismes d'évaluation de la conformité de l'article 2, point 13), du règlement (CE) n°765/2008 ; PE et Cons. UE, règl. n°765/2008, 9 juill. 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le Règlement n°339/93 du Conseil, art. 2, pt. 13 : JOUE n°L 218, 13 août 2008, p.30.
[827] Règl. eIDAS, art. 21, 2.
[828] Règl. eIDAS, art. 21, 2. et art. 22. Voir également : Comm. UE, déc. exéc. 2015/1505, 8 sept. 2015 établissant les spécifications techniques et les formats relatifs aux listes de confiance visées à l'article 22, paragraphe 5, du règlement eIDAS : JOUE, n°L 235, 22 sept. 2015, p.26.
[829] Règl. eIDAS, art. 17, 1 et 2.
[830] Décret n°2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information ».
[831] Règl. eIDAS, art. 24, 1.
[832] Règl. eIDAS, art. 24, 1, a et b.
[833] Règl. eIDAS, art. 24, 1, c.

au niveau national qui fournissent une garantie équivalente en termes de fiabilité à la présence en personne »[834]. Imaginons, par exemple, une technique reposant sur la comparaison de l'image de la personne avec celle d'un titre d'identité qui fait l'objet d'un contrôle d'intégrité à distance[835].

344. Le certificat électronique, en lui-même, est une attestation électronique qui associe les données de validation d'une signature électronique à une personne physique et confirme son nom ou son pseudonyme[836]. Le certificat est une forme de carte d'identité électronique qui permet d'établir un lien entre une personne et sa signature électronique[837], en l'absence du nom du signataire apparent, à l'instar de la signature manuscrite.

345. L'absence de vérification de signature par un PSCQ attestée par la délivrance d'un certificat ne permet pas au procédé de signature de la *blockchain* de bénéficier de la qualification de signature électronique qualifiée. La nécessaire ré-intermédiation du PSCQ dans la signature électronique qualifiée est tout à fait critiquable dans le contexte de la *blockchain*. L'alourdissement du processus probatoire est exactement ce que la technologie cherche à abolir en théorie. Partant, l'intervention de ce tiers est un obstacle à l'assimilation de la signature électronique qualifiée pour une signature *blockchain*. Elle constitue plus largement la seconde pierre d'achoppement entre la signature *blockchain* et le règlement eIDAS.

346. En définitive, les critères d'identification et celui de l'intervention d'un tiers de confiance qualifié faisant défaut dans la signature par la *blockchain* publique classique, celle-ci sera exclue de la qualification des signatures avancées et qualifiées. Cela ne signifie pas pour autant que les signatures électroniques accordées par la *blockchain* sont dépourvues de valeur probante[838].

[834] Règl. eIDAS, art. 24, 1, d.
[835] T. Douville, « Informatique - Le règlement européen sur l'identification électronique et les services de confiance (eIDAS) – Etude », JCP E n°1, 5 Janv. 2017, n°13.
[836] Règl. eIDAS, art. 3, 14.
[837] F. Schuhl, *Cyberdroit. Le droit à l'épreuve de l'Internet*, Praxis Dalloz, 2018-2019, n°522.24, p.1168.
[838] Confirmé par le Ministère de la Justice : Question écrite n°22103 de D. Fasquelle, publiée au JO le 30/07/2019, réponse du Ministère de la Justice publiée au JO le 10/12/2019, p.10774. Voir annexe n°10.

2. La possible qualification de signature électronique avancée et qualifiée pour les signatures par *blockchain* privée ou par *blockchain* publique permissionnée après un aménagement

347. Les *blockchains* privées ou les *blockchains* publiques permissionnées pourraient venir canalyser la problématique de l'identification si elles organisent, par leurs procédés de signature, l'identification des participants.

348. **L'intervention d'un PSCQ dans les *blockchains* privées ou les *blockchains* publiques permissionnées.** Tout compte fait, si la *blockchain* privée ou publique permissionnée peut remplir la condition d'identification, il n'y a plus d'obstacle à la qualification de la signature avancée mais celle de signature électronique qualifiée implique l'aménagement de l'intervention d'un tiers. Il serait tout à fait envisageable de faire intervenir un PSCQ, ce qui lèverait le point bloquant à la qualification de signature électronique qualifiée. Des solutions techniques comme la multisignature permettent à ce jour de signer dans une *blockchain* avec un tiers de confiance[839]. L'*UE blockchain Observatory* soutient que les signatures décentralisées pourraient être employées jusqu'à un haut niveau de confiance, notamment par la reconnaissance des *blockchains* au sein des solutions de fournisseurs de services de confiance[840].

349. Notons toutefois que la jurisprudence est particulièrement vigilante quant à l'appréciation de la preuve du procédé mettant en œuvre la signature électronique qualifiée ainsi que la vérification de cette signature par un certificat qualifié délivré par le PSCQ[841]. Les solutions basées sur la technologie *blockchain* qui prévoient la délivrance de certificats fantaisistes, mais certainement pas qualifiés au sens des exigences du règlement eIDAS, ne sauraient donc être admis par les juges. Notons que cette technologie est à l'étude par certains fournisseurs de service de confiance délivrant des certificats qualifiés[842]. Il serait tout à fait possible de prévoir cette éventualité de générer un certificat dans le cadre d'une solution blockchain, soit automatiquement, soit par l'intervention du PSCQ qui associerait les données

[839] Voir *supra* n°285.
[840] EU Blockchain Observatory and Forum, Blockchain and digital identity, *op.cit.*, p.22.
[841] CA Dijon, 28 juin 2018, n°17/01790 ; CA Rouen, Ch. de la proximité, 31 mai 2018, n°17/03404 ; CA Chambéry, 2ème ch., 25 janv. 2018, n°17/01050.
[842] https://www.docusign.com/products/*blockchain* (consulté le 31/05/2020).

de validation de la signature électronique. Celui-ci serait sécurisé ou non dans la *blockchain* par son ancrage.

350. Le règlement eIDAS mentionne que le certificat électronique qualifié peut faire apparaître dans les mentions obligatoires le pseudonyme du signataire[843]. Ce pseudonyme, comme une adresse publique, devra être clairement indiqué.

351. Enfin, le recours à ce PSCQ accroit également le coût de l'investissement initial dans une solution basée sur la technologie *blockchain* et constitue précisément ce que cette architecture distribuée est censée éviter. Pour la Professeure Florence G'Sell, « *une telle situation n'est pas satisfaisante : il conviendrait ici que la blockchain permette, précisément, de s'affranchir du recours aux services d'un tiers certificateur tout en offrant une réelle sécurité juridique* »[844]. Remarquons cependant que les États membres pourront toujours reconnaître d'autres prestataires[845], propres à la *blockchain*, ce qui permettrait d'ajuster les coûts et de créer un genre spécifique d'acteurs liés à cette signature. Ces derniers ne bénéficieront pas néanmoins d'une reconnaissance transfrontalière[846]. Par exemple, des prestataires ont été mis en place pour les services de coffre-fort numérique par la loi dite « *République numérique* »[847].

352. **L'avis de l'*European Blockchain Observatory*.** Selon l'*European Blockchain Observatory*, pour être juridiquement contraignantes, les signatures *blockchains* doivent répondre aux normes les plus élevées. Cette norme la plus élevée correspond ainsi à l'usage de la signature électronique qualifiée, ce qui requiert le recours aux services d'un PSCQ. C'est pourquoi en l'état actuel, selon cet Observatoire, les transactions de la *blockchain* elles-mêmes n'auraient pas de force juridique[848].

---

[843] Règl. eIDAS, annexe IV, c).
[844] F. G'Sell, « Preuve et signature numérique », *op.cit.*, p.104.
[845] Règl. eIDAS, cons. 25.
[846] T. Douville, « Informatique - Le règlement européen sur l'identification électronique et les services de confiance (eIDAS) – Etude », JCP E n°1, 5 Janv. 2017, n°13.
[847] Loi n°2016-1321 du 7 octobre 2016 pour une République numérique, art.87.
[848] EU Blockchain Observatory and Forum, Legal and regulatory framework of *blockchains* and smart contracts, *op.cit.*, p.12 : « *The situation is more complex when it comes to eSignatures and eSeals (signatures of a legal entity as opposed to a natural person). eIDAS recognises three different levels of eSignatures: simple, advanced and qualified. blockchains would appear to meet the technical criteria for the first two. But to be legally binding they need to meet the highest standard. That requires using the services of a recognized Trust Service Provider (TSP), or undergoing the arduous process of becoming a recognized TSP yourself. For this reason from an eIDAS perspective, blockchain transactions do not have legal authority by themselves* ». Voir *supra* n°322 la position contraire.

B. Les effets probatoires renforcés accordés à certaines signatures *blockchains*

353. Il revient en principe aux États membres de définir les effets juridiques produits par les signatures électroniques visées par le règlement eIDAS[849]. En revanche, elles bénéficient toutes du principe de non-discrimination : elles produisent des effets juridiques et sont également recevables en justice. Lorsqu'elles sont qualifiées, les signatures disposent en outre d'une reconnaissance mutuelle dans tous les autres États membres[850]. En France, les effets probatoires accordés à certaines signatures *blockchains* qui remplissent les conditions d'une signature électronique qualifiée sont liés essentiellement à la manifestation du consentement du signataire (1) et à la charge de la preuve (2).

1. La manifestation du consentement du signataire

354. **La manifestation du consentement du signataire matérialisée par la signature *blockchain***. Selon l'article 25, 2 du règlement eIDAS, la signature électronique qualifiée est équivalente à la signature manuscrite. C'est dans le Code civil qu'il convient de puiser les effets de la signature manuscrite à appliquer à la signature électronique qualifiée générée par la *blockchain*. Elle permettrait de manifester le consentement dudit signataire en vertu du premier alinéa de l'article 1367 du Code civil. La signature qualifiée par la *blockchain* accorderait la manifestation du consentement du signataire à réaliser une transaction. La fonction essentielle de la signature manuscrite est de manifester l'appropriation du contenu de l'acte par la signature qui valide l'acte juridique[851]. La signature qualifiée générée par la *blockchain* impliquant un transfert de crypto-actifs pourrait manifester le consentement de l'émetteur quant à la vente et du destinataire quant à l'achat de ces crypto-actifs. Cet effet est applicable « *aux obligations qui découlent d'un acte juridique* », ce qui ne sera pas nécessairement le cas dans une transaction simple, complexe, voire une simple inscription réalisée dans la *blockchain*. Pour néanmoins aller jusqu'au bout du raisonnement sur la reconnaissance d'une signature électronique qualifiée pour certaines signatures *blockchains*, il serait possible d'imaginer que la signature liée au *smart contract* manifeste le consentement au *smart contrat*, consentement indépendant qu'il conviendra, malgré tout, de réitérer dans le cadre du contrat autonome établi

[849] Règl. eIDAS, cons. 49.
[850] Règl. eIDAS, art. 25, 3 et 35, 3.
[851] I. Dauriac, *La signature*, thèse ss. dir. M. Gobert, Paris 2, 1997, n°209.

au préalable[852]. Il nous est cependant permis d'émettre de sérieux doutes sur la possibilité de vérifier le consentement (l'absence de trouble mental[853] ou encore de vices[854]) du signataire au sens du droit commun même dans le cadre d'une signature *blockchain* qualifiée.

2. La charge de la preuve

355. **La présomption simple de fiabilité du procédé.** La fiabilité du procédé de signature électronique qualifiée est présumée jusqu'à preuve contraire, « *lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'État* »[855]. En France, le décret du 28 septembre 2017 précise dans son premier article que « *la fiabilité d'un procédé de signature électronique est présumée, jusqu'à preuve du contraire, lorsque ce procédé met en œuvre une signature électronique qualifiée* »[856]. Pour répondre à la signature électronique qualifiée, le décret renvoie aux conditions des articles 26, 28 et 29 du règlement eIDAS. C'est une simple présomption qui peut être renversée.

356. **Une question de charge de la preuve et non de validité de la signature électronique.** Cette présomption réfragable n'affecte pas la validité de la signature mais uniquement la charge de la preuve de la fiabilité du procédé. La charge de la preuve repose sur celui qui dénie la signature. Il doit prouver que la signature électronique contestée n'émane pas de lui. En cas de doute, le contestataire se voit donc opposer l'acte électronique litigieux[857]. La présomption de fiabilité des signatures électroniques qualifiées permet donc de bénéficier d'un régime dérogatoire dans la procédure de dénégation d'écriture[858]. Ce sera au juge de déterminer si les éléments dont il dispose justifient le renversement de cette présomption[859]. Or, ce ne sera pas le cas pour les signatures électroniques simples et avancées, pour lesquelles le juge sera dans l'obligation de vérifier si les conditions de l'article 1367 du Code civil relatives à la validité de la signature sont satisfaites. Ainsi, si la signature est qualifiée dans une *blockchain* privée ou

[852] Voir les développements *infra* n°416.
[853] C. civ., art. 1129.
[854] C. civ., art. 1130.
[855] C. civ., art. 1367, al. 2.
[856] Décret n°2017-1416 du 28 septembre 2017 relatif à la signature électronique, art. 1.
[857] Contrat électronique entre professionnels, DPDA, Dalloz, n°77, janv. 2020 (mise à jour).
[858] C. proc. civ., art. 287 et s.
[859] C. proc. civ., art. 288-1.

publique permissionnée, par exemple, elle bénéficiera des avantages de la charge de la preuve au sujet de la présomption de fiabilité de la signature. Pour les autres cas, c'est au demandeur qu'il appartiendra de prouver la fiabilité de la signature.

Section 3 : La qualification juridique de droit commun envisagée pour les données datées dans le registre de la *blockchain*

357. La *blockchain* associe aux données entrées dans son registre des dates permettant de garantir la temporalité d'une donnée, d'un acte, d'un document. Cette temporalité se situe à deux moments dans la *blockchain* : à la date de l'entrée de la transaction soumise à validation par les validateurs et à la date de la validation du bloc de transaction. La datation de ces données dans la *blockchain* rejoint le procédé d'horodatage électronique reconnu en droit. Les textes généraux sont prévus par le règlement eIDAS et des textes spéciaux s'ajoutent également à l'horodatage en droit français dans le Code civil, notamment celui des courriers expédiés ou reçus par voie électronique pour la conclusion ou l'exécution d'un contrat[860] ou encore celui de la copie[861]. L'horodatage électronique peut être de deux sortes selon le règlement eIDAS : un horodatage électronique simple ou qualifié. L'horodatage effectué par la *blockchain* peut être qualifié d'horodatage électronique simple (paragraphe 1), mais cette qualification aurait tendance à lui conférer des effets insuffisants (paragraphe 2).

Paragraphe 1 : L'assimilation possible de l'horodatage *blockchain* à un horodatage électronique simple

358. La qualification qu'il est possible de retenir de l'horodatage par la *blockchain* se rapporte à celle de l'horodatage simple car les conditions de ce dernier sont satisfaites (A) et elle semble moins appropriée que celle de l'horodatage électronique qualifié (B).

[860] Décret n°2011-434 du 20 avril 2011 relatif à l'horodatage des courriers expédiés ou reçus par voie électronique pour la conclusion ou l'exécution d'un contrat, publié au JORF n°0094 du 21 avril 2011, p.7093, texte n°51

[861] Décret n°2016-1673 du 5 décembre 2016 relatif à la fiabilité des copies et pris pour l'application de l'article 1379 du code civil, publié au JORF n°0283 du 6 décembre 2016, texte n°61. Voir l'article 3 qui présume l'intégrité de la copie via une empreinte électronique par l'usage de l'horodatage électronique qualifié.

A. Les conditions de l'horodatage électronique simple satisfaites par l'horodatage *blockchain*

359. **Fonction de l'horodatage électronique simple.** L'horodatage électronique simple est visé par le règlement eIDAS comme celui pour lequel « *des données sous forme électronique* (qui) *associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant* »[862]. Cet horodatage bénéficie du principe de non-discrimination à l'instar de la signature électronique simple[863]. Sa recevabilité comme preuve en justice ne peut être refusée au seul motif qu'il est sous forme électronique et qu'il ne remplit pas les conditions de l'horodatage électronique qualifié.

360. **Assimilation de l'horodatage *blockchain* à un horodatage électronique simple.** L'entrée des transactions de la *blockchain* publique soumises pour validation aux mineurs est, d'une part, associée à un horodatage indiquant la date et l'heure d'entrée de la transaction. D'autre part, les blocs de transactions dans la *blockchain* publique sont associés à un horodatage qui annonce le moment (la date et heure) de la validation des transactions dans le registre. Ces deux horodatages de la *blockchain* sont des horodatages électroniques simples puisque des données sous forme électronique les entrées de transactions ou blocs de transactions sont associés à un instant particulier, établissant la preuve de l'existence de ces blocs de transactions à un instant donné[864]. Il est donc possible de qualifier l'horodatage par la *blockchain* d'horodatage électronique simple. Ce dernier ne pourra être en principe refusé en justice.

B. Les effets probatoires simples accordés à l'horodatage *blockchain*

361. **Le plein effet de l'horodatage *blockchain*.** Le principe de non-discrimination de l'horodatage électronique simple se retrouve au stade des effets de l'horodatage *blockchain*[865]. Les effets juridiques d'un horodatage électronique comme preuve en justice ne peuvent être refusés au seul motif que l'horodatage est sous forme électronique, et qu'il ne remplit pas les

[862] Règl. eIDAS, art. 3, 33.
[863] Règl. eIDAS, art. 41.
[864] Voir *supra* n°135.
[865] Règl. eIDAS, art. 41.

conditions de l'horodatage électronique qualifié. Ainsi, les effets de l'horodatage *blockchain* ne peuvent en principe être refusés au seul motif qu'il est électronique et qu'il n'est pas qualifié.

362. **Les effets simples de l'horodatage *blockchain*.** Dans ce cas de figure, seuls des effets simples sont donc accordés à l'horodatage *blockchain* entrant dans la qualification de l'horodatage simple. Autrement dit, le demandeur à une action aura la charge de démontrer l'exactitude de la date et de l'heure que l'horodatage indique ainsi que l'intégrité des données auxquelles cette date et heure se rapportent. Le cas échéant, cette preuve sera valide et pourra tout de même être reçue emportant les mêmes conséquences juridiques que le modèle qualifié de l'horodatage.

363. **La reconnaissance des effets de l'horodatage *blockchain* par le législateur italien.** Le législateur italien a introduit dans une loi le 11 février 2019 relative au soutien et à la simplification des entreprises et de l'administration publique l'article 8, ter, 3° qui prévoit que « *le stockage d'un document informatique par l'utilisation de technologies basées sur des registres distribués produit les effets juridiques de l'horodatage électronique visé par l'article 41 du règlement (UE) n°910/2014 du Parlement européen et du Conseil du 23 juillet 2014* »[866]. Le législateur se contente d'une reproduction verbatim des effets de l'horodatage électronique simple au sens du règlement eIDAS à celui de l'horodatage *blockchain* par renvoi à ce règlement. Cette première reconnaissance législative en Europe des effets de l'horodatage par la *blockchain* démontre une certaine lacune *intra legem* de cette loi. Elle s'abstient de préciser les modalités de consécration de cet horodatage, de sa recevabilité en justice à ses effets, en faisant appel à des notions floues. Cette lacune du législateur italien est certainement volontaire préservant la pratique des évolutions technologiques à venir.

En tout état de cause, cette solution minimale ne révèle pas les potentialités probatoires en droit de l'horodatage *blockchain* qui aspire à plus d'effet probant[867].

[866] Voir annexe n°2.
[867] Voir les propositions *infra* n°372 et s.

Paragraphe 2 : L'analogie discutée de l'horodatage *blockchain* avec un horodatage électronique qualifié

364. La qualification d'horodatage électronique qualifié au sens du règlement eIDAS pour l'horodatage *blockchain* ne peut être retenue que si les conditions de l'horodatage électronique qualifié sont remplies (A). Au-delà des discussions sur la satisfaction des critères requis, les effets probatoires désirés sont nécessairement à renforcer (B).

A. Les conditions de l'horodatage électronique qualifié à satisfaire par l'horodatage *blockchain*

365. **La liaison de la date et l'heure aux données de manière à raisonnablement exclure la possibilité de modification indétectable des données.** L'horodatage électronique qualifié est un horodatage électronique qui satisfait aux exigences fixées à l'article 42 du règlement eIDAS. Cet article exige, tout d'abord, que l'horodatage lie la date et l'heure aux données de manière à raisonnablement exclure la possibilité de modification indétectable des données[868]. Seul le second horodatage des blocs validés pourrait fournir la garantie d'intégrité totale des données liées à cette date et heure, en excluant toute modification de ces données inscrites chronologiquement dans le registre. Cet horodatage apparaît dans les données transactionnelles d'un bloc de transaction, lui-même lié à une empreinte électronique[869]. Le premier horodatage de date et heure de l'entrée d'une transaction relié à ses données transactionnelles est à exclure car il pourrait ne pas entrer de manière immuable dans le registre de la *blockchain* dans l'hypothèse où un validateur - après les vérifications de l'authentification et de la double dépense - serait amené à rejeter cette transaction[870]. Rien ne garantit que ces date et heure liées aux données transactionnelles soient intègres si celles-ci n'entrent pas de manière effective dans le registre de la *blockchain*.

366. **L'horloge liée au temps universel coordonné.** L'horodatage requiert qu'il soit, ensuite, fondé sur une horloge exacte liée au temps universel coordonné[871]. La plupart des horodatages *blockchains* font usage de l'heure Unix. Ce dispositif de calcul du temps n'est pas

[868] Règl. eIDAS, art. 42, 1, a).
[869] Voir *supra* n°137.
[870] Voir *supra* n°41 en introduction.
[871] Règl. eIDAS, art. 42, 1, b).

basé sur le nombre de secondes depuis l'époque unique du 1er janvier 1970 à 00:00, l'heure de référence internationale UTC (Universal Time Coordinated)/GMT (Greenwich Mean Time). Étant décentralisé, l'horodatage *blockchain* fait appel à l'intervention des nœuds pour son calcul. L'heure et la date des blocs ne sont précises qu'à une ou deux heures près[872]. Cet horodatage *blockchain* n'est donc pas basé sur le temps universel coordonné.

367. **L'horodatage signé au moyen d'une signature électronique avancée ou cacheté au moyen d'un cachet électronique avancé d'un PSCQ, ou par une méthode équivalente.** Enfin, l'horodatage doit être signé au moyen d'une signature électronique avancée ou cacheté au moyen d'un cachet électronique avancé d'un PSCQ, ou par une méthode équivalente[873]. L'aporie de l'identification soulevée par la signature avancée et qualifiée se retrouve bien entendu dans le cadre de l'horodatage qualifié qui requiert une signature électronique avancée[874].

368. L'alternative du cachet électronique, au moyen d'un cachet électronique avancé d'un PSCQ, ne permet pas non plus la satisfaction de ce troisième critère tant qu'il implique l'intervention d'un PSCQ, ce qui n'est pas prévu par la *blockchain* publique. Cette condition pourrait cependant se trouver remplie en envisageant d'organiser l'intervention de ce PSCQ dans le cadre d'une *blockchain* privée ou publique permissionnée, ce qui lèverait les obstacles à la qualification de l'horodatage électronique qualifié[875]. L'alternative du cachet électronique avancé d'un PSCQ est dans le cadre de l'horodatage encore de nature à constituer une contrainte de coût, de temps et de manière générale, une contradiction politique[876]. En tout état de cause, si cette dernière condition n'est pas remplie, les effets prévus par le règlement eIDAS pour l'horodatage qualifié ne peuvent pas bénéficier en théorie à l'horodatage *blockchain* en cause.

369. Une remarque vient toutefois à l'esprit au sujet de la « *méthode équivalente* » mentionnée par le règlement eIDAS. Cette alternative envisagée pour la dernière condition de l'horodatage électronique qualifié pourrait être remplie par le procédé d'horodatage *blockchain* renforcé par la technologie *blockchain* dans son ensemble.

[872] https://en.bitcoin.it/wiki/Block_timestamp (consulté le 31/05/2020).
[873] Règl. eIDAS, art. 42, 1, c).
[874] Voir n°298 et s.
[875] Voir de cet avis : T. Douville, « *blockchains* et preuve », *op.cit.*, p.2194.
[876] F. G'sell, « Preuve et signature numérique », *op.cit.*, p.105.

370. Comme le rappelle le Ministère de la Justice « *(…) rien ne permet d'assurer de la véracité d'un élément inséré dans une blockchain : seule la date de l'insertion (…)* »[877] est garantie par cette technologie. Alors que la date occupe une place d'importance dans l'enregistrement de données par la technologie *blockchain*, les effets probatoires accordés par le droit commun sont hypothétiques et insuffisants au vu des apports de cette preuve. En outre, seule une société a déjà obtenu la certification d'horodatage électronique qualifié basé sur une solution blockchain[878]. Ces constats impliquent un nécessaire renfort des effets probatoires de l'horodatage *blockchain*.

B. Les effets probatoires de l'horodatage *blockchain* à renforcer

371. **La présomption d'exactitude de date et heure et d'intégrité des données.** Lorsque l'horodatage est qualifié au sens du règlement eIDAS, il bénéficie « *d'une présomption d'exactitude de la date et de l'heure qu'il indique et d'intégrité des données auxquelles se rapportent cette date et cette heure* »[879]. Il dispose d'une reconnaissance mutuelle dans tous les autres États membres[880]. En l'état du droit, seul l'horodatage dans une *blockchain* privée ou publique permissionnée ayant fait intervenir un PSCQ et se basant sur l'UTC/GMT pourrait, en principe, bénéficier des effets de cette présomption. Pour les *blockchains* publiques, la charge de cette preuve pèsera sur les acteurs souhaitant apporter la preuve de cet horodatage[881].

372. **Le bénéfice d'une présomption de fiabilité de l'horodatage *blockchain*.** Les *blockchains* publiques peuvent pourtant fournir un haut niveau de confiance dans une information horodatée[882] et ce risque de la preuve de l'horodatage *blockchain* supporté par les usagers des *blockchains* publiques n'est pas satisfaisant[883]. S'il ne convient pas de systématiser le bénéfice de la présomption d'exactitude de la date et de l'heure (dû à l'heure ou deux de décalage)[884], il est nécessaire toutefois de mettre en exergue la fiabilité de la date et de l'heure des blocs de transactions et l'intégrité de ces données garanties par ce procédé. C'est donc une

[877] Question écrite n°22103 de D. Fasquelle, publiée au JO le 30/07/2019, réponse du Ministère de la Justice publiée au JO le 10/12/2019, p.10774. Voir annexe n°10.
[878] La société Guardtime : https://webgate.ec.europa.eu/tl-browser/#/tl/EE/1 (consulté le 31/05/2020).
[879] Règl. eIDAS, art. 41, 2.
[880] Règl. eIDAS, art. 41, 3.
[881] Voir *supra* n°362.
[882] EU blockchain Observatory and Forum, Blockchain and digital identity, *op.cit.*, p.21.
[883] Voir *supra* n°362.
[884] Voir *supra* n°366.

présomption de fiabilité de date et heure des blocs de transactions et d'intégrité de ces données qu'il conviendrait de consacrer. Il s'agirait de mettre au bénéfice de toutes les *blockchains* cette présomption, ce qui reviendrait à présumer l'intégrité de la totalité des données enregistrées dans un bloc de transaction. En tout état de cause, une mesure européenne doit soutenir cette présomption applicable à l'horodatage *blockchain*.

373. Il pourrait s'agir d'opérer une adaptation de la lettre du règlement eIDAS permettant à toutes les *blockchains* de bénéficier de cette présomption[885], et exonérant l'intervention d'un PSCQ. Les rapports France Stratégie et De la Raudière/Mis préconisent une révision du règlement eIDAS[886]. La proposition n°14 du rapport De la Raudière/Mis met en exergue la nécessité d'envisager une adaptation du régime applicable en matière de preuve électronique par une révision du règlement eIDAS. Selon ce rapport, conférer une valeur probante certaine aux informations inscrites au sein des *blockchains* suppose une modification du règlement eIDAS dès lors que la loi nationale transpose les principes fixés par le droit européen. Les rapporteurs ont d'ailleurs soutenu que la reconnaissance de la preuve par la *blockchain* « *constitue une nécessité pour l'essor de la technologie* »[887].

374. Cette préconisation est très généraliste sur les modifications du règlement eIDAS, d'autant plus qu'elle ne semble pas être à l'ordre du jour des réflexions de la Commission européenne axées sur les problématiques d'identification électronique[888]. Elle impliquerait en outre une procédure longue pour adopter ces révisions, selon l'article 294 du traité sur le fonctionnement de l'Union européenne relatif à la procédure législative ordinaire du Parlement et du Conseil européen qui prévoit, de bout en bout, un délai théorique maximal de quatorze mois[889]. Qui plus est, cette intervention très circonstanciée dans le cadre de l'usage d'une technologie pourrait se suffire d'un avis de droit dérivé proposé par la Commission européenne et adopté par le Parlement européen, qui préciserait les frictions actuelles entre le règlement eIDAS et l'horodatage *blockchain* ainsi que la signature *blockchain* et intégrerait la présomption mentionnée. Cet avis serait l'occasion de confirmer que l'horodatage *blockchain* et la signature *blockchain* peuvent prétendre à la qualification d'horodatage électronique simple

[885] Voir dans ce sens pour l'horodatage *blockchain* mais également pour la signature *blockchain* : F. G'sell, « Preuve et signature numérique », *op.cit.*, p.108.
[886] F. G'sell, « Preuve et signature numérique », *op.cit.*, p.109 ; Assemblée nationale, Rapport d'information n°1501, *op.cit.*, p.92.
[887] Assemblée nationale, Rapport d'information n°1501, *op.cit.*, p.92.
[888] European Commission, Evaluation roadmap, Report on the Application of the eIDAS Regulation, Ref. Ares(2019)6019401, 27 sept. 2019.
[889] Traité sur le fonctionnement de l'union européenne, C 326/47 publié au JOUE le 26/10/2012.

et signature électronique simple. Par ailleurs, un avis serait une invitation aux États membres à agir promptement en vue de clarifier le droit européen applicable à l'horodatage. Il est à noter néanmoins que ces avis relèvent de la catégorie des actes non obligatoires à la différence des règlements, des directives et des décisions. Ces avis non contraignants n'imposent pas d'obligations légales aux États membres. En ce sens, l'*EU Blockchain Observatory and Forum* émet une position modérée appelant à une simple clarification de la relation entre la *blockchain* et le règlement eIDAS[890].

375. **Conclusion du chapitre 1.** En conclusion, avec certains ajustements, les données transactionnelles de la *blockchain* peuvent prétendre aux qualifications des catégories de droit commun françaises, européennes ou internationales. La loi type de la CNUDCI sur les documents transférables électroniques de 2018 et le règlement eIDAS apportent un résultat large par la qualification des transactions de documents électroniques.

376. Précisément, en droit français, les transactions simples sont des paiements, c'est-à-dire des faits juridiques prouvables librement. Les transactions complexes ne trouvent de réponse adaptée que dans le commencement de preuve par écrit, le laboratoire d'essai des preuves numériques. Pour ce qui est des procédés de signature et d'horodatage de la *blockchain*, ils répondent en partie aux spécifications du règlement eIDAS, à tout le moins pour les catégories des signatures et horodatages électroniques simples[891]. Elles sont cependant insatisfaisantes pour constituer le reflet de la réelle force probante, notamment de l'horodatage *blockchain*, qui offre des perspectives pour la fiabilité de datation sans précédent. En ce sens une présomption spécifique de fiabilité de la date et de l'heure des blocs de transactions et l'intégrité de ces données doit être soutenue pour ces horodatages *blockchains*. Un avis de droit dérivé adopté par le Parlement européen serait tout à fait à propos pour préciser les points de frottement entre la *blockchain* et le règlement eIDAS et éclaircir les zones d'ombre. En d'autres termes il serait question d'admettre l'assimilation de la signature et l'horodatage *blockchain* à la signature et l'horodatage électronique simple, et de soutenir le renforcement de ce dernier.

[890] EU Blockchain Observatory and Forum, Blockchain and digital identity, *op.cit.*, p.22.
[891] Confirmé par : Assemblée nationale, Rapport d'information n°1501, *op.cit.*, p.92.

CHAPITRE 2

LES QUALIFICATIONS JURIDIQUES DE DROIT COMMUN ENVISAGEES POUR LES PREUVES DE DONNEES COMPLEMENTAIRES ENREGISTREES DANS LA *BLOCKCHAIN*

377. Les données complémentaires intégrées dans la *blockchain* comportent de nombreuses propriétés intrinsèques : d'inaltérabilité par la sécurité algorithmique de la cryptographie employée[892], de distribution et synchronisation de ces données sur tous les nœuds[893], de dilution du risque de perte de ces données ou d'attaque sur celles-ci par l'architecture distribuée du réseau (risque limité d'exposition aux cyber-attaques contrairement au serveur unique), et d'un caractère peu coûteux de l'ancrage de nombreuses données, qui poussent les acteurs publics et privés à se pencher sur cet usage. Ces avantages sont autant de bénéfices dont l'inscriveur peut tirer profit[894]. Compte tenu de ces circonstances, les données complémentaires doivent recevoir une qualification adaptée. L'assimilation de l'empreinte numérique de données ancrée dans la *blockchain* à une preuve parfaite comme une copie doit être retenue et reconnue (section 1), alors que le commencement de preuve par écrit est souhaitable pour les données en clair inscrites dans la *blockchain* (section 2).

[892] Parlement européen, Résolution du 3 oct. 2018 sur les technologies des registres distribués et les chaînes de blocs: renforcer la confiance par la désintermédiation (2017/2772(RSP)), P8_TA(2018)0373 : « *considérant que la TRD peut introduire, grâce aux mécanismes de cryptage et de contrôle nécessaires, un paradigme informatique capable de démocratiser les données et d'améliorer la confiance et la transparence, assurant un itinéraire sûr et efficace pour l'exécution des opérations* ».

[893] K. Wüst, A. Gervais, « Do you need a Blockchain ? », *op.cit.*, p.2 : dans les registres de *blockchain* publique « *l'intégrité de l'information assure la protection de l'information des modifications non autorisées, c'est-à-dire que les données récupérées sont correctes. L'intégrité de l'information est étroitement liée à la vérifiabilité publique. Si un système permet la vérification publique, n'importe qui peut vérifier l'intégrité des données* ». Pour plus de développements sur la notion vérifiabilité publique voir note de bas de page n°61.

[894] Voir sur ces avantages, notamment : G. Canivet, « Présentation de la table ronde "Preuve et blockchain" », Dossier Blockchain et preuve, Dalloz IP/IT n°2, févr. 2019, p.73.

Section 1 : L'assimilation souhaitable de l'empreinte numérique de données ancrée dans la *blockchain* à une preuve parfaite : plaidoyer pour la reconnaissance de l'empreinte numérique de données ancrée dans la *blockchain* comme une copie

378. Présentée comme un mode de preuve parfait par ses promoteurs, l'empreinte de la donnée ou de l'ensemble de données suit un processus particulier d'ancrage dans la *blockchain*. L'ancrage est le fait d'inscrire une donnée ou un ensemble de données dans la *blockchain* par l'intermédiaire de son empreinte. L'empreinte est précisément intégrée dans une transaction. Cette technique de l'ancrage permet de vérifier l'intégrité des données ancrées et d'apporter une date et une heure de cet ancrage, par un ancreur plaideur ou par un tribunal. Si une seule donnée est changée, l'empreinte sera complètement différente. À ces avantages s'ajoute celui de la confidentialité, puisque seule l'empreinte électronique est stockée est non la donnée en clair elle-même, trouvant une application idéale en matière de protection du secret des affaires par exemple. C'est en effet l'empreinte qui est divulguée dans le registre public et particulièrement au destinataire de la transaction puisqu'une fois calculée elle est insérée dans la transaction pour être envoyée à son destinataire. L'empreinte *blockchain* n'est pas « *accessible* » à tous comme il est souvent avancé car le fait de stocker l'empreinte de la donnée dans un registre de *blockchain* public ne permet pas de porter à la connaissance de tous les accédants à la *blockchain* les données sous-jacentes à l'empreinte. Elle a cependant la propriété d'être universelle et non limitée dans le temps, en tant que preuve mathématique en langage unique et déjà connu, elle pourrait être acceptée par tous les ordres juridiques sans durée, ce qui n'est pas actuellement le cas de toutes les empreintes utilisées comme preuves en justice. Par exemple, une enveloppe e-soleau de l'Institut national de la propriété industrielle (INPI) ne bénéficie d'aucune reconnaissance devant les juridictions étrangères et est conservée pendant une période cinq ans dans son système d'archivage (délai qui peut être prorogé pendant une nouvelle période de cinq ans)[895]. La fluidité est un autre de ses caractères saillants, puisqu'il est aisé en pratique de déposer un ensemble de données à ancrer sur une plateforme (intermédiaire à la *blockchain*) afin de les protéger pour se préconstituer des preuves.

[895] INPI, décision n°2016-273 relative aux modalités de dépôt, de prorogation et de restitution d'enveloppes Soleau électronique du 13 dec. 2016, art. 11.

379. De nombreux emplois des empreintes numériques sont déjà visés dans notre droit pour certaines situations : les envois, remises et notifications de l'expertise judiciaire civile[896], la lettre recommandée électronique[897], l'enveloppe e-soleau[898]. Ces empreintes numériques sont limitatives et mentionnées selon leurs finalités en droit de la preuve. Elles ne font pas apparaître de qualification juridique correspondante, ni de précisions sur la valeur juridique de l'empreinte numérique[899]. L'occasion du développement d'une empreinte distribuée utilisée dans le cadre d'une architecture informatique spécifique est alors bienvenue pour soutenir que l'empreinte numérique s'apparente à une preuve parfaite. Il convient pour cela que les conditions de droit commun de l'écrit électronique soient satisfaites, ce qui n'est pas chose aisée (paragraphe 1) mais une copie d'une nature hybride pourrait être retenue au regard de sa force probatoire particulière (paragraphe 2).

Paragraphe 1 : Les conditions de l'écrit électronique difficilement satisfaites par l'empreinte numérique de données ancrée dans la *blockchain*

380. L'empreinte *blockchain* doit tout d'abord répondre au critère d'intelligibilité de la preuve littérale (A). Lorsqu'elle est électronique, cette preuve fait l'objet de conditions particulières d'identification de la personne dont elle émane et d'établissement et de conservation de nature à en garantir l'intégrité[900]. La problématique - quoique certes classique dans la *blockchain* - de l'identification est en suspens pour l'empreinte *blockchain* ce qui nuit à sa qualification d'écrit électronique (B). L'intégrité des données garantie par l'immuabilité des propriétés des empreintes *blockchains* et du registre est néanmoins renforcée (C).

[896] Arrêté du 14 juin 2017 portant application des dispositions du titre XXI du livre Ier du code de procédure civile aux experts judiciaires, publié au JORF n°0142 du 18 juin 2017 texte n°4.
[897] Décret n°2011-144 du 2 février 2011 relatif à l'envoi d'une lettre recommandée par courrier électronique pour la conclusion ou l'exécution d'un contrat**,** publié au JORF n°0029 du 4 février 2011 p.2274 texte n°19.
[898] INPI, décision n°2016-273 relative aux modalités de dépôt, de prorogation et de restitution d'enveloppes Soleau électronique du 13 dec. 2016.
[899] Seul un exemple récent d'une décision de Cour d'appel de Nancy admet la valeur probatoire de l'enveloppe soleau pour la reconnaissance d'un droit d'auteur sur des modèles (date certaine des enregistrements) et déclare le contrefacteur de modèles identiques et similaires coupables d'actes de contrefaçon (CA Nancy, 8 sept. 2014, n°12/03201).
[900] C. civ., art. 1366.

A. L'intelligibilité de l'empreinte *blockchain* interdépendante de ses données calculées

381. **L'absence de signification intelligible de l'empreinte.** L'empreinte numérique ne semble pas, de prime abord, être dotée d'une signification intelligible au sens de l'article 1365 du Code civil, alors même qu'elle constitue une suite de lettres et de chiffres[901]. Selon le Professeur Thibault Douville, l'empreinte n'est pas lisible en soit et ne constitue donc pas au sens du Code civil un écrit[902]. L'empreinte seule ne peut être intelligible en elle-même mais elle prend tout son sens pour le calcul d'un document ou d'un ensemble de données qui, mis ensemble, le seront.

382. **La signification intelligible de l'empreinte avec ses données de calcul initiales.** L'empreinte prend forme et devient intelligible avec les données originaires qui ont servi au calcul, ils sont interdépendants. Il n'est pas possible à partir de l'empreinte *blockchain* de revenir aux données originaires et de reconstituer ces données. Pourtant, dès lors que l'on calcule l'empreinte de ces données une nouvelle fois le résultat est identique à l'empreinte initiale. Il y a là une forme de « *correspondance intelligible* » entre le document et son empreinte. Ce critère de l'écrit intelligible s'applique particulièrement aux données complémentaires ancrées dans la *blockchain*, autrement dit aux données externes que l'on a souhaité ancrer dans la *blockchain* par leur empreinte car elles impliquent des données initiales elles-mêmes intelligibles (ce qui est moins le cas des autres empreintes de la *blockchain*).

B. La problématique de l'identification des sujets de droit « *ancreurs* » en suspens

383. **L'identification variable de l'ancreur.** L'identification de la personne dont émane l'écrit pose des difficultés identiques à celles du commencement de preuve par écrit et de la signature et de l'horodatage électronique, car l'identification de l'ancreur varie en fonction de la typologie de la *blockchain*[903]. De manière générale, en fonction des critères précédemment développés, un anonymat isolé est reconnu à certains participants de *blockchains* précises, un pseudonymat des participants ancreurs au sein des *blockchains* publiques est de mise alors

[901] Voir *supra* les conditions de l'écrit n°256 et les caractéristiques de l'empreinte n°126-127.
[902] T. Douville, « *blockchains* et preuve », *op.cit.*, p.2193.
[903] Voir n°298 et s. ; n°331 et s ; n°367 et s.

qu'une indentification de ces derniers est possible au sein des *blockchains* privées et publiques permissionnées.

384. **Proposition d'identification par palier dans les *blockchains*.** Compte tenu de ce niveau d'identification variable dans les blockchains, constituant un point de frottement avec les exigences légales, il conviendrait de préciser, dans le cadre d'un écrit électronique, les degrés d'identification de la plus faible à la plus forte : anonymat, pseudonymat, et identification. C'est ainsi une identification par palier de degrés d'identification qui permettra de servir d'indicateur pour jauger l'identification de l'ancreur et accéder ou non à la qualification de l'écrit (indicateur utile aussi au commencement de preuve par écrit) :

- Le premier palier constitue un degré faible d'identification. Ce palier dans le domaine des *blockchains* est représenté par les *blockchains* anonymes, c'est-à-dire certaines catégories de *blockchains* (rares en pratique) en leurs représentations des monnaies complètement anonymes (Zcash, Monero etc).
  Dans ce cas, l'ancreur n'est pas identifié et ne pourra bénéficier de la qualification d'écrit électronique.

- Le deuxième palier établit un degré moyen d'identification. Ce palier dans le domaine des *blockchains* est représenté par les *blockchains* pseudonymes, c'est-à-dire les *blockchains* classiques comme Bitcoin et Ethereum.
  Dans ce cas, l'ancreur n'est en principe pas identifié mais pourrait l'être par un ensemble de techniques et de tables de données constituées par les divers prestataires sur actifs numériques. En fonction des cas, l'ancreur pourrait bénéficier de la qualification d'écrit électronique.

- Le troisième palier représente un degré fort d'identification. Ce palier dans le domaine des *blockchains* est représenté par des *blockchains* identifiantes. Il pourrait être atteint par certaines *blockchains* privées et publiques permissionnées.
  Dans ce cas, l'ancreur est identifié et pourra bénéficier de la qualification de l'écrit.

385. **L'absence de garantie de la qualité juridique à ancrer.** Les écueils de l'identification dans les *blockchains* nous amènent à déduire plusieurs observations générales pour l'ancrage d'empreinte de données dans la *blockchain*. L'ancrage ne permet pas de bénéficier de garanties

qu'un individu ancreur d'une empreinte dispose de la bonne qualité juridique pour ancrer[904]. En d'autres termes, c'est la vérification de l'habilitation de l'ancreur à ancrer une empreinte dans la *blockchain* qui fait défaut. Cette vérification de l'habilitation de celui qui ancre est un élément à encadrer précisément dans une convention de preuve entre les membres d'une *blockchain*[905].

386. **La résurgence de la critique du critère d'identification.** La critique du critère de l'identification n'en est pas moins virulente que celle émise pour la signature dans le cadre de l'écrit, mais ceci pour des motifs différents[906]. Avant la loi du 13 mars 2000, le critère d'origine jurisprudentiel exigeait que l'imputabilité du contenu de l'écrit électronique à son auteur ait été vérifiée ou ne soit pas contestée[907]. Cette simple notion d'imputabilité était plus large que celle d'identification intégrée par la loi du 13 mai 2000, laquelle n'a d'ailleurs pas été précisée par décret depuis. Elle était la démonstration d'un lien entre l'écrit et la signature dans le droit, notions distinguées dans nos textes mais très liées en pratique[908]. Depuis cette loi, la jurisprudence a confirmé cette nécessité d'identification par l'usage d'un procédé fiable par l'auteur de l'acte. L'absence d'élément permettant d'identifier l'auteur de l'écrit ne permet pas, selon les juges du fond, de s'assurer de l'existence d'un écrit électronique[909]. Ce nouveau critère validé par la jurisprudence ne semble assurément pas adapté à l'empreinte *blockchain* en tant qu'écrit.

---

[904] Voir à ce sujet en matière de droit d'auteur: CSPLA, Rapport de la mission sur l'état des lieux de la *blockchain* et ses effets potentiels pour la propriété littéraire et artistique, janv. 2018, p.16 ; M. O'Dair et al., Music On The Blockchain, Blockchain For Creative Industries Research Cluster, Middlesex University, report n°1, juill. 2016.
[905] Voir *infra* n°683-694.
[906] Voir *supra* n°333-335.
[907] Cass. com. 2 déc. 1997, D. 1998, jur., p.192, note D. Martin.
[908] E. A . Caprioli, « Traçabilité et droit de la preuve électronique », *op.cit.*
[909] CA Pau, 16 août 2018, n°17/01800, Confirmation : « *l'appelante démontre qu'elle connaissait le mot de passe de cette boîte mail expéditrice, et a très bien pu adresser elle-même ce message, que ce message ne comporte ni signature, ni moyen d'identification de son auteur, qu'il est étonnant que son auteur ait tutoyé l'appelante, alors même que le représentant de la société ne l'a jamais rencontrée* »; CA Paris, 2, 2, 15 nov. 2018, n°16/18608, Confirmation : concernant un SMS qui avait fait l'objet d'un constat d'huissier et qui faisait uniquement apparaître le numéro dont il provenait, les date et heure de l'émission, la Cour d'Appel de Paris indiquait que « *c'est à juste titre que l'intimée fait valoir qu'aucun élément ne permet de s'assurer qu'elle est bien l'auteur des SMS en cause, lesquels ne sont donc pas probants* » ; CA Montpellier, 6 juin 2019, n°18/05460, Confirmation : « *écrit électronique tel que visé par les articles 1366 et 1367 du code civil qui imposent pour leur application notamment l'usage d'un procédé fiable d'identification du signataire de l'écrit, ce qui n'est pas le cas d'un courriel électronique qui ne comporte aucune signature authentifiée* ».

C. L'intégrité renforcée des données garantie par l'immuabilité des empreintes numériques

387. **Mise en contexte de l'intégrité dans le numérique.** La condition d'intégrité a toute son importance depuis toujours dans le domaine numérique, le droit de la preuve doit pouvoir s'appuyer sur des éléments de preuves « *matérialisés* » sous la forme de traces électroniques préconstituées.

388. **Empreinte *blockchain* : la quintessence de la garantie d'intégrité.** L'empreinte intégrée dans la *blockchain* a pour principe de garantir l'intégrité, laquelle peut être vérifiée en calculant une nouvelle fois l'ensemble de données hachées par la même fonction initiale. Corroborée par l'immuabilité du registre, l'intégrité de l'ensemble des données hachées dans une empreinte se voit doublement assurée. La quasi impossible modification des données est confortée par cette double protection technique. Cette garantie est tant confirmée par les scientifiques[910], que par certaines institutions[911]. Le Parlement européen dans sa résolution du 3 octobre 2018 sur les technologies des registres distribués et les chaînes de blocs affirme qu'elles permettent « *d'assurer l'intégrité des données et que la possibilité de fournir une piste d'audit de témoin d'intégrité permet la création de nouveaux modèles d'administration publique et contribue à améliorer la sécurité* »[912]. Ce postulat technique pourrait cependant être ébranlé par la possible - mais rare en pratique sur les réseaux résilients - attaque mentionnée en introduction[913].

[910] A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder, *Bitcoin and Cryptocurrency Technologies*, *op. cit.*, p.15-16 ; R. Pérez Marco, « Blockchain : l'autre révolution venue du bitcoin », *op.cit.* ; Séminaire IRT SystemX, D. Augot, fonction de hachage et blockchain, *op.cit.* ; OPECST, Rapport Comprendre les *blockchains* : fonctionnement et enjeux de ces nouvelles technologies, Auditions de J-P Delahaye du 4 avr. 2018.

[911] Parlement européen, Résolution du 3 octobre 2018 sur les technologies des registres distribués et les chaînes de blocs : renforcer la confiance par la désintermédiation (2017/2772(RSP)), point G ; OPECST, Les enjeux technologiques des *blockchains* (chaînes de blocs), *op.cit.*, p.30-31 ; Assemblée Nationale, Rapport d'information n°1501, *op.cit.*, p.32-33 ; Assemblée Nationale, Rapport d'information, par la commission des finances, de l'économie générale et du contrôle budgétaire en conclusion des travaux d'une mission d'information relative aux monnaies virtuelle, *op.cit.*, p.28.

[912] Parlement européen, Résolution du 3 octobre 2018 sur les technologies des registres distribués et les chaînes de blocs : renforcer la confiance par la désintermédiation (2017/2772(RSP)), point G.

[913] Voir *supra* n°43.

Paragraphe 2 : La qualification vraisemblable de copie hybride de l'empreinte numérique de données ancrée dans la *blockchain*

389. Les preuves écrites sont mentionnées dans le Code civil au Titre IV bis « *de la preuve des obligations* » du livre trois, au Chapitre III « *les différents modes de preuve* », au titre duquel la « *sous-section 5 : les copies* » présente la copie, comme une preuve parfaite dont la force probante aurait été renforcée depuis la réforme du droit des contrats. Cette preuve parfaite se trouve frappée d'hybridité avec l'empreinte numérique dans le sens où - à la lumière des précédentes réflexions -, elle n'aurait pas été qualifiée en amont d'écrit électronique. L'ancrage, pour être qualifié de manière complète, se décompose par l'empreinte, qui est rapprochée d'une copie hybride (B), mais aussi de ses données sous-jacentes qui reçoivent une qualification miroir (A).

A. La qualification miroir des données représentées par l'empreinte

390. **La qualification du fait juridique ou de l'acte juridique projeté à retenir.** L'empreinte calcule un ensemble de données représentant des faits juridique (l'antériorité de la création d'une œuvre de l'esprit, par exemple) ou des actes juridiques (un contrat de vente d'un bien meuble, par exemple). Ces données sont calculées par une fonction de hachage cryptographique pour former une empreinte unique. Elles sont ainsi reflétées cryptographiquement par cette empreinte. Ce « *miroir cryptographique* » traduit cryptographiquement un évènement ou un acte établi par les parties. C'est ainsi une qualification que l'on pourrait nommer de « *miroir* ». Dans le cadre d'un acte juridique, la qualification de l'acte sous-jacent à l'ancrage se doit alors de considérer l'intention initiale des parties. Lorsque des parties projettent de réaliser un acte sous signature privée, voire un acte authentique[914], le simple fait de dupliquer l'acte par une empreinte et de décider de la conserver dans la *blockchain* ne doit pas dénaturer cette projection. Cet acte doit ainsi être assimilé à la qualification prévue par les parties. Cette qualification ne garantit pas toutefois la validité de l'acte ancré. Tout compte fait, il conviendrait de distinguer les fonctions techniques d'élaboration et de conservation des actes[915]. La conservation d'un acte dans la *blockchain* par

[914] Voir les limites précédemment développées n°243-244.
[915] Voir en ce sens : Table ronde, « L'officier public ministériel est-il soluble dans la blockchain ? », *op.cit.*

leur empreinte serait possible et ne doit pas altérer les projections des parties, alors que l'élaboration par la *blockchain* ne serait pas admise en droit français.

391. **La qualification de commencement de preuve par écrit selon le rapport Toledano.** Le rapport Toledano du 28 juin 2018 accorde une force moindre aux données sous-jacentes à l'empreinte. Selon ce dernier, c'est au commencement de preuve par écrit que l'acte sous-jacent à l'empreinte doit être assimilé. La quatrième recommandation sur la preuve préconise de modifier l'article 1362 sur le commencement de preuve par écrit afin d'introduire que « *l'écrit électronique enregistré dans un dispositif d'enregistrement électronique partagé répondant à des caractéristiques prévues par décret en Conseil d'État tient lieu de commencement de preuve par écrit* »[916].

B. La qualification vraisemblable de l'empreinte *blockchain* de copie hybride

392. L'empreinte d'un acte ancrée dans la *blockchain* fait l'objet de la qualification de copie au sens du Code civil mais d'une nature particulière, hybride (1), qui voit de ce fait, ses effets renforcés en matière de preuve (2).

1. La qualification de copie hybride de l'empreinte *blockchain*

393. **L'empreinte cryptographique : une copie singulière.** Il apparaît que, par essence, le support de l'empreinte se moule à la copie par la reproduction cryptographique qu'elle opère. Nos réflexions nous mènent alors à explorer la voie de la qualification de copie. La notion de copie provient du latin « *copia* » qui signifie « *abondance* ». Ce sens originaire se voit parfaitement illustré par la démultiplication des contenus numériques potentiellement copiés à l'infini. Observons toutefois que la langue française doit certainement son sens récent de copie à l'expression latine « *copiam descriendi facere* » qui permet de déduire de la notion de copie le sens de « *reproduction* ».

394. Dans le cadre de l'empreinte *blockchain*, un ensemble de données est en effet haché pour former une empreinte numérique unique propre à elle canalisant ainsi la démultiplication

[916] F. G'sell, « Preuve et signature numérique », *op.cit.*, p.109.

« *sauvage* » des contenus. Cette « *copie cryptographique* » est une copie d'un nouveau genre puisqu'elle ne reproduit pas en des termes identiques l'original, elle est un simple « *reflet cryptographique* » d'un ensemble de données. Alors que reproduire par une copie était synonyme auparavant de perte de qualité[917], elle est aujourd'hui avec l'empreinte cryptographique davantage synonyme d'exactitude technique. Les fonctions générant l'empreinte exercent une garantie technique de cette exactitude grâce à un lien cryptographique presque symbiotique entre l'empreinte ancrée et les données calculées. Pour la Professeure Marie Anne Frison-Roche « (…) *dans l'acte de conservation et de duplication, la blockchain peut être un atout technologique très précieux, en ce qu'à supposer sa fiabilité acquise, l'erreur étant exclue, c'est comme si l'on pouvait produire des originaux indéfiniment* »[918].

395. **Les obligations de conservation de l'original et de la clé privée en pratique.** L'empreinte *blockchain* se rapprocherait ainsi pertinemment de la copie fiable telle que visée par le nouvel article 1379 du Code civil issu de l'ordonnance du 10 février 2016 sur la réforme du droit des contrats[919]. Avant cette ordonnance, les copies n'avaient pas de valeur probatoire autonome, sauf certaines exceptions admises par la jurisprudence[920]. Elle n'avait pas de régime unifié et cohérent puisqu'elle faisait foi uniquement dans l'hypothèse de subsistance de l'original[921]. Désormais, peu importe que l'original subsiste, la copie - indifféremment sur support papier ou électronique - a une valeur indépendante de l'original. N'oublions pas que c'est dans un contexte de favorisation de l'archivage électronique que le législateur a dégagé le principe d'assimilation de la copie sur support papier et sur support électronique dans le but de consacrer des pratiques déjà existantes au sein des entreprises et administrations, consistant à numériser des documents et les archiver de manière fidèle et durable sur un disque dur numérique non réinscriptible (par exemple, la technique WORM (Write Once Read Many) pour les archives publiques)[922]. Cette réforme permet aux parties de faire le choix de ne pas conserver

[917] V. Gautrais, « Preuve des reproductions : vues d'ailleurs ! », Cahiers Droit, Sciences & Technologies, 2014, p.303, n°7.
[918] Table ronde « L'officier public ministériel est-il soluble dans la blockchain ? », *op.cit*.
[919] Voir de cet avis : F. G'sell, « Preuve et signature numérique », *op.cit.*, p.107.
[920] La jurisprudence est allée jusqu'à admettre la valeur des copies « *fidèles et durables* » de la photocopie d'un testament olographe dont l'original avait disparu en raison d'un événement de force majeure. Il avait été égaré fortuitement à la suite du décès de l'expert graphologue auquel il avait été remis (Civ. 1re, 31 mars 2016, n°15-12.773 : AJ fam. 2016. 266, obs. N. Levillain).
[921] N. Dissaux, C. Jamin, *Réforme du droit des contrats, du régime général et de la preuve des obligations. Commentaire des articles 1100 à 1386-1 du Code civil*, *op.cit.*, p.254.
[922] E. A. Caprioli, « Preuve des copies numériques. De la fiabilité des copies numériques », Comm. com. électr. n°2, comm. 19, févr. 2017.

l'original mais uniquement la copie et d'avoir recours sans difficulté à l'archivage électronique[923].

396. En revanche, cette obligation de conservation est centrale dans la reconnaissance de la valeur de l'empreinte *blockchain* conservée dans le registre. L'ancreur ne pourra pas être exonéré de conserver l'original. Sans celle-ci, il n'est plus possible pour l'ancreur de prouver l'intégrité des données ancrées par le jeu du calcul des empreintes, de leur vérification et comparaison. Si seule l'empreinte est gardée, il n'est pas envisageable en effet d'obtenir d'une manière ou d'une autre l'original ancré dans la mesure où l'empreinte est irréversible, ce qui ne permet pas de remonter aux données à partir desquelles elle a été calculée[924]. Il semble donc difficile que le juge soit à même de reconnaître la force probante de l'empreinte sans l'original. Cette obligation de conservation est pour le reste partiellement mentionnée à l'alinéa 3 de l'article 1379 du Code civil indiquant que la présentation de l'original peut toujours être exigée. Cette présentation apparaît à la lecture de cette disposition comme une possibilité mais non comme une nécessité à la réussite de la preuve. Enfin, précisons qu'en cas de perte, oubli ou vol de clé, le lien entre le signataire et la preuve est impossible à apporter et il ne sera plus possible de retrouver son empreinte.

397. **La nécessité de prouver la fiabilité de l'empreinte *blockchain* indépendamment des présomptions légales.** La copie au sens de l'article 1379 du Code civil doit être « *fiable* ». La fiabilité de l'empreinte sera néanmoins laissée à la libre appréciation des juges pour évaluer si la donnée initiale a été ou non modifiée[925]. C'est le juge qui déterminera si une copie est suffisamment convaincante. Des présomptions de fiabilité sont dès lors admises dans deux hypothèses : soit la présomption est irréfragable pour les copies exécutoires ou authentiques d'un acte authentique[926], comme les grosses ou expéditions, soit la présomption est simple pour la fiabilité de la copie qui présente une double propriété de reproduction à l'identique et d'intégrité, selon l'alinéa 2 de l'article 1379 du Code civil.

[923] J-D. Bretzner, A. Aynès, « Droit de la preuve », D.2016, p.2535. Voir aussi le mouvement jurisprudentiel avant la réforme qui reconnaissait à de nombreuses reprises la valeur juridique de copie alors que la partie se prévalant de celle-ci n'était pas disposée à produire l'original : CA Lyon, 6e ch., 3 sept. 2015, n°13/09407 : Com. Com. électr. 2015, comm. 95 E. A. Caprioli ; CA Paris, pôle 4 ch. 9, 11 févr. 2016 n°15/01765 : Comm. Com. électr. 2016, comm. 47 E. A. Caprioli.
[924] Voir *supra* n°127.
[925] C. civ., art. 1379, al. 1.
[926] C. civ., art. 1379, al. 1.

398. Pour cette présomption simple, la reproduction est exigée à l'identique pour la forme et le contenu de l'acte. Cette première condition dans le contexte de l'empreinte *blockchain* fait défaut dans le sens où la forme de l'acte ou de l'ensemble des données n'est pas semblable à celle-ci. Par exemple, si un contrat doit être ancré dans une *blockchain* grâce à son empreinte, le formalisme du contrat ne sera pas repris par l'empreinte. Ce contrat sera représenté par un condensat qui compresse les données entrées en une chaîne de caractères fixes (souvent 64 caractères dans la *blockchain*) de chiffres et de lettres[927]. Le contenu ne sera pas non plus suivi puisqu'aucune information de l'acte ne transparait en clair avec l'empreinte. Avant la réforme du droit des contrats, la copie devait être « *fidèle* » et durable lorsque l'original n'avait pas été conservé[928]. Cette exigence aurait nécessairement butté face à l'empreinte *blockchain*, n'étant pas fidèle à proprement parler. C'est une copie cryptographique. Cette nouvelle condition se rapproche de l'exigence de reproduction à l'identique mais elle n'affecte pas la qualification et la validité de la copie. Elle affecte seulement la charge de la preuve.

399. S'agissant de la seconde condition d'intégrité de la présomption, elle doit être garantie dans le temps par un procédé conforme dont les conditions sont fixées par le décret n°2016-1673 du 5 décembre 2016 relatif à la fiabilité des copies et pris pour l'application de l'article 1379 du Code civil. La reproduction par voie électronique doit justifier d'un procédé qui répond aux conditions prévues aux articles 2 à 6 dudit décret[929]. Ces exigences d'intégrité de la copie reproduite par voie électronique permettant de bénéficier de la présomption de fiabilité sont très strictes, notamment au sujet de la sécurité d'accès au dispositif (qui doit faire « *l'objet de mesures de sécurité appropriées* »[930]), de la qualité du procédé lui-même (qui « (…) *doit être établie par des tests sur des documents similaires à ceux reproduits et vérifiée par des contrôles* »[931]), des modalités de conservation (« *empreintes et les traces générées* (…) *sont conservées aussi longtemps que la copie électronique produite et dans des conditions ne permettant pas leur modification* »[932]), des informations du procédé (« *produire des informations liées à la copie et destinées à l'identification de celle-ci* » qui précisent « *le contexte de la numérisation, en particulier la date de création de la copie* »[933]), et de documentation du procédé de conservation (les procédés doivent être « *décrits dans une*

[927] Voir *supra* n°127.
[928] C. civ., anc. art. 1348, al.2
[929] Décret n°2016-1673 du 5 décembre 2016, art. 1.
[930] Décret n°2016-1673 du 5 décembre 2016, art. 6.
[931] Décret n°2016-1673 du 5 décembre 2016, art. 2, al. 2.
[932] Décret n°2016-1673 du 5 décembre 2016, art. 5.
[933] Décret n°2016-1673 du 5 décembre 2016, art. 2.

documentation conservée aussi longtemps que la copie produite »[934]). La sécurisation de l'accès aux dispositifs de reproduction et de conservation se fait aisément avec la clé privée d'un compte dans la *blockchain* lorsque l'empreinte est inscrite dans la transaction d'une *blockchain* publique. Un ensemble de tests sur la reproduction par voie électronique de documents similaires et les contrôles n'est pas chose trop complexe à mettre en place dans une *blockchain*, à condition de s'accorder sur cette mise en place. La conservation des empreintes dans la durée sera en principe aussi conforme à la durée de production de la copie. En revanche, les informations sur la date de la création de la copie peuvent être difficiles à apporter dans le sens où apparaît seulement la date de la validation des blocs de transactions dans le registre de la *blockchain* publique. Une documentation sur le procédé de conservation - architecture décentralisée de la *blockchain* - de l'empreinte *blockchain* n'existe pas non plus à ce jour, outre l'ensemble des Livres blancs expliquant mathématiquement les protocoles *blockchains* déployés. Cette condition d'intégrité de la copie pourra toujours être présumée remplie « *par l'usage d'un horodatage qualifié, d'un cachet électronique qualifié ou d'une signature électronique qualifiée* » telle que visée par le règlement eIDAS[935], mais les problématiques soulevées antérieurement pour la signature *blockchain* et l'horodatage *blockchain* ne permettent pas d'envisager cette voie (hormis dans le cadre de *blockchains* privées ou publiques permissionnées). Ce décret précise que l'intégrité de la copie résultant du procédé de reproduction par voie électronique est attestée par une empreinte électronique qui « *garantit que toute modification ultérieure de la copie à laquelle elle est attachée est détectable* »[936]. Précisons que l'empreinte *blockchain* qui est visée ici est une copie elle-même, ce n'est pas l'empreinte classique d'une copie matérielle ou immatérielle. De nouvelles empreintes sont aussi utilisées comme garantie de traçabilité des modifications ultérieures de l'empreinte numérique initiale[937]. Ainsi, même si la validité technologique des algorithmes permettant de calculer les empreintes *blockchains* sont dépassées, les mutations successives formalisées par de nouvelles empreintes seront admises par le décret[938].

[934] Décret n°2016-1673 du 5 décembre 2016, art. 7.
[935] Décret n°2016-1673 du 5 décembre 2016, art. 3, al. 2.
[936] Décret n°2016-1673 du 5 décembre 2016, art. 3.
[937] Décret n°2016-1673 du 5 décembre 2016, art. 4, al. 2.
[938] Voir : T. Douville qui indique que « *cet article prend intelligemment en compte les évolutions technologiques à venir, qui nécessiteront de réaliser des opérations pour assurer la lisibilité de la copie* » et que celles-ci « *ne sont pas considérées comme une altération de la copie dans son contenu ou dans sa forme si elles sont tracées et qu'une nouvelle empreinte est générée à chaque fois* » (T. Douville, « Nouveau droit des contrats (fiabilité des copies) : publication du décret d'application », D.2016, p.2517).

400. Pour l'ensemble de ces raisons, il semble peu probable que les empreintes *blockchains* puissent remplir les exigences du décret permettant de bénéficier de la présomption de fiabilité de la copie. Pour autant, cela n'affecte en rien la qualification de copie fiable. Il conviendra de prouver la fiabilité de la copie à l'appui d'arguments présentant les avantages de la *blockchain* de l'espèce. Pour la Professeure Florence G'Sell, le droit positif ne doit donc pas être substantiellement modifié, si ce n'est « *pour intégrer dans le texte du décret, une disposition propre à la blockchain prévoyant expressément que le recours à cette technologie permet, si certaines conditions techniques sont respectées, d'obtenir des copies fiables* »[939].

401. **Une proposition de loi à Monaco qualifiant l'empreinte de copie.** Une proposition de loi n°237 en date du 4 décembre 2017 relative à la *blockchain* dans la principauté de Monaco peut être citée comme piste de réflexion pour notre droit à venir. En son article 6, elle précisait que « *l'inscription d'un acte juridique dans une blockchain est présumée constituer une copie fiable, opposable et durable de l'original* »[940]. Si cette disposition imprécise provoquait le doute sur les contours de l'objet de la présomption en ce que l'inscription présumait la copie et non l'empreinte, elle n'a pas été retenue dans le Projet de loi final n°995 relative à la technologie *blockchain*[941]. Une proposition de loi française ou *lex blockchain* proposera ci-après de reconnaître à l'empreinte *blockchain* la qualification de copie et de délimiter cette reconnaissance[942].

2. Les effets renforcés de la copie hybride de l'empreinte *blockchain*

402. **La force identique de l'empreinte *blockchain* à l'original.** L'effet de l'assimilation de l'empreinte à une copie se situe essentiellement à un niveau : l'empreinte aura une force identique à l'original[943]. Cette équivalence de valeur juridique à l'original ne porte que sur la valeur probatoire et non sur la validité elle-même du document. Ainsi, l'empreinte *blockchain* aura la même valeur probatoire que l'ensemble de données original sous-jacent qui a été haché. Plus encore, il a été considéré que « *la fiabilité (de l'empreinte) est telle que la distinction entre*

[939] F. G'sell, « Preuve et signature numérique », *op.cit.*, p.107.
[940] Voir annexe n°3.
[941] Voir annexe n°4.
[942] Voir *infra* n°497-539 ; n°891.
[943] C. civ., art. 1379, al. 1.

original et copie n'aurait plus lieu d'être »[944] dans la mesure où « *la copie perdrait de sa pertinence en ce que par la fiabilité technologiquement absolue de la duplication, si la copie devient un document aussi fiable que celui dont elle est la copie technologique, alors elle est l'original elle-même* »[945]. Selon cette logique, il pourrait être admis que la notion même de copie appliquée à l'empreinte *blockchain* n'aurait pas lieu d'être puisque cette empreinte renfermerait par elle-même l'original.

403. **Le renforcement des effets de l'empreinte *blockchain* par la réforme du droit des contrats.** Par voie de conséquence, le renforcement des effets de la copie par la réforme du droit des contrats est un renforcement pour la condition probatoire de l'empreinte *blockchain* et son émancipation par rapport à l'acte ou l'ensemble de données originaires, puisque l'original ne conditionnera pas sa valeur probatoire. En principe, l'original n'a même plus besoin d'être présenté lors d'un litige, mais s'il subsiste, sa présentation peut tout de même être exigée par le juge[946].

404. En réalité, dans l'hypothèse d'un litige impliquant des preuves *blockchains*, c'est l'empreinte *blockchain* qui prouvera que des données sont restées intègres. Cette preuve produit ainsi des effets par elle-même, sans avoir besoin en pratique d'apporter l'original, sauf quant à la partie technique du calcul. Les données originales doivent donc être conservées mais il ne semble pas impératif qu'elles soient présentées avec l'empreinte pour prouver l'absence d'altération. L'empreinte *blockchain* aspire à être indépendante dans la phase de conviction des juges. Cette copie n'est donc pas qu'un « *calque cryptographique* » de son original mais dispose d'une autre finalité : son absence de modification dans le temps. Les données qui sont ancrées par leur empreinte, sont elles-mêmes inclues par l'architecture de la *blockchain* dans un ensemble d'autres empreintes[947]. C'est ainsi une garantie permettant de prouver que toute une chaîne de transactions est restée inchangée et, *a fortiori*, que les données qui ont fait l'objet d'une empreinte intégrée dans la transaction le sont aussi. La vertu de garantie d'intégrité de l'empreinte *blockchain* nous permet de la baptiser « *copie cryptographique confirmante d'intégrité* » en ce qu'elle vient corroborer l'absence de modification des données originaires. Par cette garantie, les effets de l'empreinte *blockchain* sont nettement renforcés.

[944] M.-A. Frison-Roche, « Analyse des *blockchains* au regard des usages qu'elles peuvent remplir et des fonctions que les officiers ministériels doivent assurer », *op.cit.*, p.27.
[945] *Ibid.*, p.27.
[946] C. civ., art. 1379, al. 3.
[947] Voir *supra* n°137.

Section 2 : L'assimilation souhaitable au commencement de preuve par écrit des données inscrites en clair dans la *blockchain*

405. Le stockage de données en clair par la *blockchain* permet d'exécuter des opérations sur ces données sans dépendre de stockages externes. Par ce stockage en clair de données complémentaires, l'accédant à la preuve *blockchain* (sujet de droit et tout justiciable dans une *blockchain* publique) et le participant peuvent avoir une connaissance des données inscrites[948]. Ces données en clair sont constituées par des données de toutes natures qui établissent des preuves au titre de commencements de preuve par écrit (paragraphe 1). Le *smart contract*, représentant des données complémentaires inscrites en clair par excellence, dispose de cette même qualification, mais au-delà, constitue un programme informatique (paragraphe 2).

Paragraphe 1 : La qualification de commencement de preuve par écrit à vérifier pour les données de toute nature inscrites en clair

406. Les données complémentaires inscrites en clair comme des données additionnelles d'un ancrage (des métadonnées, par exemple), un lien hypertexte, des mentions obligatoires, ou d'autres données pourront trouver une reconnaissance en droit de la preuve au titre de commencement de preuve par écrit si elles en remplissent les conditions (A). Nonobstant la satisfaction de ces conditions, leurs effets probatoires seront nécessairement réduits (B).

A. Les conditions du commencement de preuve par écrit à remplir par les données inscrites en clair

407. **La satisfaction des conditions.** Les données complémentaires en clair constituent tout d'abord un écrit, en tant qu'écrit numérique, selon l'acception classique du terme[949]. Cet écrit doit ensuite nécessairement provenir du défendeur à l'action mais il se pourrait que des données en clair soient inscrites dans la transaction par un PSAN sur mandat d'agir en nom et pour le compte de celui-ci. Pour cela, l'auteur de l'écrit doit être clairement identifié mais

[948] Cambridge Centre for Alternative Finance, University of Cambridge Judge Business School, Global blockchain benchmarking study, *op.cit.*, 2017, p.54.
[949] Voir plus en détails *supra* n°292 et s. les conditions du commencement de preuve par écrit.

l'identification est nécessairement plus souple pour le commencement de preuve par écrit. Enfin, ces données ajoutées apparaissant en clair pourront de toute évidence rendre vraisemblables l'existence et le contenu de l'élément qui sera à prouver dès l'instant où ce dernier sera directement en lien avec ces données. Le commencement de preuve des données inscrites en clair rendant vraisemblables des faits allégués sera souverainement apprécié par le juge.

408. **L'assimilation subsidiaire au commencement de preuve par écrit.** Ces données pourront donc bénéficier d'une analogie *a minima* de commencement de preuve par écrit, intégrant alors la catégorie des preuves imparfaites. Cette qualification subsidiaire de commencement de preuve par écrit constituant au même titre que la transaction complexe un « *laboratoire d'essai de la preuve moderne* », offre l'opportunité de tester ces techniques d'inscription à des fins de préconstitution de preuve.

B. Les effets probatoires limités du commencement de preuve pour les données inscrites en clair

409. **Le complément des données inscrites en clair par les copies distribuées ou les données exogènes.** Le commencement de preuve des données ajoutées en clair sera subordonné à un autre écrit imparfait. En tant qu'adminicule, il conviendra de le compléter par un autre écrit imparfait (témoignages, indices, aveu extrajudiciaire, argumentaire, second exemplaire de l'écrit etc.). Les copies distribuées sur les nœuds, ou encore des données stockées en dehors de la blockchain, pourront servir de complément de preuve, à condition qu'il y ait une forme d'unicité et un lien suffisant avec le commencement de preuve. Des données inscrites en clair dans une transaction complexe par exemple peuvent aisément insuffler ce lien suffisant par la possibilité technique de faire des renvois à des actes ou des données à l'extérieur de la *blockchain*.

410. **L'effet résiduel en pratique des données inscrites en clair.** L'addition de ces deux preuves imparfaites équivaudrait à une preuve parfaite. Ce commencement de preuve par écrit des données ajoutées en clair permet tout de même de jouer un rôle de substitut de l'écrit mais il n'a, d'une manière générale, qu'un rôle résiduel, ne couvrant pas la totalité des prétentions

en pratique au vu du nombre de données très limité en place[950]. Ainsi les données inscrites en clair devront indubitablement être complétées par d'autres preuves.

Paragraphe 2 : La qualification du *smart contract* par-delà la preuve

411. Les *smart contracts* sont des données en clair de lignes de code lisibles mais non intelligibles. Le *smart contract* se contente alors, comme les autres données inscrites en clair d'une qualification de commencement de preuve par écrit en matière probatoire dû à son impossible qualification d'acte sous signature privée (A). Par-delà ce commencement de preuve, le *smart contract* est un programme informatique (B).

A. L'impossible qualification d'acte sous signature privée

412. **L'absence de satisfaction des conditions de l'acte sous signature privée.** L'interrogation sur la possible qualification de contrat accordée au *smart contract* a été fortement débattue, faisant naitre la célèbre maxime « *le smart contrat n'est, ni un contrat, ni intelligent* »[951]. C'est pourquoi nous devons vérifier que le *smart contract* ne répond pas aux conditions de l'acte sous signature privée et le cas échéant en étayer les raisons.

413. La première condition générale de signature est déjà empêchée par son absence de reconnaissance officielle mentionnée ci-avant. Le *smart contract* n'est pas nécessairement synallagmatique en ce qu'il implique la mise en place d'une condition déclenchant une conséquence pour une partie. Ce constat exonère les participants d'établir - inadéquatement - un double original[952]. Le *smart contract*, s'il est synallagmatique, pourrait avoir pour objet une somme d'argent comme une indemnité issue d'un contrat d'assurance et se trouverait alors confronté à intégrer une mention du débiteur de la somme ou de la quantité en toutes lettres et en chiffres[953], intégrable électroniquement dans le *smart contract*. Concernant la langue, il convient que les parties, participantes à la transaction, soient en mesure de comprendre le sens

[950] Voir *supra* n°100.
[951] M. Mekki, « Les mystères de la blockchain », *op.cit.*, p.263, n°21.
[952] C. civ., art. 1375, al.1.
[953] C. civ., art. 1376.

du *smart contract*[954]. Précisément, elles doivent comprendre le langage de programmation, quand bien même elles seraient les seules à le comprendre. Il semble peu probable que chaque participant - plus ou moins profane soit-il - ait connaissance du langage de programmation spécifique des *smart contracts*[955].

414. **La qualification par défaut de commencement de preuve par écrit.** Ainsi, le rejet de la qualification d'acte sous signature privée pour le *smart contract* s'impose à nous. Il est unanime[956]. Le *smart contract* pourra alors bénéficier de la qualification par défaut de commencement de preuve par écrit si les conditions déjà mentionnées plus avant sont satisfaites.

415. **L'approche différente en droit américain.** L'état du droit américain et la doctrine en *common law* sont plus mitigés[957]. Certains États reconnaissent le *smart contract* comme un vrai contrat autonome. L'État de l'Illinois par le *Public Act* 101-0514 (HB3575) intitulé « *Blockchain Technology Act* » adoptée le 23 août 2019[958] admet que le *smart contract*, défini comme « *un contrat stocké sous forme électronique qui est vérifié par l'utilisation d'une blockchain* »[959], soit reconnu comme produisant des effets juridiques. Selon cette loi, un *smart contract* ne peut effectivement se voir refuser des effets juridiques ou un caractère exécutoire uniquement parce qu'une *blockchain* a été utilisée pour créer, stocker ou vérifier un *smart contract*, un fichier ou une signature[960]. Par ailleurs, la preuve d'un *smart contract* dans une procédure ne doit pas non plus être exclue du seul fait qu'une *blockchain* a été utilisée pour créer, stocker ou vérifier le *smart contract*[961]. Bien que le droit outre atlantique concède au

[954] Cass. 3e civ., 15 déc. 1998, n°97-17.673 : Defrénois 1999, I, 1038, obs. D. Talon.
[955] Voir *supra* n°104.
[956] G. Guerlin, « Considération sur les smart contracts », Dalloz IP/IT n°512, oct. 2017, p.513 ; D. Legeais, Fasc. 534 : Blockchain, JCl. Commercial, Lexis Nexis, 7 mars 2017, n°52 ; M. Mekki, « Les mystères de la blockchain », *op.cit.*, p.2166, n°21 ; A. Barbet-Massin, V. Dahan, « Les enjeux de la blockchain en droit d'auteur », *op. cit.*, p.22, n°8 ; M. Mekki, « Le contrat, objet des smart contrats (partie 1) », Dalloz IP/IT, juill.-août 2018, p.410-411 ; M. Clément-Fontaine, « Le smart contract et le droit des contrats dans l'univers de la mode », Dalloz IP/IT 2018, p.541 ; M. Mekki, « Le smart contract, objet du droit (partie 2) », Dalloz IP/IT, janv. 2019, p.28 ; M. Mekki, « Blockchain : l'exemple des smart contracts. Entre innovation et précaution », 15 mai 2018, p.3, n°5, https://www.mekki.fr/files/sites/37/2018/05/Smart-contracts.pdf ; G. Cattalano, « Smart contracts et droit des contrats », AJ contrat n°7, Dossier « blockchain, smart contract et droit », juill. 2019, p.321.
[957] M. Raskin, « The Law and Legality of Smart contracts », Georgetown Law Technology Review 304, 2017, p.309-310.
[958] Public Act 101-0514 (HB 3575 - LRB101 11071 RJF 56276 b). Voir annexe n°8.
[959] BTA, Section 5.
[960] BTA, Section 10, a).
[961] BTA, Section 10, c).

smart contract une reconnaissance juridique et des effets, notre droit latin et les réflexions doctrinales se sustentent d'une qualification a-probatoire.

B. La qualification de programme informatique indépendamment de la preuve

416. **Un programme informatique auto-exécutant.** La qualification du *smart contract* transcende ses enjeux probatoires. La doctrine majoritaire s'accorde unanimement en droit romano-germanique pour caractériser le *smart contract* de programme informatique « *auto-exécutant* », mis en œuvre par des lignes de code permettant de retranscrire un contrat déjà existant[962]. Le *smart contract* est alors une modalité d'exécution technique de ce contrat préexistant[963]. L'expression *smart contract* fait référence au concept de protocole informatique de contractualisation et non de contrat pur au sens juridique[964]. Ce *smart contract* vient se « *superposer au contrat* », traduisant à cet égard le langage humain en langage de programmation[965]. Ce programme informatique classique n'est ni plus, ni moins, qu'un logiciel comportant un certain nombre de lignes de code souvent publiées en open source, protégeables par ailleurs, au titre du droit d'auteur en tant qu'œuvre de l'esprit[966].

417. **Conclusion du chapitre 2.** En conclusion du chapitre 2, les données complémentaires, qu'elles soient hachées ou apparaissant comme du contenu visible, se voient reconnaître - bien que difficilement à certains égards - par les mécanismes de droit commun de la preuve, les qualifications de copie et de commencement de preuve par écrit. Si la qualification de copie est

---

[962] Cette position est partagée par la doctrine dominante française : C. Zolynski, « Blockchain et smart contract*s* : premiers regards sur une technologie disruptive », RD Banc. Fin., Dossier 4, janv. 2017, n°13-14 ; G. Guerlin, « Considération sur les smart contracts », *op.cit.*, p.512 ; M. Mekki, « Les mystères de la blockchain », *op.cit.*, p.2166, n°21 ; D. Legeais, Fasc. 534 : Blockchain, *op.cit.*, n°52 ; A. Barbet-Massin et V. Dahan, « Les enjeux de la blockchain en droit d'auteur », *op.cit.*, p.22, n°8 ; M. Mekki, « Blockchain : l'exemple des smart contract*s*. Entre innovation et précaution », *op.cit.*, p.3, n°5-6, https://www.mekki.fr/files/sites/37/2018/05/smart-contracts.pdf ; M. Mekki, « Le contrat, objet des smart contrats (partie 1) », *op.cit.*, p.410-411 ; M. Clément-fontaine, « le smart contract et le droit des contrats dans l'univers de la mode », Dalloz IP/IT 2018, p.541 ; M. Mekki, « Le smart contract, objet du droit (partie 2) », *op.cit.*, p.28 ; G. Cattalano, « smart contracts et droit des contrats », *op.cit.*, p.321.

[963] M. Mekki, « Les mystères de la blockchain », *op.cit.*, p.2166, n°21.

[964] N. Szabo, « Smart contract*s* : building blocks for digital markets », 1996, 10 p.

[965] P. de Filippi, B. Jean, « Les Smart contract*s*, les nouveaux contrats augmentés ? », Revue de l'ACE n°137, septembre 2016, p.2.

[966] Un logiciel est une œuvre de l'esprit protégée par la loi sur le droit d'auteur dès lors qu'il est original : Cass., ass. plén., 7 mars 1986, n°84-93.509, Sté Atari Ireland LTD et a. c/ Valadon et a. eisd. loc. Pour la protection des lignes de code, voir une admission implicite de la protection du code source et objet en se référant aux instructions dans les décisions : Cass., ass. plén., 7 mars 1986, Pachot, n°83-10477, SA Babolat Maillot Witt c/ Pachot ; T. com. Bobigny, 20 janv. 1995 : RIDA oct. 1995, p.324

considérée comme hybride et dérogatoire pour l'empreinte cryptographique qui ne peut être qualifiée au préalable d'écrit avec certitude, force est d'admettre qu'elle doit bénéficier d'une place privilégiée avec des effets nettement renforcés grâce aux garanties apportées par l'infrastructure technique de la *blockchain*. Toutefois, les données complémentaires en clair ne sont, ni plus, ni moins en matière probatoire, que des adminicules à compléter par d'autres éléments de preuve (même en ce qui concerne le *smart contract*).

418. **Conclusion du titre 1.** En conclusion, ce titre a cherché à reconnaître les preuves *blockchains* - nouvelles preuves numériques - en droit par leurs qualifications au regard du droit commun existant.

419. Ces preuves de données enregistrées dans la *blockchain*, bien que complexes, ont trouvé à « *s'emboiter* » aux catégories probatoires adaptées prévues par le Code civil et le règlement eIDAS. Le Code civil arrive à saisir avec plasticité certaines données transactionnelles et les données complémentaires. Les transactions simples relatives aux transactions s'apparentent à des faits juridiques. Le commencement de preuve par écrit est adéquat pour les transactions complexes et les données complémentaires en clair. L'empreinte *blockchain* est quant à elle qualifiée de copie. Dans le même temps, le règlement eIDAS saisit aussi d'autres données transactionnelles : les données signées et datées. Les procédés de la *blockchain* de signature et d'horodatage sont assimilés à des signatures et horodatages électroniques simples.

420. Par translitération de ces qualifications juridiques, le droit commun trouve à s'appliquer mais cette assimilation par « *capillarité* »[967], ne donne pas d'effets pleinement satisfaisants aux preuves *blockchains* à certains égards, notamment pour la signature, l'horodatage et l'empreinte *blockchain*.

Pour la signature et l'horodatage *blockchain*, un avis de droit dérivé adopté par le Parlement européen est proposé pour éclaircir l'application du règlement eIDAS et soutenir une présomption de fiabilité pour l'horodatage *blockchain*.

Pour l'empreinte *blockchain*, même si elle ne remplit pas les conditions de l'écrit, une qualification de copie hybride devra être retenue et délimitée grâce à sa fiabilité technique.

[967] V. Magnier, « Enjeux de la blockchain en matière de propriété intellectuelle et articulation avec les principes généraux de la preuve », *op.cit.*, p.78.

421. Des régimes ont d'ores et déjà été élaborés en droit spécial et un essai de régime général pourrait fournir une solution congruente pour accorder plus de force probante à ces preuves *blockchains*. À l'aune de ces raisons, nous nous appesantirons dans un titre 2 sur les régimes juridiques des preuves de données enregistrées dans la *blockchain*.

TITRE 2

LES REGIMES JURIDIQUES DES PREUVES DE DONNEES ENREGISTREES DANS LA *BLOCKCHAIN*

422. Les régimes juridiques de preuves des données enregistrées dans la *blockchain* sont scindés en deux : les régimes spéciaux de l'inscription de jetons déjà consacrés en droit français et un régime général de base commun à tous. L'actuel « *droit des preuves de données enregistrées dans la blockchain* » souffre « *d'atrophie probatoire* » par l'incomplétude des régimes spéciaux des instruments financiers inscrits dans la *blockchain*, analysés dans un premier chapitre (chapitre 1). Pour pallier ce handicap, nous tâcherons de mettre en lumière des propositions pour un « *régime axiomatique* » des preuves *blockchains* dans un second chapitre (chapitre 2). Comme l'énonçait toutefois Montesquieu « *les lois inutiles affaiblissent les lois nécessaires* »[968], il s'agira alors dans ce second chapitre d'établir si un régime général dans une « *loi nécessaire* » et plus généralement une politique favorable sont utiles à l'éclaircissement de ce régime. Afin d'éviter l'écueil du développement des preuves *blockchains* comme une tour de pise aux fondements instables, nous ne manquerons pas de préciser si nécessaire des règles de droit commun pertinentes et suggérer des bases internationales.

[968] Montesquieu, *De l'esprit des lois*, t. 2, Livre XXIX, chap. XVI, 1963, p.266.

CHAPITRE 1

L'INCOMPLETUDE DES REGIMES SPECIAUX NATIONAUX DES PREUVES D'INSCRIPTION DES INSTRUMENTS FINANCIERS DANS LA *BLOCKCHAIN*

423. Depuis l'essor des premiers protocoles *blockchains*, la France s'est emparée de cette technologie et de ses opportunités en matière de preuve pour consacrer trois cas d'usage matérialisés par des régimes spéciaux proposant des preuves d'inscriptions de « *token* ». Cette opération nommée « *tokenisation* » consiste en la possibilité d'inscrire un jeton représentant un actif et ses droits dans une *blockchain*[969]. Les catégories de tokenisation visées par la loi sont l'inscription de jetons utilitaires ou « *utility token* » et l'inscription de jetons financiers ou « *security token* ». La première, régie par la loi PACTE, n'offre que très peu de précision sur le régime de la preuve des inscriptions de ces jetons utilitaires hormis celle d'une mise en place d'un système de multi-signatures[970]. Si tant est qu'elle puisse constituer un aveu des limites de ce régime spécial, la seconde concernant l'inscription de l'émission et cession de minibons (section 1) et de titres financiers non cotés (section 2) dans un DEEP touchant plus largement le secteur de la finance décentralisée ou *Decentralised Finance* (DeFi) offre un apport crucial en matière de preuves *blockchains*. Ces inscriptions en DEEP - visant pour partie une forme de *blockchain* pour le législateur[971] - doivent faire l'objet de réflexions et d'analyses probatoires au regard de ces deux cas d'usage.

[969] D. Legeais, Fasc. 535 : Actifs numériques et prestataires sur actifs numériques, JCl. Commercial, Lexis Nexis, oct. 2019, n°6.
[970] AMF, Instruction DOC-2019-06, procédure d'instruction et établissement d'un document d'information devant être déposé auprès de l'AMF en vue de l'obtention d'un visa sur une offre au public de jetons, applicable au 6 juin 2019, p.4
[971] Rapport au Président de la République relatif à l'ordonnance n°2016-520 du 28 avril 2016 relative aux bons de caisse, NOR: FCPT1608300P, JORF n°0101 du 29 avril 2016 texte n°15 : « *L'ordonnance prévoit également que l'émission de minibons peut être inscrite dans un dispositif d'enregistrement électronique partagé (Blockchain), dans des conditions à préciser par décret en Conseil d'État* ».

Section 1 : Les preuves des inscriptions d'émission et cession de minibons dans un « *dispositif d'enregistrement électronique partagé* »

424. L'ordonnance n°2016-520 du 28 avril 2016 relative aux bons de caisse dite « *minibons* » prise sur le fondement de l'article 168 de la loi n°2015-990 pour la croissance, l'activité et l'égalité des chances économiques dite « *Macron* »[972], a introduit dans le Code monétaire et financier par son article L223-12 la possibilité d'émettre et de céder des bons de caisse spécifiques au secteur du financement participatif dans une *blockchain*, au côté de registres tenus individuellement par l'émetteur[973]. Ces bons de caisse spécifiques sont des titres nominatifs et non négociables comportant l'engagement par une entreprise appelée « *émetteur* » de payer à échéances déterminées un investisseur[974]. Le décret publié le 28 octobre 2016 est venu préciser l'application de cette ordonnance[975]. En outre, le décret publié le 24 décembre 2018 - après une procédure d'examen par la Commission européenne[976] - a posé les modalités techniques de mise en œuvre du DEEP (applicable aussi aux titres financiers non cotés)[977]. Cette ordonnance novatrice en matière probatoire admet l'assimilation de l'inscription de la cession de minibons dans un DEEP à un contrat écrit (paragraphe 1) et induit des effets nouveaux (paragraphe 2).

[972] Loi n°2015-990 du 6 août 2015 pour la croissance, l'activité et l'égalité des chances économiques (1), NOR: EINX1426821L, JORF n°0181 du 7 août 2015 page 13537, texte n°1.
[973] Ordonnance n°2016-520 du 28 avril 2016 relative aux bons de caisse, JORF n°0101 du 29 avril 2016, texte n°16 : R. Vabres, note Dr. sociétés 2016, n°7, repère 7 ; X. Delpech, note D. mai 2016 ; A. Reygrobellet, note RTDF 2016, chron. p.109 ; D. Legeais, note RTD Com. 2016, p.830 ; S. le Normand-Caillère, étude Dr. sociétés 2017, étude 12, n°18, p.8-9.
[974] H. Hovasse, S. Le Normand-Caillère, Fasc. 1950 : Bons de caisse, JCl. Banque, crédit, bourse, Lexis Nexis, sept. 2017 (mis à jour en janv. 2019), p.2, n°2.
[975] Décret n°2016-1453 du 28 octobre 2016 relatif aux titres et aux prêts proposés dans le cadre du financement participatif, publié JORF n°0254 du 30 octobre 2016 texte n°8 : J.-J. Daigre, note Banque et Droit 170, 2016, p.40-41.
[976] Commission européenne, Direction générale de la croissance, notification n°2018/367/F.
[977] Décret n°2018-1226 du 24 décembre 2018 relatif à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers et pour l'émission et la cession de minibons, publié au jorf n°0298 du 26 décembre 2018 texte n°33 : C. Pion, S. Blemus, note RDBF n°1, étude n°2, janv. 2019, p.25-29, X. Lavayssière, note RLDI n°144, janv. 2019, p.4-6 ; B. Mathis, note RLDI n°156, févr. 2019, p.21-22 ; B. Donderot, note BJS mai 2019, n°119u0, p.42.

Paragraphe 1 : L'assimilation de l'inscription de la cession de minibons dans un « *dispositif d'enregistrement électronique partagé* » à un contrat écrit

425. L'assimilation de l'inscription de la cession de minibons dans un DEEP à un contrat écrit peut être interprétée de deux façons : selon une lecture de la lettre de l'ordonnance minibons (A) ou selon une traduction de l'esprit de cette ordonnance (B). Ces interprétations impactent les apports probatoires de façon plus ou moins importante.

A. Des apports probatoires significatifs par la lettre de l'ordonnance minibons

426. La lecture de la lettre de l'ordonnance laisse apparaître l'objectif de l'inscription de l'émission et de la cession de minibons et la valeur probatoire de l'inscription dans un DEEP de la cession, permettant respectivement d'authentifier les opérations (1) et de les assimiler à un contrat écrit (2).

1. L'objectif de l'inscription de l'émission et de la cession de minibons dans un « *dispositif d'enregistrement électronique partagé* » : l'authentification des opérations

427. **L'authentification des émissions et cessions de minibons.** Conformément à la lettre de l'article L223-12 du Code monétaire et financier « *l'émission et la cession de minibons peuvent également être inscrites dans un dispositif d'enregistrement électronique partagé permettant l'authentification de ces opérations, dans des conditions, notamment de sécurité, définies par décret en Conseil d'État* ». L'inscription en DEEP de ces titres a pour conséquence d'authentifier des opérations d'émission et de cession dans un but opérationnel et très concret. L'« *authentification* » dans sa première acception reviendrait à vérifier l'exactitude de cette émission et cession de minibons[978]. Cette authentification qui passe traditionnellement par l'inscription en compte-titres, peut dorénavant être effectuée dans la *blockchain*. Pour cela, le décret d'application conditionne, d'une part, le fonctionnement technique de la *blockchain* afin que son registre garantisse l'intégrité des inscriptions, l'identification des propriétaires des

[978] Voir *supra* n°265.

titres, la nature et le nombre de titres détenus[979]. D'autre part, cette authentification est renforcée par un plan de continuité d'activité mis à jour de toutes les inscriptions réalisées dans le DEEP[980]. Ce plan de continuité apparaît comme un filet de sécurité dans l'usage d'un DEEP pour les émetteurs et les propriétaires de titres successifs en ce qu'il doit notamment mettre en place un dispositif externe de conservation périodique des données[981].

428. **La première reconnaissance significative de preuves *blockchains*.** Cette disposition, intégrée en dur dans le Code monétaire et financier, marque symboliquement un échelon dans la reconnaissance des preuves *blockchains* puisqu'elle confirme qu'une *blockchain* a les capacités techniques d'authentifier des opérations et le reconnait en droit. Cette solution pourrait opportunément être élargie à d'autres secteurs, ce qui n'a d'ailleurs pas été le cas, d'un point de vue textuel, dans l'ordonnance *blockchain* relative aux inscriptions en DEEP de titres financiers non cotés qui ne reprend pas strictement la notion d'authentification.

2. La valeur probatoire de l'inscription de la cession de minibons dans un « *dispositif d'enregistrement électronique partagé* » : un contrat écrit

429. **Le principe.** L'inscription d'une cession de minibons dans un DEEP est assimilée à un contrat écrit[982], telle est la lettre de l'ordonnance minibons en vertu du premier alinéa de l'article 223-13. Elle précise en ces termes que « *le transfert de propriété de minibons résulte de l'inscription de la cession dans le dispositif d'enregistrement électronique mentionné à l'article L223-12, qui tient lieu de contrat écrit …*».

430. **Les effets.** L'assimilation de l'inscription de la cession à un contrat écrit fait tomber *ipso facto* cette inscription dans le mode de preuve de droit commun de l'acte sous signature privé visé par les articles 1372 et suivants du Code civil. Elle aura ainsi pour effet de mettre à la charge des parties des obligations, c'est-à-dire de mettre à la charge de l'inscriveur, investisseur originaire dans les minibons, une obligation de céder sa créance et à la charge du

[979] Décret du 24 décembre 2018, art. R211-9-7, al. 1. Voir *infra* n°454 et s.
[980] Décret du 24 décembre 2018, art. R211-9-7, al. 2. Voir *infra* n°459.
[981] Décret du 24 décembre 2018, art. R211-9-7, al. 2.
[982] J. Deroulez, « *Blockchain* et preuve », Dalloz avocats - Exercer et entreprendre n°2, févr. 2017, p.59 : la disposition L. 223-12 du Code monétaire et financier *« semble poser un principe d'équivalence (dans ce cas) entre inscription dans une blockchain et existence d'un acte sous signature privée, alors même que dans une blockchain ne figure qu'une empreinte cryptographique des cessions visées* ».

cessionnaire une obligation d'effectuer un paiement. Ce dernier disposera - après l'inscription dans la *blockchain* - envers l'émetteur du minibon, débiteur cédé d'une créance, d'un engagement de le payer à échéances déterminées. Cette opération de cession devra être notifiée à l'émetteur, débiteur cédé, ainsi qu'au prestataire de services d'investissement ou au conseiller en investissements participatifs[983]. L'acte sous signature privée est requis pour se préconstituer une preuve et dans cette hypothèse d'existence d'un acte juridique, l'écrit doit être apporté lors d'un litige[984]. L'inscription de la cession de minibons équivalant à un contrat, il sera possible pour le plaideur d'apporter simplement le registre des transactions de la *blockchain* démontrant l'inscription de la cession de minibons concernée[985].

431. **La portée.** Les apports de cette première ordonnance reconnaissant la valeur de seing privé à une inscription dans la *blockchain* dans un cas particulier sont éminemment majeurs pour la reconnaissance probatoire de cette technologie et constituent une avancée considérable. Il se peut toutefois que le législateur n'en ait certainement pas souhaité autant.

B. Des apports probatoires tempérés par l'esprit de l'ordonnance minibons

432. **La conformité à la cession de créance civile.** En filigrane du texte de l'ordonnance minibons, il n'est pas certain que le législateur ait voulu généraliser l'assimilation de l'inscription dans une *blockchain* à un contrat écrit mais que celle-ci soit établie en raison de la nature de l'opération. En effet, l'esprit du texte de l'ordonnance minibons est de permettre la cession de minibons par un nouveau support. Celle-ci s'apparente à une cession de créance civile entre un créancier cédant investisseur dans des minibons et un créancier cessionnaire. La méthode exégétique ou téléologique - procédant selon l'interprétation de la finalité du texte - voudrait que cette inscription ait été assimilée à un contrat écrit pour se conformer au régime de la cession de créance civile. L'intention poursuivie par le législateur n'était donc pas initialement de donner la valeur juridique de contrat sous seing privé, à l'inscription dans la *blockchain* mais de se conformer à l'application des articles 1321 et 1322 du Code civil relatifs à la cession de créance civile. En attestent d'ailleurs les renvois à ces dispositions dans l'article L223-12 du Code monétaire et financier.

[983] C. mon. fin., art. L223-13, al. 2.
[984] C. civ., art. 1359.
[985] Voir *supra* n°205.

433. **Le contexte de la réforme du droit des contrats.** S'ajoute à cette interprétation extensive, le contexte de la réforme du droit des contrats central dans la rédaction de l'article L223-12 du Code monétaire et financier. L'ordonnance du 10 février 2016 abandonna le traitement de la créance civile à travers le prisme d'un contrat de vente pour la considérer comme « *un contrat par lequel le créancier cédant transmet, à titre onéreux ou gratuit, tout ou partie de sa créance contre le débiteur cédé à un tiers appelé le cessionnaire* » selon l'article 1321, explicitant, *en sus*, dans l'article 1322 que « *la cession de créance doit être constatée par écrit, à peine de nullité* ». Le risque d'éluder la précision de l'assimilation de l'inscription dans la *blockchain* à un contrat était alors de s'exposer indubitablement à des recours en nullité en chaîne de ces cessions de créance relatives aux minibons.

Paragraphe 2 : Les effets de l'inscription de la cession de minibons dans un « *dispositif d'enregistrement électronique partagé* »

434. La lecture stricte de l'article L223-13 du Code monétaire et financier induit dans l'assimilation de l'inscription de la cession des minibons dans la *blockchain*, des effets de droit commun, tant en matière de transfert de propriété des valeurs mobilières (A), que dans la naissance d'obligations entre l'inscriveur créancier cédant, le débiteur cédé et le tiers cessionnaire (B).

A. Le transfert de propriété des minibons

435. **Le principe : le transfert de la propriété des minibons.** Au-delà de transférer un droit de créance, l'inscription de la cession de minibons aura pour effet de transférer la titularité des minibons. Cet effet translatif du contrat en droit commun est consacré depuis l'ordonnance du 10 février 2016[986], abandonnant l'obligation de « *donner* » associée au transfert de propriété, soutenue par une partie de la doctrine[987]. Pour le contrat de cession de minibons, ces effets sont

[986] Code civil, section 1 : les effets du contrat entre les parties, sous-section 2 : effet translatif. Voir : S. Gaudemet, « l'effet translatif », JCP N 2015, n°47.

[987] Pour : P. Bloch, « L'obligation de transférer la propriété dans la vente », RTD civ. 1988, p.673 ; J. Huet, « Des différentes sortes d'obligations et plus particulièrement de l'obligation de donner, la mal nommée, la mal-aimée », *in* Études J. Ghestin, LGDJ 2001, p.425 ; Contre : M. Fabre-Magnan, « Le mythe de l'obligation de donner », RTD civ. 1996, p.85 ; D. Tallon, « Le surprenant réveil de l'obligation de donner – à propos des arrêts de la chambre

spécifiquement prévus par le premier alinéa de l'article L.223-13 du Code monétaire et financier selon les termes suivants « *le transfert de propriété de minibons résulte de l'inscription de la cession dans le dispositif d'enregistrement électronique mentionné à l'article L223-12 (…)* ». Ainsi, la propriété du minibon sera transférée de l'inscriveur créancier cédant au tiers cessionnaire.

436. **La condition de fond du transfert de propriété des minibons : l'inscription.** La formalité de l'inscription apparaît comme une condition de ce transfert. Partant, l'inscription est une condition de fond du transfert de propriété des minibons. Ce transfert reste consensuel même si sa preuve impose l'accomplissement de la modalité spécifique de l'inscription des minibons en compte du tiers cessionnaire[988].

B. Les obligations issues de la cession de créance des minibons

437. **La transmission d'un droit de créance.** L'assimilation de l'inscription de la cession des minibons dans la *blockchain* à un contrat écrit a un certain nombre d'effets prévus par le droit commun des contrats. Le contrat généré par l'inscription dans la *blockchain* ne créé d'obligations qu'à la charge des parties à la cession, selon le principe de l'effet relatif du contrat[989]. La cession de créance opère une transmission d'un droit de créance qui a des effets juridiques actifs puisqu'il porte sur un droit subjectif.

438. **La date du transfert de la créance.** Le premier alinéa de l'article 1323 du Code civil prévoit par ailleurs qu' « *entre les parties, le transfert de la créance s'opère à la date de l'acte* », c'est alors à la date de l'inscription de la cession que la créance sera transférée de manière effective. Ceci signifie que la créance quitte le patrimoine du cédant titulaire des minibons au moment de l'inscription de la cession. Ladite créance intègre parallèlement le patrimoine du cessionnaire au même moment de l'inscription.

commerciale de la Cour de cassation en matière de détermination du prix », D. 1992, chron. p.68 ; N. Prybis-Gavalda, *L'obligation de donner*, thèse ss. dir. M. Cabrillac, Montpellier, 1997, 714 p.

[988] R. Bonhomme (Maj par M. Bouteille-Brigant), Fasc. 90 : transfert de la propriété et des risques, JCl. Contrats – Distribution, Lexis Nexis, mars 2017.

[989] C. civ., art. 1199, al. 1.

439. **La notification.** Tant que la cession de minibons n'a pas été notifiée au débiteur, celui-ci demeure libre de refuser de se libérer entre les mains du tiers cessionnaire. Le premier alinéa de l'article 1324 du Code civil dispose, en effet, que « *la cession n'est opposable au débiteur, s'il n'y a déjà consenti, que si elle lui a été notifiée ou s'il en a pris acte* ». En pratique, il nous est permis de douter de l'effet translatif de la créance au moment de l'inscription car encore faudrait-il que l'émetteur de minibons, débiteur cédé ait été notifié au préalable ou ait donné son consentement. Dès cette notification, le tiers cessionnaire pourra réclamer le paiement de la créance qu'il détient auprès du débiteur cédé.

440. **L'opposabilité aux tiers.** Ces obligations ne seront pas cependant imputables aux tiers[990]. Ceux-ci ne pourront ni être débiteurs d'une obligation issue du contrat de cession de créance de minibons, ni créanciers de l'inscriveur ou de son co-contractant. La cession de créance sera cependant opposable aux tiers, qui devront respecter la situation juridique créée[991]. La cession est en ce sens opposable aux tiers à compter de la date de l'acte, conformément au deuxième alinéa de l'article 1323 du Code civil.

441. C'est au moment de l'inscription de la cession de minibons que cette opération sera opposable aux tiers. Ces tiers pourront d'ailleurs s'en prévaloir[992]. La possibilité d'accéder à cette preuve de cession de minibons inscrite dans le registre de la *blockchain* sera ouverte pour un tiers, essentiellement pour ce qui est de l'existence, plutôt que du contenu de cette preuve, puisqu'il n'est pas certain que ce contrat constitué dans la *blockchain* puisse comporter un ensemble de stipulations contractuelles en clair. En définitive, cet outil probatoire sera utile pour le tiers et conforme au principe d'opposabilité du contrat au tiers.

Section 2 : Les preuves des inscriptions des titres financiers non cotés dans un « *dispositif d'enregistrement électronique partagé* »

442. L'ordonnance n°2017-1674 du 8 décembre 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission des titres financiers dite « *blockchain* » introduit, sur habilitation de l'article 120 de la loi n°2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la

[990] C. civ., art. 1199, al.2.
[991] C. civ., art. 1200, al.1.
[992] C. civ., art. 1200, al.2.

modernisation de la vie économique dite « *Sapin II* »[993], un deuxième cas spécifique de l'usage de la *blockchain* pour les titres financiers non cotés[994]. Objet d'un processus de rédaction original, l'ordonnance *blockchain* a fait suite à une première consultation publique par la Direction générale du Trésor entre mars et mai 2017, qui a permis de recueillir les observations de l'ensemble des acteurs intéressés dans ce domaine. Une deuxième consultation, entre septembre et octobre 2017, a suivi pour offrir l'opportunité au public de se prononcer sur le projet d'ordonnance publié le 19 septembre 2017. L'ordonnance, adoptée le 8 décembre 2017 dans sa version définitive, a été publiée au Journal officiel le 9 décembre 2017. Cette ordonnance est entrée en vigueur au moment de la publication du décret du 24 décembre 2018. Ce décret d'application, le même que celui traitant des minibons, est venu préciser les modalités d'application de cette ordonnance et rendre opérationnel ce dispositif. Nous traiterons des principaux apports de cette ordonnance sous le prisme des preuves *blockchains* en deux temps. Dans un premier, nous examinerons l'assimilation de l'inscription des titres financiers non cotés dans un DEEP (paragraphe 1) et dans un second, les effets probatoires de cette l'assimilation (paragraphe 2).

Paragraphe 1 : L'assimilation de l'inscription des titres financiers non cotés dans un « *dispositif d'enregistrement électronique partagé* » à des inscriptions en compte-titres

443. L'assimilation de l'inscription des titres financiers non cotés dans un DEEP à celle en compte-titres implique le rapprochement du support du DEEP à celui du compte-titres (A) ainsi qu'une équivalence des garanties des inscriptions dans un DEEP et celles en compte-titres (B).

A. Le rapprochement du support du « *dispositif d'enregistrement électronique partagé* » à celui des inscriptions en compte-titres

444. **La critique sémantique du « *dispositif d'enregistrement électronique partagé* ».** Le premier alinéa de l'article L211-3 du Code monétaire et financier prévoit que les titres

[993] Loi n°2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique (1), NOR: ECFM1605542L, JORF n°0287 du 10 décembre 2016 texte n°2.
[994] Ordonnance n°2017-1674 du 8 décembre 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers, NOR: ECOT1729053R : R. Vabres, note Dr. sociétés n°1, janv. 2018, repère 1, p.1-2 ; S. Schiller, note JCP G n°3, janv. 2018, p.65-68 ; D. Legeais, note JCP E n°4, janv. 2018, act. 58, p.9-11.

financiers sont inscrits soit dans un compte-titres, soit dans un DEEP, pour ainsi dire une *blockchain*. Cette assimilation n'est pas d'une clarté limpide d'un point de vue sémantique, remarque qui sera, par la même occasion, applicable à l'usage du DEEP pour les minibons. Le terme employé de dispositif d'enregistrement électronique « *partagé* » ne fait pas nécessairement référence au caractère « *distribué* » et « *décentralisé* » d'un dispositif basé sur un protocole *blockchain*. Il serait possible de créer un dispositif d'enregistrement électronique, faisant intervenir un intermédiaire ou un organe de contrôle, qui serait ensuite partagé (centralisé et non distribué et décentralisé). Le système informatique interne utilisant une *blockchain* intégralement fermée et non partagée serait quant à lui exclu de ces nouvelles dispositions du DEEP[995]. Cette volonté de désigner la *blockchain* de manière large et neutre aurait eu pour objectif de ne pas exclure des développements technologiques ultérieurs[996], mais il va en réalité jusqu'à exclure partiellement l'usage de la technologie *blockchain* en permettant l'emploi d'un autre support technologique. Nous aurions préféré la notion plus explicite de registre numérique de transmission, d'enregistrement, et de stockage distribué ou plus succinct de registre distribué.

445. **La critique de l'absence de définition du « *dispositif d'enregistrement électronique partagé* ».** Ce terme de DEEP, qui n'a jamais été défini, instaure une ambiguïté gênante, s'apparentant à une lacune *intra legem*, autrement dit une lacune volontaire du législateur qui se serait abstenu de préciser cette notion « *flottante* » laissée dans le floue.

446. Le rapport au Ministre de l'Économie et des Finances sur les crypto-monnaies publié en juillet 2018 dit « *Landau* » confirme effectivement que le registre partagé inclut un registre distribué (*blockchain* ou non) et une base de données traditionnelle[997]. Il ne serait pas non plus impossible qu'un DEEP, non encadré par le Code monétaire et financier pour les titres limitativement visés[998], soit utilisé à d'autres fins puisqu'aucune disposition ne l'interdit

[995] Par exemple, un teneur en compte-titres ou un dépositaire central qui utiliserait la *blockchain* fermée en local comme système informatique. Voir : T. Cremers, « Qualifications juridiques de valeurs numériques et titres inscrits en DEEP », BJB n°6, n°118s0, nov. 2019, p.57.
[996] Rapport au Président de la République relatif à l'ordonnance n°2017-1674 du 8 décembre 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers publié au Journal Officiel n°0287 du 9 décembre 2017, Texte n°23.
[997] Ministre de l'Économie et des Finances, Les crypto-monnaies, Rapport au Ministre de l'Économie et des Finances Jean-Pierre Landau avec la collaboration d'Alban Genais, juill. 2018, p.6.
[998] Voir *infra* n°448.

strictement[999]. Il conviendrait dans ce contexte de donner une véritable définition propre et fonctionnelle à la possibilité d'inscrire divers types de données dans la *blockchain*[1000].

447. Notons qu'une loi du Grand-Duché de Luxembourg du 1er mars 2019 portant modification de la loi modifiée du 1er août 2001 concernant la circulation de titres luxembourgeois introduit un article 18 bis inspiré de notre DEEP français, qui consacre le « *dispositif d'enregistrement électroniques sécurisés* » pour la tenue de compte-titres et les inscriptions au côté du compte-titres traditionnel. Cette disposition tout aussi équivoque quant à la terminologie du support technologique employé apporte toutefois une précision sur le dispositif, qui inclurait les « *registres ou bases de données électroniques distribués* »[1001].

448. **Le champ des titres pour l'inscription en DEEP.** L'article L211-7 du Code monétaire et financier vise un champ restrictif (mais plus large que l'ordonnance minibons) de titres non admis aux opérations d'un dépositaire central qu'il est possible d'inscrire dans un DEEP. Le rapport au Président de la République relatif à l'ordonnance *blockchain* reprend les catégories visées précisément par les titres non admis aux opérations d'un dépositaire central, à savoir les titres de créance négociables, les parts ou actions d'organismes de placement collectif, les titres de capital émis par les sociétés par actions et les titres de créance autres que les titres de créance négociables, à condition qu'ils ne soient pas négociés sur une plateforme de négociation[1002].

449. **L'assimilation de l'inscription en DEEP à l'inscription en compte-titres.** L'inscription de ces titres dans le DEEP est assimilée à une inscription en compte-titres, en vertu du deuxième alinéa de l'article L211-3 du Code monétaire et financier qui précise que « *l'inscription dans un dispositif d'enregistrement électronique partagé tient lieu d'inscription en compte* ». Il convient cependant que cette inscription soit réalisée sur décision de l'émetteur[1003]. Cette alternative a essentiellement pour but d'accélérer la dématérialisation des titres par la tenue du registre des mouvements de titres non cotés non pas sur compte-titres mais dans un DEEP à l'heure où encore de nombreux titres sont inscrits dans des registres papiers.

---

[999] En ce sens : T. Cremers, « Qualifications juridiques de valeurs numériques et titres inscrits en DEEP », *op.cit.*, p.57.
[1000] Voir *infra* n°499 et s.
[1001] Luxembourg, Projet de loi portant modification de la loi modifiée du 1er aout 2001 concernant la circulation de titres.
[1002] Rapport au Président de la République relatif à l'ordonnance n°2017-1674 du 8 décembre 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers, NOR: ECOT1729053P, publié au JORF n°0287 le 9 décembre 2017, texte n°23.
[1003] C. mon. fin., art. L211-7.

450. **L'absence de mention précise du caractère authentifiant des opérations.** Contrairement à l'ordonnance minibons, il n'est pas fait mention du caractère authentifiant des opérations d'inscription de ces titres par la technologie *blockchain*. Il est simplement indiqué que l'inscription en DEEP doit présenter des garanties en matière d'authentification « *(...) au moins équivalentes à celles présentées par une inscription en compte-titres* »[1004]. En revenant sur les travaux du projet de loi Sapin II, la commission des finances du Sénat avait pourtant considéré la technologie *blockchain* comme une « *technologie informatique d'authentification décentralisée des opérations, sans l'intervention d'un tiers de confiance central et un grand registre de transactions public et accessible sur Internet, qui utilise un protocole de pair à pair (peer to peer) pour valider toute opération réalisée entre deux personnes* »[1005].

451. **La tenue du DEEP par un mandataire.** Comme pour la tenue de compte-titres classique qui autorise le recours à un madandataire pour tout ou partie de ses tâches[1006], il incombe à l'émetteur pour la tenue d'un DEEP, de désigner un mandataire selon l'article R211-3 du Code monétaire et financier. Il doit publier à ce titre dans le Bulletin des annonces légales obligatoires la dénomination et l'adresse de son mandataire, ainsi que la catégorie de titres financiers qui fait l'objet du mandat. Ces mandataires sont classiquement des établissements de crédit ou des cabinets d'avocats. Cela dit, avec le DEEP, il pourrait tout à fait être envisagé que ce mandataire soit le prestataire qui fournit le DEEP, ou le gestionnaire dudit DEEP[1007].

452. **Les fonctions du mandataire.** Le DEEP génère aussi des doutes sur le rôle de ce mandataire qui devra certainement se borner à « *l'inscription* » du titre. Cependant, l'emploi des termes « *administrer les inscriptions* » laisse à penser que le mandataire pourrait avoir accès au DEEP (habilitation et droit d'accès à organiser pour une *blockchain* privé ou accès libre pour une *blockchain* publique). Or, dans un compte-titres classique, si le mandataire peut « *tenir* » un compte-titres ouvert chez un émetteur, il n'y accède pas opérationnellement et ne mouvemente pas à distance le registre des investisseurs. Il ne fait que reproduire la présentation

[1004] C. mon. fin., art. L211-3, al. 2.
[1005] Sénat, avis de la commission des finances sur le projet de loi relatif à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique (loi Sapin II), 3 nov. 2016.
[1006] C. mon. fin., art. L211-8.
[1007] DG du Trésor, Consultation publique sur le projet d'ordonnance *blockchain*/titres financiers, 19 sept.-6 oct. 2017.

des titres dans le compte-titres de l'investisseur par une double saisie[1008]. Cela ouvre ainsi un champ plus large pour ces mandataires teneurs de DEEP.

B. L'équivalence des garanties des inscriptions dans un « *dispositif d'enregistrement électronique partagé* » et des inscriptions en compte-titres

453. La mise en place du DEEP implique des modalités techniques permettant des fonctionnalités similaires à l'inscription en compte. Le dispositif d'authentification dans l'inscription en DEEP des titres et leurs mouvements présente alors des garanties équivalentes (1) mais le DEEP, empreint de particularismes propres, prévoit un faisceau de preuves supplémentaires spécifiques (2).

1. Le dispositif d'authentification dans l'inscription des titres et leurs mouvements dans un « *dispositif d'enregistrement électronique partagé* »

454. **Une obligation de moyen.** Le DEEP doit présenter « *des garanties, notamment en matière d'authentification, au moins équivalentes à celles présentées par une inscription en compte-titres* »[1009]. Ces garanties sont fixées par le décret du 24 décembre 2018. Comme dans l'usage des minibons, le DEEP doit être « *conçu et mis en œuvre de façon à garantir l'enregistrement et l'intégrité des inscriptions et à permettre, directement ou indirectement, d'identifier les propriétaires des titres, la nature et le nombre de titres détenus* » en vertu de l'article R211-9-7 du Code monétaire et financier. Par l'emploi des termes « *de façon à* », il semblerait que cette garantie soit considérée comme une simple obligation de moyen[1010], se concentrant sur les objectifs à atteindre[1011].

455. **L'interrogation sur l'identification de l'acquéreur.** Sur l'identification des acquéreurs, tout d'abord, la formulation du décret ne précise pas les modalités techniques de l'identification. Elle conduit à une forme de redondance superficielle avec la disposition L211-4 du Code monétaire et financier qui exige que « *le compte-titres est ouvert ou l'inscription*

[1008] B. Mathis, « Blockchain : un décret pour rien », RLDI, févr. 2019, n°156.
[1009] C. mon. fin., art. L211-3, al. 3.
[1010] S. Schiller, T. Cremers, « Effectivité de ma représentation et de la transmission des titres financiers non cotés par une blockchain ainsi que des minibons », *op.cit.*, p.187.
[1011] B. Dondero, « La *blockchain* et le droit des sociétés », BJS mai 2019, n°119u0, p.42.

dans un dispositif d'enregistrement électronique partagé est réalisée, au nom d'un ou de plusieurs titulaires, propriétaires des titres financiers qui y sont inscrits »[1012]. La possibilité équivoque d'identifier « *indirectement* » les propriétaires des titres pourrait signifier que la *blockchain* publique, pseudonyme qui n'identifie pas directement ses participants, trouverait à s'appliquer pour cet usage[1013]. Ceci semble toutefois quelque peu illusoire dans le secteur financier traditionnel.

456. **L'interrogation sur les modalités de gestion des droits d'accès.** Ce décret n'apporte pas davantage de précisions sur les modalités de gestion des droits d'accès. En pratique, la gestion des clés privées pourrait être effectuée par un opérateur en DEEP, mais le statut de cet acteur n'est pas envisagé avec précision pour l'heure, laissant tout acteur assumer ce rôle. Dans ce vide juridique, le rôle des opérateurs/conservateurs de clés n'est pas évident mais se voit nécessairement exclu du régime prévu par la loi PACTE applicable aux prestataires réalisant des services de conservation pour le compte de tiers d'actifs numériques ou d'accès à des actifs numériques, exclusif aux activités sur jetons utilitaires et crypto-monnaies. Ce flou n'est pas de nature à constituer une garantie suffisante pour les droits des investisseurs[1014].

457. **Le support technologique agnostique.** Saluons tout de même la sagesse de ce décret qui n'enferme pas l'usage du DEEP dans un protocole de *blockchain* précis, laissant une grande place à l'expérimentation des *blockchains* sans permission, dès l'instant où elles fournissent une sécurité suffisante de façon à « *garantir l'enregistrement et l'intégrité des inscriptions* ». Ce choix de l'un ou l'autre des réseaux (permission ou sans permission) est, pour le reste, une question d'une grande importance nécessitant de reconsidérer totalement les modalités de l'inscription, la gouvernance, la performance, la confidentialité des données.

2. Le faisceau de preuves complémentaires spécifiques au « *dispositif d'enregistrement électronique partagé* »

458. **Le faisceau de preuves complémentaires.** L'équivalence des supports probatoires entre les DEEP et le compte-titres implique un particularisme à ce canal technologique d'un

[1012] C. mon. fin., art. L211-4.
[1013] C. Pion, S. Blemus, « Blockchain, minibons et titres financiers », RDBF n°1, étude n°2, janv. 2019, p.28, n°17.
[1014] En comparaison avec les cahiers des charges du teneur de compte-conservateur (Règl. gén. AMF, art. 322-1 et s.). Voir opinion de : T. Cremers, « Qualifications juridiques de valeurs numériques et titres inscrits en DEEP », BJB n°6, n°118s0, nov. 2019, p.57.

nouveau genre. Le deuxième alinéa de l'article R211-9-7 du Code monétaire et financier indique que « *les inscriptions réalisées dans ce dispositif d'enregistrement font l'objet d'un plan de continuité d'activité actualisé comprenant notamment un dispositif externe de conservation périodique des données* ».

459. **Le plan de continuité d'activité.** Un dispositif de stockage en dehors de la *blockchain* en local ou dans le cloud pour mettre en œuvre le plan de continuité d'activité (PCA) pourrait assurer cette conservation périodique. Ce PCA renforcerait la bonne gestion et serait un gage d'assurance d'une intégrité dans le temps si le DEEP fait l'objet d'un dysfonctionnement quelconque[1015]. Ce PCA peut sembler redondant avec l'existence du registre distribué mais n'oublions pas que dans la mise en œuvre des protocoles de *blockchain*, il n'est pas exclu qu'il y ait des dysfonctionnements à l'occasion des modifications faites des différentes versions du protocole[1016].

460. **Le relevé des opérations individualisé.** Le propriétaire pourrait aussi disposer d'un relevé des opérations individualisé, selon l'alinéa 3 de l'article R211-9-7 Code monétaire et financier, mais cette possibilité semble redondante avec les caractéristiques essentielles même du DEEP qui est un registre établissant par définition l'ensemble des opérations. Reste à savoir si la faisabilité technique ne sera pas trop ardue et ne constituerait pas un obstacle à cette possibilité. Charge à un prestataire fournissant ce type de technologie de registres distribués, de pouvoir techniquement extraire l'ensemble de ces opérations et de permettre ainsi au propriétaire des titres de disposer de son relevé des opérations individualisé. La formulation de cet article ne semble toutefois pas imposer une obligation d'extraction de ces relevés mais en indiquer une simple faculté avec l'emploi du verbe « *pouvoir* » comme ceci « *lorsque des titres sont inscrits dans ce dispositif d'enregistrement, le propriétaire de ces titres peut disposer de relevés des opérations qui lui sont propres* ».

[1015] C. Pion, S. Blemus, « Blockchain, minibons et titres financiers », *op.cit.*, p.27, n°15.
[1016] Voir par exemple le bug du 18 septembre 2018 sur le réseau bitcoin : https://bitcoincore.org/en/2018/09/20/notice/ (consulté le 31/05/2020).

Paragraphe 2 : Les effets probatoires de l'assimilation de l'inscription des titres financiers non cotés dans un « *dispositif d'enregistrement électronique partagé* » à des inscriptions en compte-titres

461. Les effets probatoires sont effectifs dès l'inscription dans un DEEP, qui apparaît comme l'élément générateur de ces effets (A). Par assimilation à l'inscription en compte-titres, la nature du droit à prouver dans le cadre de l'inscription en DEEP est celle d'un droit réel : le droit de propriété du titre financier non coté (B).

A. L'élément générateur des effets probatoires : l'inscription dans un « *dispositif d'enregistrement électronique partagé* »

462. **Le fait générateur : l'inscription dans le DEEP**. L'élément déclencheur des effets probatoires dans le cadre du DEEP et du compte-titres résulte, selon l'article L.228-1, alinéa 9 du Code de commerce, « (…) *de l'inscription des valeurs mobilières au compte de l'acheteur ou dans un dispositif d'enregistrement électronique partagé* (…) ».

463. **Les effets probatoires.** À compter de l'inscription, désignée comme fait générateur des effets en matière de preuve, la propriété de la valeur mobilière, est transférée. Autrement dit, en cas de cession de valeur mobilière, cette opération juridique de transmission d'un droit de propriété de l'émetteur au souscripteur est réalisée par l'inscription. Ainsi dès l'inscription en DEEP, le transfert de propriété du titre financier non coté est réalisé, à l'instar du minibon pour lequel l'évènement de l'inscription conditionne également le transfert[1017]. L'enjeu d'inscrire un jeton financier dans la *blockchain* publique est de taille sur les effets probatoires puisque la lenteur du réseau pourrait impliquer une différence avec le moment de l'inscription effective dudit jeton.

[1017] Voir *supra* n°435-436.

B. La nature du droit à prouver sur les titres financiers non cotés

464. **La preuve d'un droit réel sur les titres financiers non cotés.** Le célèbre développeur du protocole Bitcoin Andreas Antonopoulos dans son ouvrage de 2014 indiquait que la transaction dans la *blockchain* comprend « *une preuve de propriété* » pour chaque bitcoin entré dans le registre, dont le transfert sous la forme d'une signature numérique de son propriétaire peut être validé de façon indépendante par quiconque[1018]. Cet auteur visionnaire sur la preuve de propriété entendue au sens informatique, exprimait déjà ce que le droit français décida de développer plus tard pour l'inscription des titres financiers non cotés (et des minibons). Dans ce contexte, le transfert de propriété d'un titre est en principe prouvé par l'inscription en DEEP mais il pourra être facilité par la présomption de propriété du titre au profit du titulaire du compte dans le DEEP.

465. L'inscription en DEEP a pour effet de transférer la propriété au bénéfice de l'acquéreur des titres, en vertu de l'alinéa 9 de l'article L228-1 du Code de commerce, indiquant que « *(…) le transfert de propriété résulte de l'inscription des valeurs mobilières au compte de l'acheteur ou dans un dispositif d'enregistrement électronique partagé (…)* ». Cet article ne précise pas toutefois comment prouver ce droit de propriété sur les titres financiers non cotés. C'est au cœur du droit existant que l'on trouve des réponses aux zones grises en matière de preuve *blockchain*.

466. **Une présomption de propriété du titre financier non coté transposée au profit du titulaire du compte en DEEP.** Compte tenu de l'assimilation du support du DEEP à celui du compte-titres, selon le deuxième alinéa de l'article L211-3 du Code monétaire et financier, nous devrions logiquement pouvoir assimiler les effets probatoires de l'inscription en compte-titres à celui de l'inscription en DEEP. Les titres financiers non cotés bénéficieraient grâce à cette assimilation, d'un traitement juridictionnel favorable de la preuve permettant de présumer de leur titularité.

467. En fonction de la nature du conflit, selon qu'il oppose ou non le titulaire du compte ou un tiers, la présomption de titularité d'un titre pourra être irréfragable ou réfragable. Si le conflit l'oppose à un tiers, les titres inscrits bénéficieront d'une présomption irréfragable de propriété, conformément à l'article L211-16 du Code monétaire et financier, tandis que si le conflit

[1018] A. M. Antonopoulos, *Mastering Bitcoin : Unlocking Digital Cryptocurrencies*, *op.cit.*, p.25

l'oppose à son ayant cause, ces titres bénéficieront d'une présomption simple de propriété, en vertu de l'alinéa 9 de l'article L228-1 du Code de commerce susmentionné et de l'article L211-17 du Code monétaire et financier. Aussi, l'introduction de la présomption irréfragable impliquant la possession en matière de titres financiers est la conclusion de longs débats doctrinaux soutenus[1019]. Il est désormais considéré que ces articles font application du principe de droit commun selon lequel « *en fait de meubles, la possession vaut titre* » visé par l'article 2276 du Code civil. Dès lors, deux fonctions distinctes attribuées à la possession mobilière doivent être distinguées : la fonction probatoire reposant sur la présomption simple de propriété et la fonction acquisitive de propriété, qui repose sur une présomption irréfragable[1020].

468. C'est ainsi une présomption irréfragable ou simple de propriété des titres dont bénéficie le titulaire en compte-titres classique qu'il convient de transposer au DEEP dans le cadre des titres financiers non cotés. Lorsqu'elle sera réfragable, opposant le titulaire du compte-titres en DEEP et son ayant cause, elle supportera la preuve contraire, mais à charge pour celui qui entend revendiquer la propriété des titres inscrits dans un DEEP d'en apporter la preuve contraire. De plus, dès lors qu'il s'agira d'une possession de titre non coté à prouver, la preuve de cette possession sera uniquement prouvée simplement. Enfin, dans une *blockchain* privée, il serait aisé d'apporter la preuve de l'inscription des titres financiers non cotés dans un compte puisque l'adresse publique est souvent reliée à une identité, alors que dans la *blockchain* publique, la clé publique peut certainement difficilement faire foi lors d'un litige, sauf à alimenter cette preuve par d'autres éléments particulièrement probants.

469. **Conclusion du chapitre 1.** En définitive, bien que l'apport de l'ordonnance minibons soit symboliquement cardinal en droit de la preuve par son assimilation de l'inscription de la cession des minibons à un contrat écrit (qui renvoie au droit commun des écrits sous signature privée), ces régimes spéciaux soulèvent encore moult interrogations. Ce sont tantôt des questions suscitées sur le fond : de terminologie et de définition, tantôt des questions matérielles comme les modalités d'authentification des opérations, l'identification de l'acquéreur, les

[1019] C. Merkin, B. de Saint Mars, « Transfert de propriété sur le marché des valeurs mobilières », RD bancaire et bourse, janv. 94, p.1-2 ; H. le Nabasque, A. Reygrobellet, « L'inscription en compte des valeurs mobilières », RDB 2000, p.261, n°70 ; F. G. Trébulle, *L'émission de valeurs mobilières*, Economica, 2002, n°752 ; D. Robine, « La réforme du transfert de propriété des valeurs mobilières in l'ordonnance n°2004-604 du 24 juin 2004 portant réforme du régime des valeurs mobilières », LPA, 22 sept.2005, p.49, n°12 et n°18 ; A. Couret, H. Le Nabasque, *Droit financier*, Dalloz, 1ère éd., 2008, p.681, n°1132.

[1020] A. Constantin, « Bourses de valeurs - Affaire Madoff : les belles questions de droit posées par la propriété des titres Luxalpha », etude doctr. n°434, JCP G n°15, 11 avr. 2011, p.709, n°7.

modalités de gestion des droits d'accès. Ce cadre incomplet de la preuve par le DEEP et circonscrit à des domaines particuliers : les minibons et celui plus large mais tout de même restrictif des titres non-admis aux opérations d'un dépositaire central de titre, ne sont pas de nature à organiser et garantir l'efficacité pleine et parfaite de l'ensemble des données enregistrées dans la *blockchain*. C'est au législateur qu'il revient d'endosser ce rôle légistique et aux politiques publiques de parachever le cadre des preuves *blockchains*[1021]. Il convient alors de s'intéresser à la politique, aux principes, et aux textes législatifs et réglementaires qui pourraient être formulés (chapitre 2).

[1021] Voir en ce sens : Sénat, avis n°710 (2015-2016) sur le Projet de loi relatif à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, de M. Albéric de Montgolfier, fait au nom de la commission des finances, déposé le 22 juin 2016, p.272 : « *Pour ces trois raisons, le champ de la présente habilitation n'est qu'une première étape dans la construction d'un « droit de la blockchain », que votre rapporteur appelle de ses vœux* ».

CHAPITRE 2

ESSAI D'UN REGIME GENERAL TRANSNATIONAL DES PREUVES D'ENREGISTREMENTS DE DONNEES DANS LA *BLOCKCHAIN*

470. Ce chapitre a pour objectif d'établir une proposition de reconnaissance générale des preuves *blockchains*, tout en permettant une certaine plasticité pour une adaptation malléable à la pluralité de typologies de *blockchains* et usages possibles. Alors que d'aucuns appellent à une « *exception blockchain* »[1022] ou une « *excuse blockchain* »[1023], il s'agira pour notre part dans ce chapitre de reconnaître la force de ces preuves pour les soutenir. L'objectif ne sera pas d'établir un cadre coercitif astreignant centré sur les produits/services, ou les acteurs à l'instar de la loi PACTE qui axe son apport sur les obligations incombant aux émetteurs d'ICO et aux PSAN, mais de s'inspirer davantage du timbre des ordonnances minibons et *blockchain* teintées d'innovation. Pour cela, nous nous appuierons sur la précédente mise en perspective des faiblesses des qualifications retenues ainsi que des régimes spéciaux trop sectoriels pour proposer des principes de bonne facture et une politique à l'échelle mondiale des preuves de données enregistrées dans la *blockchain* (section 1). Nous soumettrons ensuite la réception adéquate de cette ossature internationale par un régime français dualiste de *hard law* et *soft law* (section 2).

Section 1 : Une proposition d'ossature internationale principielle et politique des preuves de données enregistrées dans la *blockchain*

471. Le caractère international par nature des preuves générées par les *blockchains* implique qu'elles ne s'arrêtent pas aux frontières des pays. Ces preuves sont intrinsèquement sans frontière ce qui implique deux préoccupations au niveau international : d'une part, d'établir des principes généraux applicables par tous les États (paragraphe 1), et, d'autre part, de les asseoir

[1022] T. Schrepel, « Is Blockchain the Death of Antitrust Law ? The Blockchain Antitrust Paradox », Georgetown Law Technology Review / 3 Geo. L. Tech. Rev. 281, juin 2018, p.285.
[1023] *Ibid.*, p.328.

par une politique commune composée d'un certain nombre d'actions dans le cadre d'un programme mondial (paragraphe 2).

Paragraphe 1 : De la réflexion sur l'établissement de principes sur les preuves de données enregistrées dans la *blockchain* en droit international

472. Pour créer les grands principes des preuves *blockchains* en vue d'un socle international général qui dépasse les simples intérêts de chaque État et des acteurs privés nationaux, la méthodologie constitue le point névralgique dans la rédaction de ces principes (A). Il s'agira ensuite d'étudier en détail les principes proposés (B).

A. L'importance de la méthode dans la rédaction de principes internationaux sur les preuves de données enregistrées dans la *blockchain*

473. **Méthodologie dans la production des normes.** L'essentiel de l'enjeu réside dans le choix du texte, support de ces principes et l'organisation ou l'institution qui sera à même d'impulser et de soutenir ce projet de principes. Le concept ancien de « *légalisation variable* » présente une méthodologie dans la production de norme[1024]. Ce concept met en exergue une multiplicité de modes de coopération internationale selon des degrés d'institutionnalisation : le degré de force juridique permettrait d'élaborer une norme de façon plus ou moins contraignante, le degré d'engagement offrirait l'élaboration d'une norme plus ou moins précise, le degré de délégation d'autorité proposerait la mise en place de sanctions en cas de non-respect de la norme.

474. **Le support approprié de production des normes.** Les règles de conflit de lois s'appliquent déjà en droit international du cyberespace, à défaut d'autres textes, pour déterminer quelles règles nationales trouvent à s'appliquer à une situation comportant un élément d'extranéité[1025]. Adopter des règles matérielles de droit international privé, des règles substantielles sous forme de principes internationaux s'appliquant dès qu'une situation

[1024] K. W. Abbott, R. O. Keaohane, A. Moravcsik, A.-M. Slaughter, D. Snidal, « The Concept of legalization », International Organization, vol. 54, n°3, Summer 2000, p.401-419.
[1025] Voir *supra* n°162 et s.

internationale entre dans le champ d'application d'un traité est une première option[1026]. L'intérêt de ces règles est qu'elles donnent directement la solution du litige sans avoir à passer par une règle de conflit de lois.

475. La seconde option pourrait trouver sa source dans une convention ou un accord international de droit international public. L'avantage d'un accord international réside dans la portée qu'il peut avoir puisqu'il est signé entre États et ceux qui le ratifient ou y adhèrent sont tenus de le respecter. En revanche, le domaine poursuivi par nos principes est trop borné au seul champ de la technologie *blockchain*. Par exemple, la « *convention de Genève* » du numérique à l'étude engagerait les gouvernements à adopter les normes requises afin de protéger les citoyens sur Internet en temps de paix. Il semblerait que rédiger un traité sur une technologie en particulier ne soit pas approprié car le sujet est trop restreint et ses enjeux n'embrassent qu'un nombre limité d'individus sur un objet autre que celui des droits et libertés fondamentaux.

476. Une autre option consisterait à s'orienter sur un instrument juridique de l'Organisation de coopération et de développement économiques (OCDE), à l'instar de la convention en négociation pour la taxation des géants du numériques[1027]. Il ne semble pas toutefois que ce type de mesures contraignantes soient adaptées à un besoin de reconnaissance des éléments d'une technologie. D'autant plus qu'elles ne seraient pas suffisamment précises pour être intégrées dans un accord à ce stade d'évolution technologique de la *blockchain*.

477. Par ailleurs, une charte de bonnes conduites et des recommandations non contraignantes délivrées par des organisations internationales comme l'Organisation des Nations Unies pourraient tout à fait être envisageables concernant la reconnaissance internationale des preuves *blockchains*[1028]. Ces outils de *soft law* dans le système juridique international font parfois céder le droit dur[1029] dans le domaine du numérique. L'exemple européen d'une charte éthique d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement en

[1026] Elle est proposée par la Professeure F. Jault-Seseke : F. Jault-Seseke, « La blockchain au prisme du droit international privé, quelques remarques », *op.cit.*, p.545.
[1027] https://www.liberation.fr/france/2020/01/17/taxe-gafa-un-accord-a-l-ocde-sinon-la-guerre-commerciale_1773724 (consulté le 31/05/2020).
[1028] Cette alternative est aussi proposée par la Professeure F. Jault-Seseke : F. Jault-Seseke, « La blockchain au prisme du droit international privé, quelques remarques », *op.cit.*, p.545.
[1029] P. M. Eisemann, « The gentleman's Agreement comme source du droit international », JDI, 1979, p.329.

est une bonne illustration[1030]. Nous développerons le contenu de ces instruments et orientations de politique internationale ci-après.

478. **Loi type de la CNUDCI sur la *blockchain*.** C'est un texte législatif qui doit être envisagé par la CNUDCI[1031]. Cette Commission est appelée à représenter les régions, les systèmes juridiques, économiques et sociaux, conformément à une répartition équilibrée entre les pays développés et en voie développement. Sa principale mission est alors « *d'encourager l'harmonisation et l'unification progressive du droit commercial international* » des trente-six États membres[1032]. La CNUDCI a préparé un nombre de textes juridiques de différentes natures, notamment des traités[1033], des lois-type[1034], des guides et textes de nature contractuelle[1035].

479. Une loi type, « *instrument de pluralité d'expression* »[1036], est un outil hybride qui serait d'un intérêt certain au sujet de la technologie *blockchain* dans le but de réduire les incertitudes quant à l'effet juridique résultant de l'usage de cette technologie et de contribuer ainsi à favoriser son économie et son efficacité entre les États membre. Elle serait proposée à la volonté des États et leur laisserait ainsi une marge d'appréciation large[1037]. Cette loi type aurait davantage pour but d'harmoniser plutôt que d'unifier et pourrait tout au plus être volontairement intégrée ou adaptée en droit interne par les législateurs[1038]. Elle s'inscrirait dans une démarche générale de proposition des principes généraux internationaux de la technologie

[1030] Conseil de l'Europe, CEPEJ, Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement, Adoptée lors de la 31e réunion plénière de la CEPEJ, 3-4 déc. 2018.
[1031] Créée par une résolution 2205 (XXI session) du 7 déc. 1966 pour promouvoir l'harmonisation et l'unification progressives du droit commercial international.
[1032] B. Goldman, « Les travaux de la Commission des Nations unies pour le droit commercial international », JDI, 1979, p.747 ; E. Ustor, « Développement progressif du droit commercial international : un nouveau programme juridique de l'O.N.U. », AFDI, 1980, p.289 ; R. David, « La Commission des Nations unies pour le droit commercial international », JDI, 1980, p.453 ; J.-A. Estrella-Faria, « The work of the United Nations Commission on International Trade Law (U.N.C.I.T.R.A.L.) », RDU, 1996, p.476 ; Le droit commercial uniforme au XXIe siècle, actes du Congrès de la Commission des Nations unies pour le droit commercial international, New York, 18-22 mai 1992, Nations unies, New York, 1995. Site Internet C.N.U.D.C.I., https://uncitral.un.org/fr (consulté le 31/05/2020).
[1033] Par exemple : la Convention pour la reconnaissance et l'exécution des sentences arbitrales étrangères (New York, 1958) ; la Convention des Nations unies sur les contrats de vente internationale de marchandises (Vienne, 1980) ; la Convention des Nations unies sur l'utilisation de communications électroniques dans les contrats internationaux (New York, 2005).
[1034] Par exemple : Loi type CNUDCI sur l'arbitrage commercial international, 1985 ; loi type CNUDCI sur le commerce électronique, 1996 ; loi type CNUDCI sur les signatures électroniques, 2001.
[1035] Par exemple : le règlement d'arbitrage de la CNUDCI.
[1036] S. Poillot-Peruzzetto, « Les méthodes de la CNUDCI : le choix de l'instrument », LPA n°252, 18 dec. 2003, p.47.
[1037] P. Kahn, « La modélisation au service de la fonction normative de la CNUDCI : la modélisation comme instrument », LPA n°252, 18 dec. 2003, p.62.
[1038] M. Luby, « La CNUDCI et l'intégration régionale », LPA n°252, 18 dec. 2003, p.28-33 ; H. Kenfack, « La limitation des textes de la C.N.U.D.C.I aux relations internationales », LPA n°252, dec. 2013, p.75 ;

blockchain établis en des termes abstraits dont un pan inclurait des développements sur la preuve. Elle permettrait en effet d'harmoniser les niveaux d'avancement de chaque État en droit de la preuve en matière de *blockchain* imposant des principes transnationaux dépassant les droits de tradition civiliste et de *common law*[1039]. Par ailleurs, ces principes pourraient être incorporés dans les droits nationaux tels quels pour les États dont les ressources en juristes sont limitées[1040]. Ces adoptions rapides seraient nettement plus efficaces que la procédure de ratification prévue pour une directive et son champ d'application territorial serait plus large. Notons cependant que le succès de ces modèles de loi type au sein des États ne repose pas tant sur leur autorité, mais sur leur utilité quant aux nécessités conjoncturelles[1041]. La loi type vivrait une « *existence indépendante* »[1042] dans chaque ordre national en fonction des besoins spécifiques en matière de technologie *blockchain*.

480. Dans le cadre des changements perpétuels et évolutifs des protocoles de *blockchain* (soit d'établissement de nouveaux protocoles, soit de mise à jour des protocoles existant), la principale difficulté posée par un cadre figé d'une loi type serait qu'une réglementation trop drastique limite, voire anéantisse l'innovation[1043]. Un protocole d'accord dépourvu de force juridique ne serait à l'inverse pas efficace. Il convient donc d'établir des principes neutres qui ne s'adressent ni aux acteurs, et ni aux produits et services[1044]. Les positions des législateurs français et européens partagent largement cette idée de neutralité[1045]. Dans sa résolution du 3 octobre 2018 sur les technologies des registres distribués et les chaînes de blocs, le Parlement européen met en exergue l'idée de renforcer la confiance par la désintermédiation, en son Point H et M, précisant que l'approche normative doit « *être favorable à l'innovation et fondée sur le principe de la neutralité technologique, ce qui permettra également de créer des écosystèmes*

[1039] Voir à ce sujet un projet plus général de droit transnational de la preuve pensé par une partie de la doctrine : L. Cadiet, « Observations sur l'internationalisation du droit de la preuve », *in* Studi di diritto processuale civile in onore di Giuseppe tarzia, Tome I, II, III, giuffrè. editore, 2005, p.305 et 320 ; L. Cadiet et O. Chase, Culture et administration judiciaire de la preuve, XIIe congrès de l'association internationale de droit judiciaire, Mexico, 2003 ; M. Mekki, L. Cadiet, C. Grimaldi, *La preuve : regards croisés*, *op.cit.*, p.175-276.
[1040] S. Poillot-Peruzzetto, « Les méthodes de la CNUDCI : le choix de l'instrument », *op.cit.*, p.47.
[1041] P.Kahn, « La modélisation au service de la fonction normative de la CNUDCI : la modélisation comme instrument », *op.cit.*, p.63.
[1042] P.Kahn, « La modélisation au service de la fonction normative de la CNUDCI : la modélisation comme instrument », *op.cit.*, p.64.
[1043] Voir notamment de cet avis : J.-M. Mis, « Crypto-monnaie : une régulation/réglementation « contre-nature » ou « naturellement indispensable » à son développement ? », Dossier : la justice pénale à l'épreuve des crypto-monnaies, Dalloz IP/IT n°10, oct 2019, p.550.
[1044] Voir l'avis divergent du législateur sur le sujet des crypto-monnaies qui soutient que les règles « *s'adressent aux acteurs et non aux produits eux- mêmes* » (J.-M. Mis, « Crypto-monnaie : une régulation/réglementation « contre-nature » ou « naturellement indispensable » à son développement ? », *op.cit.*, p.550).
[1045] Voir une critique moderne de la neutralité : G. Babinet, La technologie est-elle « neutre » ?, 12 nov. 2019, https://www.lesechos.fr/idees-debats/cercle/la-technologie-est-elle-neutre-1147002 (consulté le 31/05/2020).

et des pôles d'innovation favorables à l'innovation »[1046] et assurer « *(…) la sécurité juridique et (le respecte du) principe de neutralité technologique, tout en promouvant la protection des consommateurs, des investisseurs et de l'environnement* »[1047].

481. Pour le Professeur Thibault Schrepel, si nous décidons de réglementer, il ne faut pas aller à l'encontre de cinq grands principes de la *blockchain*[1048] : le pseudonymat (ne pas imposer la divulgation de l'identité), l'architecture distribuée (ne pas imposer la centralisation qui est à l'origine d'un préjudice causé par un seul acteur), le pair-à-pair (ne pas imposer la réintroduction de l'intermédiaire), l'immuabilité (ne pas permettre d'effacer les données ou revenir sur une transaction, cela impacterait la confiance placée en cette technologie), et la liberté du consensus. Il préconise que le législateur adopte la nouvelle méthode de « *l'infiltration normative* »[1049] et encore la « *réglementation prophylactique* »[1050] pour éviter les obstacles juridiques aux usages encore à découvrir. La CNUDCI doit en définitive mener une politique volontariste minimale, c'est-à-dire une intervention avec prudence dans le cadre de cette loi type[1051] afin de ne pas établir un cadre trop contraignant mais évolutif, offrant une certaine souplesse et marge de manœuvre aux différents pays.

B. Les principes internationaux sur les preuves de données enregistrées dans la *blockchain* à retenir

482. **La construction terminologique : la notion de « *technologie de registres distribués* ».** En préalable, un effort de construction terminologique doit être réalisé dans un but de cohérence entre tous les ordres internes. Ne sera pas retenue, pour qualifier la technologie *blockchain*, la notion de « *base de données distribuée* ». Cette notion est impropre à la technologie *blockchain* dans le sens où bien que la configuration de certaines *blockchains* privées permette le stockage

[1046] Parlement européen, Résolution du 3 oct. 2018 sur les technologies des registres distribués et les chaînes de blocs: renforcer la confiance par la désintermédiation (2017/2772(RSP)), P8_TA(2018)0373, Point H.
[1047] Parlement européen, Résolution du 3 oct. 2018 sur les technologies des registres distribués et les chaînes de blocs: renforcer la confiance par la désintermédiation (2017/2772(RSP)), P8_TA(2018)0373, Point M.
[1048] T. Schrepel, « Is Blockchain the Death of Antitrust Law ? The Blockchain Antitrust Paradox », *op.cit.*, p.328-331.
[1049] *Ibid.*, p.285.
[1050] *Ibid.*, p.329.
[1051] Position partagée de manière générale par : F. A. Hayek, « The Use of Knowledge in Society », The American Economic Review Vol. 35, n°4, sept., 1945, p.519-530.

de données, ces dernières sont souvent chiffrées, et les *blockchains* publiques pour le reste ne peuvent pas contenir de nombreuses données.

483. Le *Cambridge Centre for Alternative Finance* retient la notion de base de données distribuée dans une représentation circulaire des outils de la technologie *blockchain*[1052]. Les bases de données distribuées embrasseraient la technologie de registre distribué qui inclut la technologie *blockchain*, qui elle-même comprend les *blockchains* à permission[1053]. Les bases de données distribuées sont un type de base de données qui n'a pas de base maîtresse centrale décidant unilatéralement de la mise à jour de la base de données, mais les bases de données sont répliquées dans plusieurs pays[1054]. Les registres distribués seraient un sous ensemble des bases de données distribuées utilisant un modèle d'organisation diffèrent de relation entre les nœuds du réseau de « *menace accusatoire* » afin de prévenir la présence de nœuds malhonnêtes sur le réseau[1055]. Et la *blockchain* sous division du registre distribué partagerait le même modèle de menace accusatoire mais présenterait des caractéristiques supplémentaires qui les distinguent.

484. C'est aussi l'interprétation du Parlement européen qui retient dans sa résolution du 3 octobre 2018 sur les technologies des registres distribués et les chaînes de blocs une « *technologie des registres distribués* » (TRD) qui inclurait la *blockchain* « *considérant que la chaîne de blocs n'est que l'un des différents types de TRD* »[1056]. L'utilisation d'une structure spéciale de données qui regroupe les transactions en blocs, et la diffusion de données à tous les participants permet de tenir cette position[1057]. Dans ce type de *blockchain*, il existe enfin des *blockchains* privées. Cette vision circulaire ne semble pas être adaptée à une loi type en termes abstraits.

485. Celle-ci doit alors retenir la notion de « *technologie de registres distribués* » ou « *distributed ledger technology* », terme explicite et précis caractérisant la technologie *blockchain*. Elle serait définie comme un registre distribué entre différents serveurs permettant

[1052] Cambridge Centre for Alternative Finance, University of Cambridge Judge Business School, Global blockchain benchmarking study, *op.cit.*, p.23.
[1053] *Ibid.*, p.23, 24.
[1054] *Ibid*, p.23.
[1055] *Ibid*.
[1056] Parlement européen, résolution sur les technologies des registres distribués et les chaînes de blocs: renforcer la confiance par la désintermédiation (2017/2772(RSP)), point I.
[1057] Cambridge Centre for Alternative Finance, University of Cambridge Judge Business School, Global blockchain benchmarking study, *op.cit.*, p.24.

la transmission, l'enregistrement, et de stockage de données sur support numérique sans organe central de contrôle, et de gestion.

486. **Les principes retenus dans la loi type sur la *blockchain*.** Un ensemble de principes concernant la valeur juridique, la non-discrimination, la sécurité et l'éthique inventoriés ci-après doivent poser les jalons de l'usage viable et uniforme de la technologie *blockchain* au sein des États membres. La matrice des principes suivants seraient consacrés dans la loi type sur la *blockchain* par des articles sur la preuve prévus à cet effet :

- Valeur juridique des données enregistrées dans un registre distribué

La signature par la *blockchain* est considérée comme une signature électronique.
L'horodatage par la *blockchain* est considéré comme un horodatage électronique.
Le registre de la *blockchain* est considéré comme un registre électronique.

- Non-discrimination des données enregistrées dans un registre distribué

Une signature, un horodatage ou toute autre donnée inscrite et enregistrée dans un registre distribué ne peut se voir refuser sa validé et ses effets au seul motif que le registre est électronique et distribué.

- Satisfaction de l'exigence de fiabilité et sécurité du registre distribué

Peu importe la nature du registre distribué mis en œuvre, lorsque la loi soumet la possibilité d'utiliser un registre distribué pour inscrire des données, il doit être fait usage d'un registre distribué dont la fiabilité et sécurité est suffisante.

- Éthique dans la technologie de registres distribués

Les acteurs et fournisseurs de services liés à la technologie de registres distribués s'engagent au respect des droits fondamentaux et des lois visant à lutter contre le blanchiment ou le financement du terrorisme dans la conception et la mise en œuvre des registres distribués.

- Égalité des traitements dans la technologie de registres distribués

Aucune disposition de la présente loi n'est appliquée de manière à exclure, restreindre ou priver d'effets juridiques l'usage d'un registre distribué quelle que soit la nature du registre distribué

employé dès l'instant où il satisfait aux exigences mentionnées ci-avant et aux exigences de la loi applicable.

487. **L'approche avant-gardiste de droit américain.** L'État de l'Illinois aux États-Unis a déjà, par anticipation à ces principes généraux, admis dans la *Blockchain Technology Act*, la valeur et les effets des procédés de la *blockchain* dans la section 10 de ce texte. Elle précise que si une loi exige une signature, la présentation d'une *blockchain* qui contient électroniquement la signature ou vérifie l'intention d'une personne de fournir la signature satisfait à la loi[1058]. Dans une procédure, la preuve d'une signature ne doit pas être exclue du seul fait qu'une *blockchain* a été utilisée pour créer, stocker ou vérifier le *smart contract*, le fichier, ou la signature[1059]. Par ailleurs, elle ajoute qu'une signature ne peut se voir rejeter d'effets juridiques ou un caractère exécutoire uniquement parce qu'une *blockchain* a été utilisée pour créer, stocker ou vérifier une signature[1060].

488. En outre, d'autres États américains tels que le Tennessee[1061], l'Arizona[1062], et New York[1063] discutent actuellement des dispositions de projets de loi portant l'admission et ses modalités de la signature *blockchain*. *E-Sign Act* au niveau de la loi de l'État fédéral[1064] est plutôt favorable à cette admission puisqu'il précise qu'une signature peut apparaître sous la forme électronique dès lors que la personne qui a joint cette signature ou l'a logiquement associée à un contrat ou un registre, avait l'intention de signer le document[1065]. La souplesse de ces dispositions de l'*E-Sign Act* et sa possible adaptation à des technologies nouvelles ne posent, sans nul doute, pas les mêmes difficultés que le règlement eIDAS. Par ailleurs, d'autres mesures sont à l'étude au Nevada[1066], Tennessee[1067], en Ohio[1068], et à New York[1069] comme celles proposant de reconnaître la valeur juridique des enregistrements - à l'image de documents électroniques - dans la *blockchain*. Compte tenu de toutes ces initiatives, il est louable de penser

[1058] BTA, Section 10, d).
[1059] BTA, Section 10, b).
[1060] BTA, Section 10, a).
[1061] TN SB1662.
[1062] HB 2417.
[1063] NY A08780.
[1064] Voir *supra* n°179 en partie préliminaire.
[1065] E-Sign, Section 106 (5).
[1066] NV SB398.
[1067] TN SB1662.
[1068] SB 300.
[1069] NY A08780.

qu'aux États-Unis le droit appréhende mieux l'architecture distribuée de la *blockchain*, que notre droit latin[1070].

Paragraphe 2 : De la réflexion sur des actions pour les preuves de données enregistrées dans la *blockchain* dans le cadre d'une politique mondiale

489. Pour asseoir le rayonnement des preuves générées par la *blockchain*, la réflexion sur les actions à mener par une politique mondiale prend place par des objectifs poursuivis par cette politique (A) pour ensuite laisser s'exprimer des actions mondiales concrètes sur les preuves de données enregistrées dans la *blockchain* (B).

A. Les objectifs poursuivis par une politique mondiale sur les preuves de données enregistrées dans la *blockchain*

490. **La complémentarité des objectifs.** L'établissement d'une politique mondiale contribue au développement progressif d'une ossature internationale uniforme assurant une pérennité par des actions de long terme. Elles exercent un rôle complémentaire pour accompagner la loi type de la CNUDCI sur la *blockchain* et assurent un levier de l'activisme gouvernemental au niveau international. Cette réflexion n'a donc pas pour objectif d'aboutir à l'élaboration de normes au sens strict du terme mais à la proposition d'une politique mondiale de la *blockchain*, afin de favoriser son développement, ainsi que l'égalité et les chances de tous les États de participer à ce développement.

491. **La portée des objectifs.** Il sera établi un cadre de discussion international. Ces actions auront un caractère politiquement influent, alors même qu'elles impliquent une « *procéduralité légère* » et une flexibilité[1071]. Cette politique posera des canaux de coopération entre les États sur la technologie *blockchain* afin d'empêcher l'apparition de pratiques souverainistes. Le forum économique mondial du G20 - déjà très actif sur les sujets de crypto-monnaie,

[1070] F. G'Sell, « Comment traiter juridiquement la décentralisation ? Les ordonnances blockchain et la Lex Cryptographia », *op.cit*.
[1071] F. Chatzistavrou, **«** L'usage du soft law dans le système juridique international et ses implications sémantiques et pratiques sur la notion de règle de droit », Open Edition, Le Portique, janv. 2005, p.7, n°26 et s.

notamment celle de banque centrale à l'étude[1072] - trouverait un ancrage à propos dans l'impulsion de cette initiative de politique globale sur la *blockchain*.

B. Les actions mondiales concrètes sur les preuves de données enregistrées dans la *blockchain*

492. **Le groupe international d'experts sur la *blockchain* de l'OCDE.** La politique serait concrètement déployée au sein de l'OCDE dans la continuité de la création du centre politique *blockchain* de l'OCDE en 2018 par son Comité des marchés financiers en coopération avec le Comité de la politique de l'économie numérique[1073]. Ce centre soutient actuellement la coordination de travaux et constitue ainsi un point de référence mondial grâce à un groupe international d'experts réunis au *Blockchain Expert Policy Advisory Board* (BEPAB) (ou conseil consultatif politique d'experts sur la *blockchain*)[1074], comptabilisant quarante-cinq gouvernements de pays membres et non membres de l'OCDE, des représentants de la Commission européenne, du secteur privé, et de la société civile. Pour l'heure, ces derniers sont chargés d'établir des *high-level blockchain policy principles* (ou grands principes politiques de la *blockchain*), de rédiger des rapports et de siéger aux événements annuels de l'*OECD Global Blockchain Policy Forum* (ou Forum mondial de l'OCDE sur la *blockchain*)[1075].

493. Dans le même temps, la Commission européenne a créé en avril 2018 *The European Blockchain partnership*, un partenariat sur la blockchain qui réunit les membres de l'Espace économique européen[1076]. Cette politique européenne impulse un travail commun des signataires à la réalisation du potentiel des services basés sur la *blockchain* au profit des citoyens, de la société et de l'économie[1077]. Le partenariat met aussi en place une infrastructure européenne de services de *blockchain* ou *European Blockchain Services Infrastructure* (EBSI) qui fournira des services publics transfrontaliers à l'échelle de l'Union européenne en utilisant

[1072] World Economic Forum, Insight Report, Central Bank Digital Currency Policy-Maker Toolkit, Centre for the Fourth Industrial Revolution, janv. 2020, http://www3.weforum.org/docs/WEF_CBDC_Policymaker_Toolkit.pdf (consulté le 31/05/2020).
[1073] http://www.oecd.org/finance/oecd-*blockchain*-policy-forum.htm (consulté le 31/05/2020).
[1074] http://www.oecd.org/finance/oecd-forms-a-high-level-expert-group-on-*blockchain*.htm (consulté le 31/05/2020).
[1075] https://www.oecd.org/finance/oecd-*blockchain*-policy-forum.htm (consulté le 31/05/2020).
[1076] https://ec.europa.eu/digital-single-market/en/*blockchain*-technologies (consulté le 31/05/2020).
[1077] *Ibid*.

cette technologie. En 2020, l'EBSI projette le déploiement d'un réseau de nœuds distribués dans toute l'Europe, en soutenant des applications axées sur des cas d'usage sélectionnés[1078].

494. Notons que la France s'est aussi dotée d'une « *Task force Blockchain* » réunissant des experts du secteur public et privé[1079]. À l'occasion de la formation de cette *task force*, une stratégie nationale *blockchain* a été lancée, fruit d'un travail mené par la Direction générale des entreprises rattachée au Ministère de l'Économie et des Finances avec l'écosystème de la *blockchain*[1080].

495. **La proposition d'une politique volontariste de l'OCDE.** L'OCDE projette, *en sus*, d'aider les gouvernements dans leurs prospectives stratégiques de planification des scénarii sur des horizons à long terme[1081]. En revanche, le rôle de cette politique mondiale impulsée par l'OCDE doit être plus volontariste et force de proposition. Il convient de baser cette politique sur des objectifs concrets grâce aux propositions d'actions mondiales suivantes :

- guider les États membres et non membres dans leur transformation technologique par la *blockchain* en les conseillant pour établir un environnement politique encourageant l'innovation par la technologie *blockchain* ainsi qu'une réglementation favorable pour cela et viable sur le long terme ;
- établir les priorités nationales pour les États membres et non membres en matière de *blockchain* afin de répartir les opportunités de création de richesse et de développement économique ;
- rédiger une charte éthique pour les acteurs de la *blockchain*, les entreprises, et les États membres et non membres ;
- surveiller les risques d'utilisations abusives et soutenir les usages éthiques de la *blockchain* ;
- soutenir l'expérimentation de projet de solutions basées sur la technologie *blockchain* ;

[1078] *Ibid*.
[1079] https://www.latribune.fr/entreprises-finance/bercy-lance-sa-task-force-*blockchain*-pour-pousser-l-adoption-dans-l-industrie-824584.html (consulté le 31/05/2020).
[1080] https://www.entreprises.gouv.fr/numerique/lancement-de-la-strategie-nationale-*blockchain* (consulté le 31/05/2020).
[1081] https://oecdonthelevel.com/2020/01/22/how-the-oecd-can-release-the-power-of-*blockchain*/ (consulté le 31/05/2020).

- soutenir la recherche sur l'évolution des protocoles *blockchains* (notamment et en priorité, la recherche sur les algorithmes de consensus de substitutions respectueux de l'environnement) ;

- étendre le champ des experts de l'OCDE aux développeurs travaillant sur les protocoles *blockchains* depuis l'origine ;

- échanger et connaître la complexité des protocoles déployés par certaines entreprises et institutions et leurs évolutions (rapides en pratique) afin de permettre aux États membres et non membres ainsi qu'aux autres entreprises de s'adapter ;

- soutenir les entreprises et institutions souhaitant transformer leurs modèles et changer leur façon de créer et de capter de la valeur grâce à cette technologie.

Cette ossature internationale suggérée pourra former une boîte à outils utile en France mais aussi aux autres pays. Il relève du ressort des institutions nationales dans leurs politiques publiques et des législateurs nationaux d'adapter cette matrice avec plus ou moins de libéralisme. Nous établirons dans les développements suivants une proposition de réception en droit interne de cette ossature par un régime dual de *hard law* et *soft law* relatif aux preuves de données enregistrées dans la *blockchain* (section 2).

Section 2 : Une proposition de réception en droit interne de l'ossature internationale : un régime dualiste *hard law* et *soft law* sur les preuves de données enregistrées dans la *blockchain*

496. Les « *preuves putatives* » transnationales établies par la *blockchain* doivent se voir reconnaître en droit français sur la base du canevas international préétabli[1082]. Le législateur français préconise une réglementation « *d'avance de phase* » par un cadre expérimental[1083], à l'instar de celui proposé par les ordonnances minibon et *blockchain* mais qui reste d'une portée restreinte. Le député Jean-Michel Mis déclare qu' « *après 11 mois de travaux, 40 auditions et déplacements en France, en Suisse et aux États- Unis, le constat est sans appel si nous voulons que se développent en France des entreprises innovantes, il nous faut un cadre réglementaire,*

[1082] Voir en ce sens : F. G'sell, « Preuve et signature numérique », *op.cit.*, p.99 : « *(…) l'apport de la technologie blockchain dont le droit de la preuve doit tenir compte* ».
[1083] J.-M. Mis, « Crypto-monnaie : une régulation/réglementation « contre-nature » ou « naturellement indispensable » à son développement ? », *op.cit.*, p.550.

financier et fiscal qui permette à notre pays d'être attractif, mais aussi qui sécurise les investisseurs et les usagers »[1084] . Les praticiens appellent pour la majorité d'entre eux à une « *attitude raisonnable* »[1085] des législateurs : réglementer de manière trop hâtive serait prendre le risque de mal réglementer. Les législateurs ne doivent pas utiliser la complexité de cette nouvelle technologie pour justifier d'une réglementation trop répressive ou d'une « *sur-réglementation* »[1086]. La promotion de l'innovation est une entreprise risquée qu'il convient de stabiliser à travers un cadre normatif souple de *hard law* par une *lex blockchain* (paragraphe 1) et de *soft law* sur les preuves de données enregistrées dans la *blockchain* (paragraphe 2).

Paragraphe 1 : De la réflexion sur une *lex blockchain* à la française sur les preuves de données enregistrées dans la *blockchain*

497. La réflexion sur une loi générale relative à la technologie *blockchain* c'est-à-dire une « *lex blockchain* » aux caractéristiques d'une *hard law* doit porter en partie sur la reconnaissance des données enregistrées dans la *blockchain*. Il n'est plus à confirmer que la preuve légale préconstituée favorise la simplicité et la sécurité, prisées par les plaideurs[1087]. Le juge n'a plus qu'à appliquer de façon automatique la règle probatoire, pour aboutir à la vérité cryptographique exacte. *A contrario*, la liberté de la preuve ne servirait pas la vérité cryptographique car elle supposerait une amplitude dans l'interprétation. Or, la vérité cryptographique est exacte et ne nécessite pas une interprétation très large, seulement pour déterminer la fiabilité technique du protocole. Le principe de liberté de la preuve est sans doute celui qui laisse toutefois le plus de chances à la manifestation de la vérité juridictionnelle, puisqu'il donne au juge toute la latitude pour se fonder sur les preuves les plus pertinentes[1088]. Il instaure en contrepartie une potentielle *« recherche probatoire hasardeuse »* et un *« pouvoir judiciaire excessif »*[1089].

[1084] *Ibid.*, p.550.
[1085] Institut Sapiens, Y. de Monbynes et G. Grandval, Rapport Bitcoin totem et tabou. Que présage l'essor des crypto-monnaies ?, *op.cit.*, p.88.
[1086] T. Schrepel, « Is Blockchain the Death of Antitrust Law ? The Blockchain Antitrust Paradox », *op.cit*, p.285.
[1087] F. Ferrand, Preuve, *op.cit.*, n°27.
[1088] X. Lagarde, « La preuve en droit », *in* Le temps des savoirs, Odile Jacob, 2003, p.103.
[1089] F. Terré, *Introduction générale au droit*, 9e éd., 2012, Précis Dalloz, no 609.

498. La deuxième recommandation du rapport Toledano incite à la réflexion sur les modalités techniques à retenir pour reconnaître une pleine force juridique à la signature et à l'horodatage réalisés sur une *blockchain*[1090]. Pourtant, cette *lex blockchain* n'est soutenue, ni par le législateur, ni par le Ministère de la Justice[1091]. C'est une tentative vaine par les amendements n°773, n°434, et n°1309 déposés au projet de loi n°1088 PACTE - examiné en Commission spéciale - d'ajout à l'article 1358 du Code civil sur la liberté de la preuve des dispositions sur la preuve *blockchain*. Cette proposition de modification était alors introduite comme ceci : « *Hors les cas où la loi en dispose autrement, la preuve peut être apportée par tout moyen. Lorsqu'il est électronique, le moyen consiste notamment en l'usage d'un dispositif électronique d'enregistrement partagé, de nature publique ou privée, dès lors que ledit dispositif électronique d'enregistrement partagé répond à des conditions définies par décret en Conseil d'État* »[1092]. Ces amendements ont été, rejeté pour le premier et non soutenus pour les deux derniers. Pour justifier de ce rejet, il a été argué que ces enregistrements dans la *blockchain* - constituant une preuve par tout moyen possible à apporter pour prouver un fait - « (…) *relève(nt) moins de la loi que de l'usage* ». Pour le rapporteur des affaires économiques de la loi, il ne paraissait « *(…) pas utile de détailler les moyens électroniques concernés* »[1093]. Le ministre de l'Économie et des Finances a ajouté que « *par ailleurs, le Code civil prévoit explicitement que la preuve de l'origine, de la date et de la nature des contributions intellectuelles peut être apportée par tout moyen, sans n'en mentionner aucun à dessein. La rédaction actuelle du Code civil présentant l'avantage d'une plus grande souplesse et couvrant, par définition, la blockchain ou toute autre forme de preuve qui pourrait être mise à disposition (…)* »[1094]. L'absence de nécessité d'intégrer une disposition spécifique dans le droit commun au côté du principe de liberté de la preuve des faits juridiques est ressortie de ces débats parlementaires. Au stade de la liberté de la preuve, le Code civil n'a point besoin d'être précisé pour user de la *blockchain* au soutien du succès de la preuve d'un fait mais nous ne saurions être aussi catégoriques lorsque la preuve n'est pas libre et quant aux modes de preuves spécifiques des différents procédés permis par la *blockchain* (signature, horodatage et empreinte *blockchain*) qui suscitent encore de nombreuses interrogations. Cette partie aura donc pour

[1090] F. G'sell, « Preuve et signature numérique », *op.cit.*, p.109.
[1091] Question écrite n°22103 de D. Fasquelle, publiée au JO le 30/07/2019, réponse du Ministère de la Justice publiée au JO le 10/12/2019, p.10774. Voir annexe n°10.
[1092] Voir annexe n°5.
[1093] Pour le rejet de l'amendement n°773 voir : Projet de loi n°1088 dit « PACTE », Commission spéciale chargée d'examiner le projet de loi relatif à la croissance et la transformation des entreprises, Compte rendu n°18, Réunion du Jeudi 13 sept. 2018, Séance de 15 heures, http://www.assemblee-nationale.fr/15/cr-cspacte/17-18/c1718018.asp (consulté le 31/05/2020).
[1094] Voir annexe n°6.

objet de reconnaître la « *certification* » de données inscrites dans un registre distribué (A), puis l'« *authentification* » de l'« *inscriveur* » de ces données (B) ainsi que leurs datations dans ce registre (C).

A. La certification des données inscrites dans un registre distribué

499. La certification des données inscrites dans un registre distribué suscite des réflexions quant au choix même de la notion de « *certification* » (1), aux contours de cette reconnaissance (2), et aux modalités de vérification des données inscrites dans un registre distribué (3). Elle suppose enfin que tout plaideur puisse engager des recours contestant cette certification (4).

1. Le choix de la notion de « *certification* »

500. **L'exclusion de la vérification de la véracité des données dans la « *certification* ».** Les données inscrites dans une *blockchain* publique ou privée permettent leur certification. C'est le terme de « *certification* » qui sera retenu et non d' « *authentification* » car l'authentification au sens d'une opération consistant à vérifier la véracité d'un document ou d'une donnée porterait à confusion en ce que des données fausses, corrompues, voire illégales comme du contenu pédopornographique peuvent être intégrées dans la *blockchain*[1095]. La *blockchain* ne peut pas, par elle-même, garantir la qualité et l'exactitude des données externes - que l'on pourrait appeler autrement « *non-natives* » - entrées et stockées dans le registre distribué. Une *blockchain* n'évalue pas si une donnée entrante est vraie ou non. Si l'entrée est inexacte ou incorrecte, la *blockchain* la traitera comme d'autres données intégrées dans la *blockchain*[1096]. Elle sera ensuite transmise et stockée avec son caractère inexact ou erroné. Les registres certifiants de données ne sont corrects que si l'information répertoriée l'est aussi elle-même. Par exemple, si un registre de droits de propriété intellectuelle contient des erreurs dans les transferts desdits droits, cela ne permettrait pas, en tout état de cause, de connaître la titularité exacte de ces droits. La problématique de l'ancrage de fausses informations est une difficulté technique qui persiste avec l'immuabilité du registre. La technologie *blockchain* aggrave cette

[1095] R. Matzutt , J. Hiller, M. Henze , J. Henrik Ziegeldorf , D. Mullmann , O. Hohlfeld, K. Wehrle , « A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin », *op.cit.*, p.6-7.
[1096] Cambridge Centre for Alternative Finance, University of Cambridge Judge Business School, Global blockchain benchmarking study, *op.cit.*, p.18.

problématique initiale de fausse donnée ou contenu illicite en rendant quasiment impossible l'effacement ou la modification d'une fausse donnée ou d'un contenu.

501. **La confusion générée par la notion d'« *authentification* ».** Bien qu'authentifier (selon son premier sens toujours) soit un synonyme de certifier[1097], construit d'après cette notion signifiant vérifier, attester l'authenticité d'un document ou d'un écrit[1098], il porte à confusion avec l'authentification dégagée par le règlement eIDAS. Selon ce règlement, authentifier est un processus numérique consistant en l'identification électronique d'une personne physique ou morale ou l'origine et l'intégrité d'une donnée[1099].

502. Certifier peut, en outre, se traduire en anglais par « *authenticate* » tout comme authentifier, ce qui a pu créer des confusions avec le second sens de l'authentification de notre système latin[1100]. À titre d'illustration, l'État du Vermont aux États-Unis a admis dans une loi H.868 (Act no. 157) relative au développement économique divers l'auto-authentification ou « *self-authenticating* » des enregistrements numériques dans la *blockchain* conformément à loi 902 du Vermont sur la preuve, s'ils sont accompagnés d'une déclaration écrite faite sous serment d'une personne qualifiée[1101]. Précisons qu'aux États-Unis la loi fédérale sur la preuve, la *Federal Rules of Evidence* permet l'auto-authentification de nombreuses preuves numériques. En d'autres termes, des éléments de preuve peuvent s'authentifier eux-mêmes et nécessitent pas de preuves extrinsèques pour être admis. C'est le cas des documents certifiés générés par un processus ou un système électronique[1102] ou encore des données certifiées copiées à partir d'un dispositif électronique, d'un support de stockage ou d'un fichier[1103].

503. **L'abstraction de l'intervention d'une autorité publique dans la notion de « *certification* ».** La certification est définie au sens fort comme le fait pour une autorité de rendre certain un acte ou un fait en affirmant après vérification, sa véracité, son authenticité, son origine, sa conformité. Au sens atténué, il s'agirait pour une personne quelconque d'attester, d'affirmer avec assurance l'existence d'un fait[1104]. Cependant, cette notion au sens fort introduit

[1097] Voir *supra* n°268.
[1098] G. Cornu, *Vocabulaire juridique*, *op.cit.*, Voir authentifier n°1, p.106.
[1099] Règl. eIDAS, art. 3, 5.
[1100] Voir *supra* n°268.
[1101] H. 868 (Act no. 157) relating to miscellaneous economic development, signed by Governor 6/2/16, Sec. I.1. 12 V.S.A. § 1913. Voir annexe n°12.
[1102] FRE 902, Rule 902, (13).
[1103] FRE 902, Rule 902, (14).
[1104] G. Cornu, *Vocabulaire juridique*, *op.cit.*, Voir sens n°1 de certifier, p.160.

la nécessaire intervention d'une autorité qui n'est pas indiscutablement prescrite. En revenant à l'origine latine du terme certification, nous nous rendons compte qu'étymologiquement *certificare* est issu de *certus* qui signifie « *certain* » et *facere* « *rendre certain* ». Cette étymologie ne fait assurément pas référence et ne distingue pas quant à l'intervention ou non d'une autorité, ce qui conforte la sélection de ce terme. Rappelons en effet que dans le cadre d'une *blockchain* publique, l'autorité absente est substituée par la puissance cryptographique, qui est telle qu'elle rend certaine l'existence les données inscrites dans son registre, alors que dans celui d'une *blockchain* privée ou publique permissionnée, une ou plusieurs autorités peuvent intervenir représentée par une ou plusieurs entités publiques ou privées[1105].

504. Notons toutefois que la possibilité déjà reconnue de l'« *authentification* » des opérations de cession de minibons dans le DEEP sera regardée comme un usage spécial réglé par l'illustre principe selon lequel les règles spéciales dérogent aux règles générales[1106]. Il s'agira ainsi de reconnaître par l'inscription générale de données dans la *blockchain*, leurs certifications, résultat de cette action.

2. Les contours de la reconnaissance de la certification des données inscrites dans un registre distribué

505. **La reconnaissance juridique de la certification de données inscrites dans un registre distribué.** La reconnaissance de la certification de données par la *blockchain* implique que cette certification des données (en clair ou non), inscrites dans un registre distribué, dispose d'une valeur juridique en droit français. Il pourrait être indiqué dans cette loi que toutes données inscrites dans un registre distribué valent certification de ces données.

506. **La présomption simple de fiabilité de la certification dans les *blockchains* publiques.** La certification de données réalisée dans un registre résilient de *blockchain* publique serait dès lors présumée fiable. Comme mentionné dans la partie technique préliminaire plus avant : plus les nœuds d'une *blockchain* sont importants, plus le réseau est robuste, moins les transactions du registre sont altérables[1107]. C'est la raison pour laquelle une présomption légale

[1105] Voir *supra* n°20 et s.
[1106] En latin : *Specialia generalibus derogant*.
[1107] Voir *supra* n°99.

sous la forme d'une « *présomption de postulat* »[1108] est bienvenue pour les *blockchains* publiques. Celui au profit duquel cette présomption existe serait dispensé de preuve de fiabilité de la *blockchain* publique en cause. Cette présomption simple pourrait toutefois être renversée par celui qui apporte par tout moyen la preuve que la *blockchain* publique utilisée n'était pas fiable.

507. **L'hypothèse du *fork*.** Cette intégrité mérite une analyse différente dans l'hypothèse de *fork*[1109]. Lorsqu'un *hard fork* est voté, tout le registre antérieur reste valable et deux registres existent séparément l'un de l'autre pour l'avenir : le registre traditionnel au côté d'un registre nouveau. Il n'est pas certain que dans ce cas, le nouveau registre puisse prétendre à autant de fiabilité que l'ancien car ce dernier sera composé d'un nombre moins important d'acteurs adhérant au réseau. Il serait logique que ce nouveau registre perde en sécurité. Dans cette hypothèse, il conviendrait alors d'exclure du bénéfice de la présomption le nouveau registre issu du fork.

508. Contractuellement, cette hypothèse de *fork* peut être anticipée à l'origine, d'une part, en permettant une réévaluation du nouveau registre et l'établissement de la valeur probatoire des nouvelles inscriptions[1110], et d'autre part, en précisant la constance de la valeur probatoire pour les inscriptions déjà réalisées. Lorsqu'elle n'est pas anticipée en amont, cette hypothèse peut aussi faire l'objet d'un avenant signé entre les membres de la chaîne ancienne et nouvelle dans le but de s'accorder sur l'évolution de la nouvelle chaîne[1111]. La décision du 26 février 2020 du Tribunal Commercial de Nanterre met en lumière la nécessaire vigilance des parties (surtout lorsqu'elles sont averties) dans la rédaction de conditions générales de vente d'une plateforme d'échange de crypto-monnaies au sujet de l'hypothèse de *fork*[1112]. En l'espèce, la plateforme d'échange n'avait pas anticipé que le *fork* puisse donner lieu à la création d'une crypto-monnaie différente : le bitcoin cash dans le cas du *hard fork* de Bitcoin. Le juge condamne alors l'absence

[1108] A.-B. Caire, *Relecture du droit des présomptions à la lumière du droit européen des droits de l'homme*, Pedone, coll. publications de l'Institut International des Droits de l'Homme, th. ss. dir. J.-P.Marguénaud, 2012, p.35, 76 ; M. Mekki, « Charge de la preuve et présomptions légales. L'art de clarifier sans innover », Droit & patrimoine n°250, sept. 2015, p.6.
[1109] Voir *supra* n°26. Voir aussi : A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder, *Bitcoin and Cryptocurrency Technologies*, *op. cit.*, p.96-98.
[1110] Voir *infra* n°691.
[1111] M.-A. Ledieu, « La Baas démocratise la blockchain », *op.cit.*, p.367.
[1112] T. com. Nanterre, 26 févr. 2020, n°2018F00466, BitSpread c/ Paymium : « *Attendu enfin que le tribunal observe que les CGU de PAYMIUM comme les 3 contrats de prêt signés entre les parties aux dates susvisées, ne comportent pas de clause quant à l'attribution d'éventuelles crypto-monnaies issues de " hard forks ", alors même que les parties sont des professionnelles averties du marché des crypto-monnaies, l'une pour y exercer des activités de conseil aux investisseurs et de tenue de marché, l'autre pour exploiter une plateforme d'échange* ».

de clause d'attribution d'éventuelles crypto-monnaies issues de *hard fork* et considère comme infondée une demande subsidiaire d'indemnisation sur la base de l'enrichissement sans cause.

509. **La présomption simple d'identification de l'inscriveur dans les *blockchains* privées.** Par ailleurs, ces données inscrites dans un registre distribué pourraient bénéficier de la qualification d'écrit électronique à condition de pouvoir prouver que la *blockchain* en cause réussi à identifier l'inscriveur. Dans une *blockchain* privée ou publique permissionnée, l'identification de l'inscriveur pourrait être présumée une fois le troisième palier susmentionné atteint[1113], jusqu'à preuve du contraire. Celui au profit duquel cette présomption existe serait dispensé de preuve d'identification de l'inscriveur. Cette présomption simple pourra toutefois être renversée par celui qui apporte par tout moyen la preuve que la *blockchain* privée ou publique permissionnée utilisée ne permet pas d'identifier l'inscriveur.

510. **La qualification de copie de l'empreinte de données inscrites dans un registre distribué.** Précisons que si les données inscrites dans un registre distribué sont une empreinte numérique de données, elles pourraient bénéficier de la qualification de copie au sens de l'article 1379 du Code civil[1114]. L'empreinte numérique inscrite dans un registre distribué serait dite fiable au sens de l'article 1379 du Code civil dès l'instant où l'intégrité de l'ensemble de données serait vérifiée par un nouveau calcul de l'empreinte desdites données. Si l'empreinte initiale est identique à l'empreinte des données calculée au moment de la vérification, l'intégrité des données ancrées serait acquise en l'absence de modifications des données ancrées à l'origine. L'ancreur devra alors conserver les données originales sur un espace de stockage externe à la *blockchain* pendant toute la durée nécessaire à prouver ces données[1115]. Si elle est dite fiable, l'empreinte numérique aura la même force probante que les données qu'elle représente. Dans ce cas, un simple renvoi à l'article du Code civil sur la copie dans la *lex blockchain* sera suffisant ; une modification du Code civil pour l'unique sujet de la technologie *blockchain* ne semble pas opportun.

[1113] Voir *supra* n°384.
[1114] Voir *supra* n°393 et s.
[1115] Voir une obligation de conservation similaire du tiers chargé de l'acheminement des lettres recommandées électroniques : Décret n°2011-144 du 2 février 2011 relatif à l'envoi d'une lettre recommandée par courrier électronique pour la conclusion ou l'exécution d'un contrat, art. 2 al. 2

3. Les modalités de vérification des données inscrites dans un registre distribué

511. Un certain nombre de palliatifs peuvent être prévus à la problématique de la vérification du contenu intégré dans la *blockchain*. Dans l'hypothèse où le contenu souhaiterait être vérifié, l'idée de faire intervenir des acteurs traditionnels, de nouveaux acteurs privés ou une autorité pour contrôler les données intégrées dans la *blockchain* est soulevée.

512. **Les acteurs traditionnels.** Des acteurs traditionnels, comme des notaires, des avocats, ou des huissiers pourraient ainsi être habilités en vue de détenir un droit d'écriture[1116].

513. **Les nouveaux acteurs privés.** Selon la chercheuse Primavera de Filippi, « *sans opérateur de confiance ou autorité de confiance chargée d'examiner et de valider les données enregistrées sur une chaîne de blocs, il n'existe aucune garantie quant à la qualité et à l'exactitude des informations stockées dans une blockchain* »[1117]. La pratique est aujourd'hui courante d'introduire des données par référence à une base de données fiable externe à la *blockchain*. Déjà plusieurs *blockchains* s'appuient sur une source de données exogène fournie par des prestataires nommés « *Oracles* ». Ce pourvoyeur de données fournit des informations de référence fiables comme des certificats prouvant l'identité d'une personne ou d'un actif. Dans ces cas, la confiance est externe, dévolue à des acteurs qui ne font pas partie de la chaîne[1118].

514. **Les nouveaux acteurs publics.** Le rapport De la Raudière/Mis a proposé aussi l'évaluation de l'intérêt de consacrer dans une loi le statut de tiers de confiance numérique chargé d'assurer la protection de l'identité, des documents, des transactions, d'auditer et de certifier les protocoles *blockchains*[1119].

515. Une technique sans intervention de tiers doit néanmoins être considérée. Elle consisterait à trouver une solution dans l'interopérabilité pour partager directement des informations entre les différentes *blockchains* sans qu'il ne soit nécessaire de faire intervenir une autorité ou un acteur. De telles solutions sont souvent utilisées pour fournir la confiance

[1116] En ce sens : M. Mekki, « Blockchain et métiers du droit en questions », Dossier « Blockchain et métiers du droit : une force vive ou subversive ? », Dalloz IP/IT n°2, févr. 2020, p.89.
[1117] P.de Filippi, A. Wright, *Blockchain and the Law*, *op.cit.*, p.114.
[1118] EU Blockchain Observatory and Forum, Scalability interoperability and sustainability of *blockchains*, *op.cit.*, p.11.
[1119] Assemblée nationale, Rapport d'information n°1501, *op.cit.*, p.63.

nécessaire à l'échange de données ou à l'exécution d'opérations, créant ainsi un pont direct entre *blockchains*[1120].

4. Les recours contre la certification des données inscrites dans un registre distribué

516. **La procédure de vérification d'écriture.** Des garde-fous sont à prévoir à l'encontre de cette certification. Il est possible d'envisager le recours de droit commun de procédure de vérification d'écriture à l'encontre de la certification qui remplirait les obligations de l'écrit, conformément à l'article 287 du Code de procédure civile. Cette dénégation porterait vraisemblablement sur l'écrit sous signature privée sous-jacent à une empreinte certifiée par la technologie *blockchain*. Il s'agirait d'un recours d'une partie qui dénierait la certification qui lui est attribuée ou qui contesterait celle attribuée à un l'inscriveur. Il ne serait pas question de vérifier la validité de l'acte, ni la portée ou le sens de clauses, mais seulement l'attribution de l'écriture à une personne[1121]. C'est ainsi une dénégation qui ruinera l'efficacité probatoire de l'écrit sous-jacent[1122].

517. **L'exclusion de la procédure de faux.** La procédure de faux des articles 299 et suivants du Code de procédure civile doit être exclue de la certification de données par la *blockchain,* dans la mesure où le faux matériel qui résulte d'un acte fabriqué au soutien d'une imitation de l'écriture d'autrui ou d'un acte qui a été altéré par des ratures ou des additions[1123], ne peut trouver à s'appliquer dans un contexte d'échange de données numériques quasiment inaltérables. Seul le faux intellectuel pourrait être envisagé puisqu'il ne comporte aucune intervention sur l'écrit lui-même mais il est possible de recourir à cette action uniquement lorsque la portée d'un acte en est dénaturée par le rédacteur. C'est en d'autres termes lorsque l'acte constate comme vrais des faits faux dans le cadre de l'acte authentique que ce recours s'applique[1124]. Cependant, l'élaboration d'un acte authentique étant difficilement envisageable avec le support de la *blockchain,* celui-ci ne pourrait pas constater comme vrais des faits faux

[1120] EU Blockchain Observatory and Forum, Scalability interoperability and sustainability of *blockchains, op.cit.*, p.11.
[1121] Cass. civ., 8 janv. 1936 : DH 1936, p.97.
[1122] C. Brahic Lambrey, Fasc. 10 : Vérification d'écriture. Faux et inscription de faux, *op.cit.*, n°2.
[1123] *Ibid.*, n°40.
[1124] *Ibid*.

dans ces circonstances[1125]. La procédure de faux ne pourra donc être un recours envisageable dans le cadre de la certification de données par cette technologie.

Cette action de certifier établie[1126] est dédiée à l'inscriveur et permet, par la même, de l'authentifier.

B. L'authentification de l'inscriveur de données dans un registre distribué

518. L'authentification de l'inscriveur de données dans un registre distribué implique dans un premier temps d'expliquer les raisons du choix de l'emploi du terme « *authentification* » (1), dans un second de comprendre les effets de cette authentification, c'est-à-dire l'assentiment à certifier des données (2), pour dans un dernier temps envisager les recours possibles à cette authentification (3).

1. Les raisons de l'authentification de l'inscriveur

519. **L'imputabilité de la transaction.** L'inscriveur, sujet de droit, est titulaire d'un droit de propriété sur une paire de clés (dans une *blockchain* publique) une clé publique accessible et une clé privée constituant sa signature qu'il garde secrète. Cette clé privée lui permet de signer une transaction créant ainsi un lien entre elle et le signataire. C'est une notion d'authentification et non d'identification qui est mobilisée, permettant à l'inscriveur usant d'une signature *via* la *blockchain* de prouver qu'il possède bien la clé privée correspondant à sa clé publique[1127]. L'enjeu de cette notion d'identification revient finalement à l'interrogation de l'imputabilité de la transaction, soit la question de savoir qui est l'inscriveur des données dans le registre de la *blockchain*[1128]. L'impossible vérification de l'habilitation du titulaire d'un droit ayant qualité à ancrer ne permet pas de retenir cette identification[1129]. Cette interrogation sur l'identification

[1125] Voir *supra* n°265 et s.
[1126] G. Cornu, *Vocabulaire juridique*, *op.cit.*, Voir certification, p.160 : c'est le résultat de l'action et l'action de certification elle-même que recouvre la notion de « certification ».
[1127] A. Barbet-Massin, « Le droit de la preuve des œuvres d'art », *op.cit.*, p.16.
[1128] Voir sur la question de l'imputabilité : T. Douville, « *blockchains* et preuve », *op.cit.*, p.2194.
[1129] Sur cette question en droit d'auteur : CSPLA, Rapport de la mission sur l'état des lieux de la *blockchain* et ses effets potentiels pour la propriété littéraire et artistique, *op.cit.*, p.16 ; Marcus O'Dair et al., Music On The Blockchain, Blockchain For Creative Industries Research Cluster, Middlesex University, rapport n°1, juill. 2016. Voir aussi : A. Barbet-Massin, V. Dahan, « Les enjeux de la blockchain en droit d'auteur », *op.cit.*, p.21, n°3.

dans la *blockchain* peut être mise en perspective avec la préconstitution d'une preuve classique qui ne permet pas non plus réellement de vérifier la titularité.

520. **La consécration de la signature électronique simple et la charge de la preuve.** La clé privée correspond à une signature électronique simple telle que visée par le règlement eIDAS et ne permet pas l'accès à l'identification mais à « *des données sous forme électronique qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer* »[1130]. Toute transaction réalisée avec une clé publique dans un registre d'une *blockchain* signée par une clé privée pourrait être présumée avoir été effectuée par le titulaire de ladite clé privée jusqu'à preuve du contraire[1131]. La charge de la preuve pèserait sur celui qui conteste de prouver que l'inscriveur n'était pas titulaire de la clé privée. Cette présomption simple est adéquate puisqu'elle doit pouvoir être réfragable compte tenu des phénomènes de vols et pertes de clés[1132]. Elle pourrait cependant mettre en difficulté le titulaire originaire face à un prétendu titulaire qui aurait volé ou récupéré sa clé privée. Dans ce cas, le titulaire originaire devra démontrer qu'il était bien à l'origine le véritable titulaire de la clé privée[1133].

2. L'assentiment à certifier des données dans un registre distribué

521. **Distinction entre consentement et assentiment.** Précisons qu'en inscrivant dans le registre d'une *blockchain*, l'inscriveur ne manifeste pas sa volonté de certifier des données avec une signature électronique simple. Ce n'est pas un consentement car la volonté unilatérale de certifier n'implique pas la rencontre de deux volontés à l'occasion d'une offre et d'une acceptation, c'est un assentiment à inscrire une donnée[1134].

[1130] Règl. eIDAS, art. 3.10.

[1131] Voir en sens à Monaco le projet de loi n°995 relative à la technologie blockchain du 20 mai 2019, art. 3 : « *Toute action réalisée au sein d'un dispositif d'enregistrement numérique sur un registre partagé au moyen d'une clé privée, vérifiée par Ia clé publique correspondante, est présumée l'avoir été par le titulaire de Iadite clé privée jusqu'à preuve contraire* ».

[1132] F. G'sell, « Preuve et signature numérique », *op.cit.*, p.108.

[1133] Voir en sens à monaco l'exposé des motifs du projet de loi n°995 relative à la technologie *blockchain* du 20 mai 2019 : « *il appartient donc à ce titulaire de prouver que cette clé a été volée ou divulguée à un tiers et utilisée aux fins de réaliser une transaction donnée. Le présent projet de loi a ainsi pris le parti de responsabiliser pleinement le détenteur de la clé privée en lui faisant supporter le risque de sa divulgation* ».

[1134] Ici l'unilatéralisme ne remettrait pas en cause le principe selon lequel « *nul ne peut se constituer de preuve à soi-même* » car ce n'est pas un registre établi uniquement pas l'inscriveur puisqu'il est aussi validé par des nœuds. Voir au sujet de l'unilatéralisme en droit de la preuve : Cl. Mouly-Guillemaud, « La sentence "nul ne peut se

3. Les recours contre de l'authentification d'un « *inscriveur* » dans un registre distribué

522. **La procédure de vérification de signature.** Des recours sont à envisager en contestation de l'authentification d'un « *inscriveur* » certifiant être l'auteur de données inscrites dans un registre. La procédure de vérification de signature de l'article 287 du Code de procédure civile permet de dénier la signature qui est attribuée à l'inscriveur. Un acteur de la *blockchain* pourrait aussi déclarer ne pas reconnaître la signature qui est attribuée à son auteur. Pour cela, le juge vérifiera les conditions de validité de la signature visées par l'article 1367 du Code civil[1135].

523. Cette procédure pourra donc être soulevée uniquement en cas d'identification du signataire de la *blockchain*[1136]. Même si les *blockchains* poseront des difficultés sur l'identification du signataire et la possibilité d'invoquer ce recours, lorsque la contestation de l'authentification par la dénégation de signature sera possible, elle sera *a priori* moins problématique que la vérification d'écriture manuscrite en ce que la preuve cryptographique est techniquement beaucoup moins contestable[1137].

524. **La théorie de l'apparence.** En cas d'échec du recours en contestation de signature, il sera toujours possible d'imaginer que le plaideur puisse se prévaloir de la théorie de l'apparence. En effet, ce dernier aurait pu s'engager dans une transaction de la *blockchain* alors que la signataire n'était pas celui qu'il prétendait. Cette théorie jurisprudentielle a été élaborée par les tribunaux français afin justement de protéger le « *tiers abusé* » à un accord qui croyait légitimement que sa contrepartie avait le pouvoir de conclure un tel accord, bien que cela n'était pas le cas[1138].

---

constituer de preuve à soi-même" ou le droit de la preuve à l'épreuve de l'unilatéralisme », RTD civ. 2007, p.253 et s.

[1135] Cass. civ. 1ère, 6 avr. 2016, n°15-10.732, F-D : cette décision rappelle que le juge est tenu de vérifier les conditions de validités de signature. La juridiction de proximité dans le cas d'espèce s'était contentée d'une simple énonciation que la signature avait été identifiée par un procédé fiable garantissant le lien de la signature avec l'acte auquel elle s'attachait dès lors que la demande d'adhésion portait mention de la délivrance de ce document par la plateforme de contractualisation en ligne permettant identification et authentification des signataires. Cela ne suffisait pas car elle n'avait pas vérifié si le procédé de signature électronique en cause procédait d'un dispositif sécurisé de création de signature électronique, ni que la vérification de cette signature reposait sur l'utilisation d'un certificat électronique qualifié.

[1136] Voir *supra* n°347 et s.

[1137] Voir avis de L. Grynbaum sur la fiabilité de la signature électronique qui respecte les exigences, comparée à une signature manuscrite : L. Grynbaum, Fasc. 10 : La preuve littérale, JCl. Civil Code – Art. 1316 à 1316-4, Lexis Nexis, 19 dec. 2011 (maj 7 dec. 2016), n°37.

[1138] A. Benabent, *Droit des obligations*, Lextenso, sept. 2018, n°500.

525. Pour s'appuyer sur la théorie de l'apparence, il conviendra que le plaideur démontre deux conditions cumulatives : une condition objective et subjective[1139]. Premièrement, la condition objective implique que la partie invoquant la théorie de l'apparence ait commis une « *erreur légitime* », c'est-à-dire dire qu'elle ait effectué les vérifications habituelles et nécessaires. Elle doit avoir, en somme, fait preuve de diligence raisonnable pour vérifier que le signataire était habilité à signer la convention. Cette condition peut être prouvée par tout moyen. Elle sera délicate à prouver dans le contexte de la *blockchain*, dans le sens où les participants à une transaction n'ont pas les capacités techniques pour vérifier qu'elles ont mutuellement les pouvoirs pour signer une transaction. Dans une *blockchain* privée ou publique permissionnée, il sera plus aisé de connaître qui a les habilitations pour intégrer des informations dans le registre distribué entre les acteurs.

526. Deuxièmement, la condition subjective exige que la partie qui invoque la théorie de l'apparence agisse de bonne foi : si cette partie connaissait la vérité, elle ne pourra pas bénéficier de la théorie de l'apparence. Il est à noter que la bonne foi est présumée sauf preuve contraire de la part de l'autre partie.

527. D'une manière générale, l'application de la théorie de l'apparence est très circonstanciée et la jurisprudence est assez hétérogène selon les circonstances de chaque cas d'espèce[1140]. Il n'existe pas de jurisprudence pour le moment relative au recours à la théorie de l'apparence dans l'utilisation d'une signature électronique, et encore moins d'une signature par la *blockchain*.

528. **Le délit d'usurpation d'identité numérique.** C'est enfin sur le fondement du droit pénal qu'il pourra être envisagé le délit d'usurpation d'identité numérique, puni d'un an d'emprisonnement et de 15 000 euros d'amende en vertu de l'article 226-4-1 du Code pénal[1141]. Le fait d'employer la clé publique et privée d'un tiers pourra effectivement s'apparenter à de

[1139] *Ibid.*, n°495-498.

[1140] Exemples d'application de la théorie de l'apparence : le signataire de la contrepartie avait un titre qui pouvait laisser croire à l'autre partie que le signataire était dûment habilité, lorsqu'il avait valablement signé des accords antérieurs avec cette même partie (Cass., 1ère civ., 4 mai 2017, n°16-16853) ; le signataire de la contrepartie était auparavant le dirigeant de l'entité qui était partie à l'accord (CA Versailles, 16 mai 2017, n°16/03049). Contre (exemples de refus) : lorsque l'accord indiquait expressément l'entité qui pouvait accepter l'accord et que cette dernière n'avait pas accepté l'accord (Cass. Com, 26 sept. 2018, n°17-15420) ; dans le cadre d'un contrat de bail commercial, la Cour de cassation a conclu que le locataire était tenu de vérifier la procuration du signataire qui était le directeur du locataire (Cass. Com, 19 janv. 2016, n°14-11604).

[1141] Voir une récente condamnation pour usurpation d'identité et cyber-harcèlement à un de prison ferme : TGI de Paris, 14ème ch. corr., jugement correctionnel du 27 juin 2019.

l'usurpation dans l'usage de plusieurs données numériques permettant d'identifier le signataire en vue de troubler sa tranquillité. La clé publique pourrait se rapprocher d'une donnée de nature à identifier autrui et la clé privée à celle permettant de signer une transaction pour ensuite envoyer un ordre. Nous supputons que l'expression « *données permettant d'identifier autrui* » pourrait être interprétée de façon plus large dans un contexte numérique compte tenu des positions adoptées par les juridictions et les autorités de protection des données sur les données indirectement identifiantes[1142].

C. La datation des données enregistrées dans un registre distribué

529. La datation des données enregistrées dans un registre distribué de *blockchain* impose de répondre à deux questionnements : celui de l'opposabilité de la date (1), à savoir quelle date s'imposera parmi celles présentes dans le registre, et celui des contours de l'objet de la date (2).

1. L'opposabilité de la datation du registre distribué

530. **Les deux datations existantes.** La datation des données enregistrées dans le registre d'une *blockchain* intervient à deux moments : lors de l'entrée de la transaction avant sa validation et lors la validation des blocs de transactions.

531. **La date et l'heure de validation des blocs de transactions opposable.** La date la plus pertinente à retenir pour la constitution d'une preuve est celle de la date de validation des transactions dans le registre, dans le sens où un bloc de transactions peut tout à fait se voir rejeter par le validateur du réseau et ne jamais être inscrit dans le registre de la *blockchain*. Il convient de ne pas perdre en mémoire qu'entre le moment de l'entrée de la transaction en attente de validation et sa validation effective, un intervalle de temps peut être plus ou moins espacé. Il peut se passer entre dix minutes et plusieurs heures si le réseau est encombré sur la *blockchain* Bitcoin[1143]. Ajoutons que l'horodatage des blocs peut être décalé d'une à deux heures par rapport aux temps universel coordonné[1144]. Cet effet dilatoire de l'horodatage par la *blockchain*

[1142] Voir *supra* n°303.
[1143] A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder, *Bitcoin and Cryptocurrency Technologies*, *op. cit.*, p.17.
[1144] Voir *supra* n°366.

publique implique une forme de « *preuve à effets différés* ». La datation retenue qui peut être opposable est donc celle des dates et heures de validation des blocs de transactions.

2. Les contours de l'objet de la date des données horodatées dans un registre distribué

532. **La notion de date certaine des données horodatées dans la *blockchain*.** La notion de date et heure doit se voir fixée avec davantage de précisions dans le cadre de l'horodatage *blockchain*. Il est souvent mentionné que l'horodatage par la *blockchain* apporterait une « *date certaine* » des données enregistrées dans le registre[1145], ce qui sera déterminant pour l'opposabilité de cette date aux tiers. Distinguons la date certaine dans le contexte du droit civil et dans celui de la propriété intellectuelle. En droit civil, la date certaine d'un acte sous signature privée est visée limitativement par l'article 1377 du Code civil. Seuls ces trois événements confèrent la certitude de la date à cet acte : le premier, le plus courant, résulte de l'enregistrement, formalité fiscale qui produit des conséquences civiles exceptionnellement, le deuxième est le décès d'une partie, et le troisième est la constatation de l'acte dans un acte authentique. Par exemple, n'ont pas date certaine, le cachet de la Poste ou la légalisation par un commissaire de police. Notons ainsi que la date non certaine d'un acte sous signature privée est inopposable aux tiers alors que l'acte authentique qui a date certaine est en revanche opposable à tous, c'est-à-dire qu'il dispose de l'aptitude permettant de « *forcer les tiers à reconnaître son existence et à se faire respecter* »[1146]. En principe, le formalisme pour acquérir date certaine pour les actes sous signature privée ne peut comporter aucun substitut, la jurisprudence admet cependant un tempérament en reconnaissant l'opposabilité de la date qui n'avait pas acquis date certaine. La simple connaissance de la date véritable d'un acte sous signature privée par un tiers permet de rendre cette date opposable[1147].

[1145] D. Legeais, Fasc. 534 : Blockchain, JCl Commercial, 7 Mars 2017, n°26 ; V. Fauchoux, A. Gouazé, « Pourquoi la blockchain va révolutionner la propriété intellectuelle ? Application pratique au secteur de la mode », Propriétés intellectuelles n°65, oct. 2017, p.24 ; N. Bictin, « Quelle place pour la blockchain en droit français de la propriété intellectuelle », Propriétés intellectuelles n°65, oct. 2017, p.19 ; M. Mekki, « Les mystères de la blockchain », *op.cit.*, p.2162, n°14 ; A. Favreau, « L'avenir de la propriété intellectuelle sur la blockchain », *op.cit.*, p.11.

[1146] R. Wintgen, *Étude critique de la notion d'opposabilité. Les effets du contrat à l'égard des tiers en droit français et allemand*, thèse ss. dir. J. Ghestin, Paris 1, 2002, LGDJ, coll. Bibliothèque de droit privé, t. 426, 2004. Voir aussi la définition de l'opposabilité comme « qualité reconnue à un élément de l'ordre juridique par laquelle il rayonne indirectement hors de son cercle d'activité directe" (J. Duclos, *L'opposabilité : essai d'une théorie générale*, thèse, Rennes, 1981, LGDJ, coll. Bibliothèque de droit privé, 1984, n°2-1, p.22).

[1147] Cass. civ. 3e, 6 janv. 1972, *Bull. civ.* III, no 6 : la Cour de cassation approuve le pourvoi d'avoir dit : « *un acte sous seing privé qui n'a pas acquis date certaine est opposable à des tiers s'il est démontré que ces tiers en ont eu effectivement connaissance* ».

533. Pour le reste, en dehors des cas visés par la loi, l'acte n'a pas de date certaine et n'est donc pas opposable aux tiers. Le défaut de date certaine entraîne l'inopposabilité de la date aux tiers, mais aussi de l'acte. La preuve de la date certaine de l'acte commande ainsi son opposabilité aux tiers[1148]. Cela étant, le principe veut aussi qu'une inopposabilité ne peut être invoquée que par des tiers de bonne foi. Dans le cadre de la *blockchain*, la date conférée par le registre de la *blockchain* pose question car elle ne répond pas aux hypothèses de l'article 1377 du Code civil, sauf à ce qu'un document ancré corresponde lui-même à ces hypothèses. Cela rejoint plus généralement la problématique de savoir si l'horodatage traditionnel peut conférer date certaine en droit civil et devenir opposable aux tiers. La réponse est négative dans le cadre de ces hypothèses[1149], mais dans une perspective plus large, cette réponse suscite une reconsidération.

534. Cette notion de date certaine est aussi employée dans le secteur du droit de la propriété intellectuelle et est transposée à la *blockchain* dans ses usages pour le secteur créatif. La date certaine n'est pas visée littéralement dans le Code de la propriété intellectuelle mais plutôt celle de date de priorité[1150]. La jurisprudence en fait cependant mention[1151], et la pratique admet que cette date certaine soit acquise à l'issue d'une procédure administrative auprès d'un office de propriété intellectuelle dès l'instant où un titre est délivré. Nonobstant ces cas précis développés, l'horodatage hybride s'affranchit de ces hypothèses et exprime une certitude dans sa date étant donné qu'il fait l'usage d'un horodatage distribué[1152]. Cette date de l'horodatage devrait pouvoir être opposable aux tiers à un moment précis.

[1148] J. Ghestin et G. Goubeaux, *Traité de droit civil : introduction générale*, LGDJ, 1983, p.547-548, n°635.

[1149] Voir en ce sens : A. Barbet-Massin, « Le droit de la preuve des œuvres d'art », *op.cit.*, p.15 ; M. Mekki, « *Blockchain*, smart contracts et notariat : servir ou asservir », *op.cit.*, act. 599, p.11 ; M. Julienne, « Pratique notariale et numérique : état des lieux », Dalloz IP/IT n°2, fevr. 2019, p.99-100, n°12 ; M. Mekki, « *Blockchain* et métiers du droit en questions », Dossier « Blockchain et métiers du droit : une force vive ou subversive ? », *op.cit.*, p.86.

[1150] En matière de dessins et modèles dans certaines industries : CPI, art. R511-5 ; R511-6 ; En matière de brevets d'invention : CPI, art. L612-3 ; L612-4 ; L612-21 ; L614-4 ; L614-13 ; L614-15 ; L614-20 ; L614-29.

[1151] Cass. ch. civile, 21 mai 1958, Preuilh c/ Miremont ; Cass. ch. com., 24 juin 2014, n°13-12.067, Société JM Weston c/ Société Capuce ; CA Paris, Pôle 5, 30 juin 2015, n°2014/03937, B (Hassan, Luxembourg) c/ First line SARL ; TGI Paris, 21 janvier 1977, Syndicat national des constructeurs de navires et embarcations de plaisance c/ Gouget ; TGI Paris, 3e chambre, 21 janvier 1998, V (Antoine) et Design volanis c/ PSA Peugeot Citroën (SA) et automobiles Citroën (SA) ; TGI Nanterre, 1ère ch., 17 janvier 2008, n°07/02870, Société Chocoladefabriken Lindt & Sprüngli AG c/ SAS Maison du chocolat ; TGI Paris, Chambre civile 3, 20 mai 2008, n°06/08868, S.A. Poiray france c/ Société Histoire d'or ; TGI Bobigny, 5e ch., 1ère section, 14 septembre 2010, n°09/08983, Société d'exploitation ubu c/ Société ms pretty ; TGI Nanterre, 1ère chambre, 27 octobre 2011, n°09/08069, Société Morganne bello c/ Société By les poulettes ; TGI Nanterre, 1ère ch., 21 février 2013, n°11/09310, Société Lauramé c/ Société Cevimod.

[1152] Voir *supra* n°135 ; n°366 et s.

535. **La date de l'existence des données horodatées dans la *blockchain*.** La date précise qu'il conviendra de retenir pour les inscriptions dans le registre de la *blockchain* est la date de l'existence de ces données. Pour la Maître de conférences Amélie Favreau, il s'agit d'une date de possession en matière de propriété intellectuelle qui est révélée par la technologie *blockchain*[1153]. Nick Szabo le célèbre inventeur du *smart contract* dans un article « *Secure Property Titles with Owner Authority* » invoquait également le fait d'utiliser techniquement des preuves de possession par la *blockchain*[1154]. À la différence de l'existence qui est le simple fait pour une chose d'exister[1155], la possession est le fait de disposer en maître de quelque chose et pouvoir en tirer profit et jouissance[1156]. Lorsque l'inscriveur inscrit dans le registre de la *blockchain*, il réalise une forme d'acte déclaratoire que ce qui est inscrit existe à un instant donné. Il pourrait être question de la date de l'existence d'un acte, d'un contrat, d'un droit (droit de propriété intellectuelle non-enregistré), d'un usage (droit de propriété intellectuelle enregistré), ou d'un fait, comme l'enregistrement d'une chaîne d'évènements dans la *blockchain* correspondant à l'authenticité d'un sac de luxe, à l'origine d'un produit alimentaire, ou encore aux différents stades d'une œuvre collective. Au regard de ces illustrations, c'est bien la date d'existence des données inscrites dans le registre numérique distribué qu'il est opportune de retenir.

536. **La présomption irréfragable de la date d'existence des données horodatées dans la *blockchain*.** Cette date d'existence devrait être présumée irréfragable dans une *blockchain* publique puisqu'elle est d'une véracité particulière[1157]. C'est avec la marge laissée dans l'avis du Parlement européen, qui inclurait une présomption dans le cadre de l'horodatage, que le droit français pourrait accorder une présomption de date de l'existence des données dans le registre d'une *blockchain* publique qu'il ne serait pas possible de renverser. Dans un tel cas, l'assertion selon laquelle les blocs enregistrés dans le registre à une heure et date précises ne peuvent être inter-changés sauf à subir une attaque des 51%, ne pourrait pas être ébranlée. Contrairement à l'« *infirmité* » de l'acte sous signature privée écrit qui pourrait être antidaté ou postdaté[1158], peut-on vraiment discuter de la valeur probante d'une preuve scientifique qui est par définition

[1153] A. Favreau, « L'avenir de la propriété intellectuelle sur la blockchain », *op.cit.*, p.16.
[1154] N. Szabo, « Secure Property Titles with Owner Authority », 1998, https://nakamotoinstitute.org/secure-property-titles/ (consulté le 31/05/2020)
[1155] https://www.cnrtl.fr/definition/existence (consulté le 31/05/2020)
[1156] *Ibid*.
[1157] Voir *supra* n°99 sur la résilience du réseau de *blockchain* publique.
[1158] C. Grimaldi, « L'acte sous-seing privé, l'acte authentique et l'acte contresigné par un avocat : quelle utilité », JCP E n°1, 7 janv. 2010, 2008.

incontestable[1159]. La date d'existence des données horodatées devrait donc en ce sens être toujours irréfragable pour les *blockchains* publiques. La vérité temporelle issue de l'horodatage *blockchain* serait imposée au juge par cette présomption irréfragable. Cette expression légale de normalité exprimerait une probabilité très forte[1160] de la datation par la *blockchain*.

537. En France, l'amendement n°1317 déposé au projet de loi n°1088 PACTE examiné en Commission spéciale a proposé d'introduire une présomption mais de nature simple de l'existence et de date du contenu dans un DEEP à la suite de l'article 1358 du Code civil dans les termes suivants « *... tout fichier numérique enregistré dans un dispositif électronique d'enregistrement partagé (DEEP), de nature publique ou privée vaut preuve de son existence et de sa date, jusqu'à preuve contraire, dès lors que ledit DEEP répond à des conditions définies par décret* »[1161]. Cet amendement a finalement été retiré avant discussion[1162]. Ce retrait marque sans nul doute les réticences quant à l'intégration d'une technologie si nouvelle dans le Code civil.

538. Un projet de loi monégasque relatif à la *blockchain* prévoit lui que « *toute information enregistrée dans un dispositif d'enregistrement numérique sur un registre partagé vaut présomption simple de son existence, de son contenu et de sa date, jusqu'à preuve contraire sous réserve du respect des exigences fixées par ordonnance souveraine* »[1163]. Toujours est-il que l'horodatage *blockchain* concerne une preuve de l'existence à une date d'un contenu et non une preuve du contenu lui-même enregistré dans un registre distribué. La *blockchain* prouve en effet l'existence des données, l'existence du contenu mais elle ne prouve pas la véracité de la donnée, le contenu lui-même. Il convient donc de ne surtout pas retenir une présomption de contenu.

539. En présence de la présomption irréfragable, aucun recours ne sera envisagé en contestation de la date et l'heure des données enregistrées dans le registre de la *blockchain*. La

[1159] R. Houin, « Le progrès de la science et le droit de la preuve », *op.cit.*, p.70.
[1160] J. Dabin, *La technique de l'élaboration du droit positif spécialement en droit privé*, Bruxelles, Bruylant, 1935, n°256, p.292 ; A.-B. Caire, *Relecture du droit des présomptions à la lumière du droit européen des droits de l'homme*, Pedone, coll. publications de l'Institut International des Droits de l'Homme, thèse ss. dir. J.-P. Marguénaud, 2012, p.425 et s. ; J. Rivero, *Fictions et présomptions en droit public français*, *in* C. Perelman, P. Foriers (ss. dir.), Bruxelles, Bruylant, 1974, p.107 et s. ; M. Mekki, « Vérité et preuve. Rapport français », *op.cit.*, p.818, n°11.
[1161] Voir annexe n°7 l'amendement n°1317 et l'amendement identique CL380.
[1162] http://www.assemblee-nationale.fr/dyn/15/amendements/1088/CSPACTE/1317 (consulté le 31/05/2020).
[1163] Projet de loi n°995 relative à la technologie blockchain du 20 mai 2019, art. 2. Voir annexe n°4.

présomption irréfragable de date certaine de l'existence des données dans la *blockchain* sera effectivement un instrument axiologique, c'est-à-dire au service d'une politique substantielle de promotion des propriétés cryptographiques de cette technologie[1164].

Paragraphe 2 : De la réflexion sur des mesures de *soft law* sur les preuves de données enregistrées dans la *blockchain*

540. La *soft law* s'éloigne de la conception hiérarchique verticale et monolithique du droit[1165], propice à appréhender l'horizontalité et la décentralisation de la *blockchain*. Les normes de *soft law* sont difficilement contestables[1166] car elles sont rarement contraignantes. Dans certains cas, le respect des instruments non contraignants est extrêmement efficace et n'aurait probablement pas été profitable si les normes étaient contenues dans un texte contraignant[1167].

541. Deux modèles sont à envisager pour sécuriser l'usage de la technologie *blockchain*, un premier modèle à intervention étatique minimale sous la forme d'une certification des produits et services d'une *blockchain*, voire des protocoles eux-mêmes (A)[1168]. Cette certification sous forme de labellisation implique une logique d'encouragement et d'accompagnement des autorités publiques attribuant le label avec cette triple fonction « *d'identifier, distinguer, valoriser* »[1169]. Il sera cependant exclu la possibilité d'une auto-certification selon une démarche auto-déclarative pour les acteurs privés eux-mêmes. Cette démarche où l'acteur garantit respecter certains engagements qu'il s'est lui-même imposé semble vaine et peu efficace. Nous prêtons classiquement à la puissance publique le bénéfice d'une présomption d'objectivité qui n'est pas accordée aux acteurs privés. Il est peu raisonnable de penser qu'une information pleinement transparente avec une garantie d'objectivité soit accordée par une

[1164] M. Mekki, « Regards substantiel sur le « risque de la preuve ». Essai sur la notion de charge probatoire », *in La preuve : regards croisés*, *op.cit.*, p.21 ; P.Deumier, *Introduction générale au droit*, 2e éd., LGDJ, 2013, n°91, p.82.
[1165] A. Flückiger « Pourquoi respectons-nous la *soft law* ? », Revue européenne des sciences sociales XLVII-144, OpenEdition, 2009, p.74, n°3.
[1166] S. Dinah, *Commitment and Compliance : The Role of Non-Binding Norms in the International Legal System*, Oxford 2000.
[1167] D. L. Shelton, *Soft law*, *Handbook of International Law*, Routledge Press, 2008, p.20.
[1168] A. Barbet-Massin, « Le droit de la preuve des œuvres d'art », *op.cit.*, p.16.
[1169] J.-M. Pontier, « La politique de labellisation », AJDA 30/2017, sept. 2017, p.1705.

personne privée partie prenante dans les bénéfices des ventes escomptés d'un produit ou un service labellisé. La certification publique inspire une confiance plus généreuse. Les labels privés sont quant à eux trop nombreux et leur délivrance est bien trop opaque, faisant naître des réserves. Il sera donc question ici de proposer l'intervention d'un label attribué exclusivement par une personne publique pour consolider la poursuite d'un intérêt public, général de protection des utilisateurs et acheteurs des produits et services liés à la technologie *blockchain*.

542. Un second modèle serait celui sans aucune intervention d'État, qui supposerait que le marché des acteurs distribuant des solutions basées sur la technologie *blockchain* s'autorégule (mais ne s'auto-certifie pas) par des guides pratiques, des chartes (B).

A. Un modèle de certification sous forme de labellisation « *optionnelle* »

543. Le modèle de certification par la labellisation « *optionnelle* » correspond tout à fait à une application très concrète dans le secteur des nouvelles technologies, à l'image de la labellisation délivrée par la CNIL concernant la conformité des produits et procédures quant au traitement de données à caractère personnel. Celle-ci est optionnelle car la certification est dite « *volontaire* », elle ne pourra impliquer de contraindre les acteurs à se soumettre à cette référence. Cette labélisation renvoie à une « *certification* »[1170] correspondant à une activité de contrôle de respect de la conformité d'un produit, d'un service ou d'une personne à un référentiel, lequel est constitué de norme technique comportant des exigences et préconisations. Ces exigences soumettent les produits ou services à des appréciations techniques de la technologie ce qui appelle à une harmonisation des interprétations des standards tant les protocoles de la *blockchain* sont divers. La certification fait intervenir aussi l'homologation. L'homologation de l'administration est appropriée dans une technologie très innovante à risques potentiels. C'est une forme d'approbation ou d'accord à la demande qui lui est faite par une autorité ou un organe compétent sur un produit ou un service par rapport à des spécifications préétablies[1171]. En substance, la certification est une procédure par laquelle un organisme accrédité et un organisme certificateur indépendant attestent qu'un produit ou un service est conforme à des caractéristiques décrites par un référentiel de certification, constitué

[1170] Le terme certification ici employé est à distinguer de la certification permise par la technologie *blockchain* susvisée *supra* n°500 et s.
[1171] J.-M. Pontier, « La politique de labellisation », *op.cit.*, p.1702.

généralement par une norme technique[1172]. Le critère matériel de la certification d'un produit ou service liés à la *blockchain* (1) sera présenté d'une part, et son critère organique sera traité, d'autre part (2).

1. Le critère matériel de la certification

544. **Objet du label.** L'objet même de la certification permettrait d'attester la conformité d'un produit ou service lié à la *blockchain,* voire d'allier les caractéristiques de produits (normes techniques d'un protocole, par exemple) et de services (normes relatives aux modalités de la maintenance d'un logiciel applicatif, par exemple), de « *type mixte* »[1173].

545. **Une labellisation des protocoles et des algorithmes.** Ce label serait intéressant pour les protocoles de la *blockchain* dans l'objectif par exemple d'attester la fiabilité auprès d'un juge quant à l'intangibilité des données inscrites dans une *blockchain*. Pour le Ministère de la Justice, il convient de sécuriser la preuve *blockchain* en établissant cette forme de « *certification* » des protocoles[1174]. Cette fiabilité inclurait la validation de la fiabilité du réseau en lui-même ainsi que les détails des algorithmes utilisés : la fiabilité des algorithmes utilisés par la signature *blockchain,* les fonctions de hachage et les algorithmes de consensus. Bien que ces algorithmes soient étudiés par des mathématiciens, des chercheurs en informatique, des cryptographes et des experts techniques et parfois approuvés, une approbation de référence serait appropriée. Le rapport Toledano émet une recommandation dans le sens de cette reconnaissance des algorithmes pour la signature[1175].

546. **Une labellisation « *en une fois* ».** La labellisation ne doit pas nécessiter de faire intervenir dans le déploiement de chaque service une procédure contraignante, à l'instar des fournisseurs de solution de signature électronique qualifiée qui sont agréés non pas pour une prestation de signature fournie à un client mais pour chaque signature. Cela ne reviendrait finalement pas à introduire un tiers de confiance « *nocif* » pour la *blockchain* car la certification s'introduirait à l'origine une seule fois pour certifier les protocoles. Il conviendrait bien entendu

[1172] F. Lagarde, « règlementation, normalisation, certification, labellisation… : élément de définition », Jurisport n°188, juill./août 2018, p.19
[1173] T. Dumortier, « La certification au service de l'administration : essai de typologie et enjeux juridiques », RDP, nov. 2012, p.1614.
[1174] Assemblée nationale, Rapport d'information n°1501, *op.cit.*, p.92.
[1175] F. G'sell, « Preuve et signature numérique », *op.cit.*, p.109.

d'établir une durée de validité courte dans le temps du label pour faire face aux évolutions rapides de ces protocoles de *blockchain*, par exemple, une durée limitée à une année. Si le produit ou service n'est plus conforme au référentiel fixé, il pourrait être retiré par l'organe certificateur.

547. **Élaboration du référentiel.** La certification intervient en principe sur la base d'une comparaison à un référentiel élaboré par une personne privée (l'association française de normalisation pour établir une norme ISO par exemple) ou une autorité publique (label Marianne par exemple). C'est un document technique définissant les caractéristiques que doit présenter un produit, un service, et les modalités de contrôle de la conformité à ces caractéristiques[1176]. Les professeurs en sciences économiques Paola Tasca et informatiques Claudio J. Tessone prônent la nécessité d' « *établir des architectures standardisées pour cartographier le domaine et promouvoir la coordination de la recherche et du développement d'initiatives* »[1177]. À cette fin, le rapport De la Raudière/Mis vise de façon large toutes les initiatives tendant à favoriser l'établissement de standards européens ou internationaux pour le fonctionnement des *blockchains*[1178]. Alors que l'*EU Blockchain Observatory and Forum* recommande spécifiquement la nécessité d'élaboration de normes pour les identités numériques dans le cadre de la *blockchain* et pour l'interopérabilité entre *blockchains* par exemple[1179].

548. **Le rejet de l'élaboration d'un référentiel par une personne privée (ou normalisation).** Ces normes techniques sont établies, pour la majeure partie, par des personnes privées[1180]. Cette forme d'élaboration de normes se nomme souvent « *normalisation* »[1181]. La normalisation des produits et services de la *blockchain* est recommandée par une partie de la doctrine[1182] et le Parlement européen. La résolution du Parlement européen du 3 octobre 2018

[1176] C. conso., art. L433-3.
[1177] P.Tasca, Claudio J. Tessone, « Taxonomy of *Blockchain* Technologies. Principles of Identification and Classification », *op.cit.*, p.8.
[1178] Rapport d'information n°1501, *op.cit.*, p.92.
[1179] EU Blockchain Observatory and Forum, Scalability interoperability and sustainability of blockchains, *op.cit.*, p.20.
[1180] A. Penneau et D. Voinot, fasc. 970, Normalisation, JCl. Concurrence - Consommation, Lexis Nexis, oct. 2010.
[1181] C'est une démarche d'encadrement technique qui est selon le décret du 16 juin 2009 relatif à la normalisation « *une activité d'intérêt général qui a pour objet de fournir des documents de référence élaborés de manière consensuelle par toutes les parties intéressées, portant sur des règles, des caractéristiques, des recommandations ou des exemples de bonnes pratiques, relatives à des produits, à des services, à des méthodes, à des processus ou à des organisations. Elle vise à encourager le développement économique et l'innovation tout en prenant en compte des objectifs de développement durable* » (Décret n°2009-697 du 16 juin 2009 relatif à la normalisation, art. 1).
[1182] F. Jault-Seseke, « La blockchain au prisme du droit international privé, quelques remarques », *op.cit.*, p.545 ; T. Douville, « *blockchains* et preuve », *op.cit.*, p.2194.

sur la *blockchain* exprime au point 42 « *qu'il importe d'adopter une approche globale de la normalisation, pour que les entreprises innovatrices ne soient pas exclues par la réglementation de l'Union européenne* »[1183]. Cette normalisation, activité d'élaboration de normes volontaires de références, c'est-à-dire des spécifications ou des référentiels techniques, est adoptée par des organismes privés, instances de normalisation au plan international, européen, ou national, à l'instar de l'Organisation internationale de normalisation (ISO), du Comité européen de normalisation (CEN), ou de l'association française de normalisation (AFNOR). Par exemple, dans le but d'élaborer des normes sur la signature électronique, c'est le Comité sur les signatures électroniques de la Commission européenne qui a financé des organismes européens de normalisation, le CEN et l'Institut européen des normes de télécommunication (ETSI), pour établir l'*European Electronic Signature Standardisation Initiative*. La normalisation est destinée à garantir la confiance entre les acteurs économiques d'un côté et les consommateurs de l'autre. À l'échelle nationale, de nombreuses entreprises adhèrent à l'AFNOR, qui est une association d'utilité publique sous la tutelle du Ministère chargé de l'industrie.

549. Une trentaine d'acteurs privés et publics seulement travaillent déjà à l'établissement de normes techniques prévues par l'ISO dans le cadre du TC307 *Blockchain and electronic distribued ledger technologies*[1184]. L'objectif de l'ISO TC307 est d'établir une terminologie et un vocabulaire commun dans le secteur de la *blockchain*, une architecture de référence compte tenu de la multiplication des implémentations des protocoles *blockchains*, de classifier les cas d'usage, de sécuriser et rendre confidentielles les données personnelles, de gérer des identités et les contrats intelligents[1185]. Le Parlement européen dans le point 41 de sa résolution du 3 octobre 2018 se félicite « *des initiatives d'organisations telles que l'ISO pour l'établissement de normes pour les TRD; (et) invite la Commission à poursuivre sa collaboration avec d'autres organisations internationales pour les travaux de normalisation* »[1186].

[1183] Parlement européen, Résolution du 3 oct. 2018 sur les technologies des registres distribués et les chaînes de blocs: renforcer la confiance par la désintermédiation (2017/2772(RSP)), P8_TA(2018)0373.
[1184] Sur demande de son membre Australien, l'ISO a créé un nouveau comité technique sur la *blockchain* en septembre 2016 : https://www.iso.org/committee/6266604.html (consulté le 31/05/2020). Voir : O. Peyrat, J.-F. Legendre, « Pourquoi la normalisation s'intéresse-t-elle à la *blockchain* ? », Annales des Mines - Réalités industrielles, août 2017, p.97.
[1185] O. Peyrat, J.-F. Legendre, « Pourquoi la normalisation s'intéresse-t-elle à la blockchain ? », *op.cit.*, p.97.
[1186] Parlement européen, Résolution du 3 oct. 2018 sur les technologies des registres distribués et les chaînes de blocs: renforcer la confiance par la désintermédiation (2017/2772(RSP)), P8_TA(2018)0373.

550. La présence de chaque pays dans ces instances internationales de rédaction de normes est primordiale pour conserver une certaine souveraineté et prévenir suffisamment pour éviter de se voir imposer des normes. Caroline de Condé, la responsable de la Commission de normalisation *blockchain* de l'AFNOR en France explique qu' « *il est particulièrement important que la France soit positionnée dans ces comités internationaux, notamment pour que, par la suite, elle ne se voit pas imposer des standards qui rendraient les acteurs français moins compétitifs* »[1187].

551. À l'échelle européenne, un groupe de discussion baptisé *EU Focus Group on blockchain* a été établi sous l'égide de la CEN[1188]. Un comité technique européen devrait alors être en cours de création. Ce dernier proposera certainement des solutions quant aux différents points de frottement entre les éléments techniques de la *blockchain* et le règlement européen eIDAS et le RGPD.

552. En France, l'AFNOR a établi sa propre commission comptant 29 membres, parmi lesquels des prestataires, des intermédiaires, des acteurs assurant le support technique, un usager, un évaluateur, et un acteur public sont présents[1189]. Cette commission couvrirait le même domaine d'activité que l'ISO/TC 307. Elle se charge de déterminer une terminologie technique et juridique, une taxonomie, et une architecture technique.

553. Cette norme est privée et d'accès payant[1190], même si la nature juridique de la norme homologuée AFNOR est administrative[1191]. L'AFNOR pourrait cependant associer les pouvoirs publics à plusieurs niveaux dans l'élaboration des normes si un projet de normes était initié par l'intermédiaire de représentants de l'administration siégeant dans les comités techniques d'élaboration de ces normes.

554. L'établissement de ces référentiels internationaux, européens et français par des personnes privées est largement soutenu par le Parlement européen qui dans le point 38 de sa

---

[1187] G. Marraud des Grottes, « Preuve blockchain : et si la soft law était une première étape ? », Wolters Kluwer, Actualités du droit, 6 dec. 2019, p.3.
[1188] https://www.cencenelec.eu/news/articles/Pages/AR-2018-04.aspx (consulté le 31/05/2020).
[1189] https://norminfo.afnor.org/structure/afnorcn-*blockchain*/commission-de-normalisation-blockchain/123293 (consulté le 31/05/2020).
[1190] A. Penneau, « Normalisation. 3 questions : l'accessibilité aux documents AFNOR en question », JCP E n°18, n°320, 4 mai 2017, p.5. Une jurisprudence du Conseil d'État oblige les consultations gratuites sur le site Internet de l'AFNOR pour les normes dont l'application est rendue obligatoire (CE, 28 juill. 2017, n°402751, inédit).
[1191] CE, 10ème et 3ème sous sect., 17 févr 1992, Textron, req. 73230 ; CE, 9ème et 10ème sous-sect., 8 mars 2002, SARL Plettac Echafaudages, req. 210043.

résolution du 3 octobre 2018 « *demande à la Commission de promouvoir le développement de normes techniques avec les organisations internationales concernées, telles qu'ISO, UIT et CEN-CENELEC, et de procéder à une analyse approfondie du cadre juridique existant dans les différents États membres en ce qui concerne la force exécutoire des contrats intelligents* »[1192].

555. **La préconisation de l'élaboration d'un référentiel par une personne publique par une charte.** Bien qu'une multitude de voies pour l'élaboration de normes soit possible, l'auteur du référentiel devra plutôt être public, que privé, sous la forme d'une « *charte* », afin d'éviter l'écueil d'une mainmise trop hâtive par les fournisseurs de technologie sur un référentiel. L'ISO précise que « *l'élaboration d'une norme s'apparente à l'exécution d'une symphonie où chacun est appelé à jouer sa partition* »[1193] mais cette symphonie pourrait rapidement virer à la mélodie « *atonale* » et « *dissonante* » si certains acteurs privés établissent des normes tournées autours des protocoles *blockchains* les plus développés dans l'unique dessein de servir leurs activités.

556. Par ailleurs, trois techniques sont utilisées par les autorités publiques pour l'usage de ces normes : une référence directe ou référence globale aux normes en vigueur qui consiste à indiquer que le produit ou service doivent être conformes aux normes en vigueur, une référence avec identification glissante qui renvoie à une norme, sans pour autant mentionner la référence de la dernière norme homologuée, et une référence avec identification complète de la norme qui désigne précisément la norme, sa référence et son année d'homologation généralement par un arrêté qui fixe ces exigences techniques[1194]. L'objectif dans le cadre du référentiel des protocoles *blockchains* et des services est de conférer un caractère symbolique au référentiel, qu'il soit un outil extra-juridique utilisé comme un instrument d'attestation.

2. Le critère organique de la certification

557. Dans le processus de certification de produits et services liés à la technologique *blockchain*, il convient qu'un organisme « *(…) distinct du fabricant, de l'importateur, du*

[1192] Parlement européen, Résolution du 3 oct. 2018 sur les technologies des registres distribués et les chaînes de blocs: renforcer la confiance par la désintermédiation (2017/2772(RSP)), P8_TA(2018)0373.
[1193] https://www.iso.org/fr/standards.html (consulté le 31/05/2020)
[1194] F. Aubry-Caillaud, F., Fasc. 560 : normes techniques et certifications, JCl. Europe Traité, Lexis Nexis, avr. 2018, p.6, n°17.

vendeur, du prestataire ou du client, atteste qu'un produit, un service ou une combinaison de produits et de services est conforme à des caractéristiques décrites dans un référentiel de certification »[1195]. Cet organisme certificateur impliquerait l'intervention d'une personne publique ou une personne privée indépendante qui aurait reçu une délégation par l'État et qui est accréditée et contrôlée par le comité français d'accréditation (COFRAC).

558. L'ANSSI, autorité nationale en matière de sécurité et de défense des systèmes d'information, semble la plus compétente pour certifier des produits et services liés à la technologie *blockchain*. La labellisation serait alors une forme « *d'étiquetage valorisé* »[1196] par l'ANSSI censée attester la conformité aux produits et services d'exigences pré-établies. Elle serait par ailleurs un indicateur pour les justiciables, les acteurs de marché et les juges[1197]. Dans le cadre de la certification de sécurité des produits et services délivrés sous son auspice, l'ANSSI fait tout de même appel à un laboratoire privé agréé par elle, nommé le Centre d'Évaluation de la Sécurité des Technologies de l'Information (CESTI). Seule l'évaluation technique des produits et services est prise en charge et est menée par ce laboratoire. C'est donc un prestataire qui est habilité à intervenir dans le processus de certification. L'ANSSI organe certificateur des produits et services de la *blockchain* est public mais pourrait donc faire appel à un prestataire pour procéder à l'évaluation technique des produits et services. Ce prestataire serait toutefois garant de fournir indépendance et intégrité dans ses missions, d'attester d'un certain niveau d'expertises techniques de connaissance des protocoles, et de justifier d'une capacité matérielle à les évaluer. Enfin, il conviendrait de mettre en place un système de reconnaissance de la certification à l'étranger et de mise en relation entre les différents prestataires de confiance des divers pays pour maintenir une uniformité dans la certification.

559. L'entité certifiée serait essentiellement des personnes privées, comme des consultants, des prestataires, des fournisseurs de technologie, ou encore des sociétés de projet qui déploient des protocoles publics ou privés de *blockchain*. En définitive, ce label est surtout un moyen de sécurisation, notamment de prévention contre les usages illicites, pour le consommateur et les entreprises qui souhaitent faire appel à un produit protocolaire de la *blockchain* ou un service de solution *blockchain*.

[1195] C. conso., art. L433-3.
[1196] J.-M. Pontier, « La politique de labellisation », *op.cit.*, p.1700.
[1197] Voir *infra* n°632 en partie 2.

560. En somme, ce label apparaît sous forme de « *bénédiction laïque* »[1198] garant de la qualité d'un produit ou service lié à la technologie *blockchain*. Le label repose sur une adhésion volontaire mais il pourrait devenir subrepticement une contrainte s'érigeant en prétexte d'entrave à des projets informatiques. Ce risque doit être considéré. Il pourrait être à terme discriminant pour les produits et services, projets *blockchains* non labélisés ayant pourtant les mêmes caractéristiques. La labellisation n'a de sens que si elle est accompagnée d'une légitimation de l'État par ses citoyens conduisant à une acceptation de ses activités de labellisation. La remise en question de cette légitimation par les idéologies *cypherpunks* et autres crises sociales actuelles peuvent constituer des limites à la réussite de ces labels. Dans un contexte où le label ne parviendrait pas à construire un régime efficace de certification, il conviendra d'envisager une seconde option de lignes directrices sans intervention étatiste directe.

B. Les lignes directrices sans intervention étatique directe

561. Si l'on considère que l'intervention direct des États dans la mise en œuvre de la reconnaissance de la qualité des protocoles et des prestations est à proscrire, tant d'un point de vue de sa maturité, que de ses développements à venir, cela implique de proposer une boîte à outils composée de guides nationaux de bonnes pratiques par l'ANSSI (1), mais aussi par la participation et le soutien des guides et initiatives des communautés de développeurs liées à ces projets d'élaboration de protocole (2). Il se révèle d'ailleurs nécessaire pour ces deux groupes de travailler de concert sur ces guides afin de s'accorder et fournir des lignes directrices de référence proches des réalités du secteur.

1. Les guides de bonnes pratiques relatives à la sécurité de l'ANSSI

562. Un guide de bonnes pratiques à adopter dans la constitution d'un protocole et l'établissement d'une solution informatique de *blockchain* pourrait avoir un intérêt certain. Ce guide devrait avoir dans un premier temps une portée nationale pour toucher les projets français et trouver à s'appliquer au plus grand nombre d'acteurs et ce de façon uniforme. Alors que

[1198] J.-M. Pontier, « La politique de labellisation », *op.cit.*, p.1706.

l'ANSSI a actuellement une position de retrait face à la technologie *blockchain*[1199], un guide publié par cette agence prend tout son sens et pourrait avoir son importance en pratique[1200]. Il a été fortement soutenu dans la recommandation n°3 du rapport Toledano qui précise qu'il convient d'impliquer l'ANSSI de manière à faire apparaître de bonnes pratiques concernant « *l'offre blockchain* » actuellement développée par des tiers[1201]. L'ANSSI sensibilise déjà les entreprises et administrations aux bonnes pratiques en matière de sécurité appliquées à des thèmes du plus général au plus sectoriel[1202].

563. Il pourrait s'agir de recommandations relatives au choix du consensus en lui-même pour ne pas compromettre le registre, à la résilience du réseau, à une veille sur l'attaque des 51% (et les autres), à la vérification de la scalabilité, à la vérification des vulnérabilités et risques de l'environnement (applications, interfaces, ou encore objets connectés) en dehors même de la *blockchain*. Les risques généraux de sécurité en matière de *blockchain* sont par ailleurs détaillés par l'ISO mais sont similaires à d'autres systèmes d'information. Ils traitent de la mauvaise gestion de l'information, notamment l'altération, la suppression, la destruction non autorisée et la divulgation, la vulnérabilité de mise en œuvre, incluant les mécanismes cryptographiques ou encore des fuites d'informations au moment de l'exécution, de la mauvaise gestion des mécanismes cryptographiques, y compris l'utilisation d'algorithmes faibles, et de la mauvaise gestion des privilèges de l'utilisateur. L'ISO évoque aussi des risques spécifiques en fonction de chaque *blockchain,* notamment au niveau du contrôle d'accès aux comptes[1203].

2. Les guides de bonnes pratiques et référentiels opérationnels de développeurs

564. Les développeurs dans le secteur de la *blockchain* sont au-devant de la scène, mettant souvent en œuvre des solutions inventives, parfois en langage de code nouveau pour la création de protocole ou de logiciel. Ces développeurs ont du reste progressivement établi des librairies de codes et des briques technologiques réutilisables. Inspirés d'un ensemble de ressources

[1199] Rapport de la mission interministérielle sur les verrous technologiques des *blockchains,* Task Force *Blockchain,* 10 fevr. 2020, p.16.
[1200] A. Barbet-Massin, « Le droit de la preuve des œuvres d'art », *op.cit.*, p.16 ; A. Barbet-Massin, « Réflexions autour de la reconnaissance juridique de l'horodatage *blockchain* par le législateur italien », RLDI n°157, mars 2019, p.43.
[1201] F. G'sell, « Preuve et signature numérique », *op.cit.*, p.109.
[1202] https://www.ssi.gouv.fr/administration/bonnes-pratiques/ (consulté le 31/05/2020).
[1203] ISO TC307/WG2, Rapport technique « Distributed Ledger Technology: Security and Privacy », Annexe E.

disponibles en open source, ces véritables auteurs-compositeurs de codes dans la *blockchain* ne sont pas à l'abri d'une erreur glissée dans le code risquant ainsi un certain nombre d'événements malencontreux.

565. Des standards techniques open sources sont très empruntés sur certains protocoles, comme l'ERC (*Ethereum Request for Comment*) pour le protocole Ethereum. Ce dernier est établi par des développeurs dans le but de fournir aux autres développeurs des conseils techniques dans la construction du code[1204]. Parallèlement, de nouvelles propositions de normes ERC peuvent être soumises à la communauté Ethereum par une *Ethereum Improvement Proposal* (EPI)[1205].

566. Certains langages possèdent déjà des guides complets de codage, par exemple JavaScript. Développer une forme de « *kit* » intra-développeurs dans le domaine de la *blockchain* est une boîte à outils qui se relève nécessaire pour des solutions pérennes liées à la *blockchain*, notamment pour faire un choix dans ses outils de travail, préparer son développement, gérer son code source, sa bibliothèque et le SDK (*Software development kit*) ou le kit de développement en français, renforcer la qualité du code (sur les *smart contracts)*, pour éviter les bugs, documenter le code et l'architecture[1206]. En principe, en matière de code écrit pour développer des *blockchains*, il convient de remplir un certain nombre de principes préconisés par le CNRS : être facile à lire, avoir une organisation logique, être explicite pour montrer son intention, et être robuste au regard du temps[1207]. Même si le label aboutit, ces guides peuvent tout à fait venir en complément pour justement aider à l'obtention du label et véhiculer des lignes directrices.

567. **Conclusion du chapitre 2.** En conclusion de ce deuxième chapitre, le cadre général sur les preuves de données enregistrées dans la *blockchain* doit être mûrement réfléchi pour être complété par le législateur et les institutions.

568. Avec une impulsion internationale nécessaire et adaptée à la physionomie des preuves *blockchains*, de grands principes spécifiques par une loi type de la CNUDCI devront être

[1204] https://docs.ethhub.io/built-on-ethereum/erc-token-standards/what-are-erc-tokens/ (consulté le 31/05/2020).
[1205] *Ibid*.
[1206] CNIL, Guide rgpd du developpeur, 28 janv. 2020, https://www.cnil.fr/fr/la-cnil-publie-un-guide-rgpd-pour-les-developpeurs (consulte le 31/05/2020).
[1207] CNRS, Cours de P.-A. Champin, Voir Bonnes pratiques de programmation, https://perso.liris.cnrs.fr/pierre-antoine.champin/enseignement/algo/cours/algo/bonnes_pratiques.html (consulté le 31/05/2020).

consacrés. Cette loi type porterait sur la valeur juridique des données enregistrées, la non-discrimination de ces données, la fiabilité et la sécurité du registre distribué, ainsi que l'éthique dans la technologie de registres distribués. Cette loi devra être accompagnée d'une politique globale de l'OCDE plus soutenue permettant de guider les États dans leur transformation technologique par la *blockchain* ; d'établir les priorités nationales pour les États en matière de *blockchain* ; de rédiger une charte éthique pour les acteurs de la *blockchain*, les entreprises, et les États ; de surveiller les risques d'utilisations abusives et soutenir les usages éthiques de la *blockchain* ; de soutenir l'expérimentation de projet de solutions basées sur la technologie *blockchain* ; de soutenir la recherche sur l'évolution des protocoles *blockchains* ; d'étendre le champ des experts de l'OCDE aux développeurs travaillant sur les protocoles *blockchain* depuis l'origine ; d'échanger et connaître la complexité des protocoles déployés par certaines entreprises et institutions ; de soutenir les entreprises et institutions souhaitant transformer leurs modèles grâce à cette technologie.

569. Le droit français devrait pouvoir transposer avec souplesse ces principes en retenant dans une *lex blockchain* les particularismes de preuves *blockchains* en trois axes : sur la certification des données inscrites dans un registre distribué, l'authentification de l'inscriveur dans un registre distribué et la datation de données enregistrées dans un registre distribué. Comme la prudence le commande dans l'innovation, un label optionnel délivré par l'ANSSI permettrait d'attester la conformité d'un produit ou service lié à la *blockchain* par rapport à un référentiel extra-juridique élaboré par une personne publique. Également, des guides de bonnes pratiques de l'ANSSI, comme des développeurs ainsi que leurs référentiels (notamment le référentiel ERC pour Ethereum) seront de nature à faire évoluer graduellement et qualitativement les projets relatifs à la *blockchain* incluant ces preuves.

570. **Conclusion du titre 2.** En synthèse de ce titre 2, notre législateur français, véritable précurseur dans la consécration de régimes spéciaux expérimentaux, ne saurait se réduire à ces avancées sur les minibons et les titres financiers non cotés, bien que symboliquement significatives en matière de preuves *blockchains*. Les apports de l'ordonnance minibon pour l'essentiel sont inédits. Mais force est d'admettre que ces régimes spéciaux du DEEP sont incomplets et circonscrits à un domaine très particulier.

571. Les preuves *blockchains* doivent être appréhendées, non par de seuls éloges panégyriques nationaux, mais par des organisations internationales pour border son encadrement de concert avec des politiques publiques et des principes internationaux.

572. Par la réception de ces principes, le droit français pourrait trouver des remèdes dans un régime général souple de labellisation optionnel et de *hard law*, car les normes utiles de *soft law* restent de « *juridicité atténuée* » et en partie privées[1208]. En France, le législateur tarde à donner la sécurité probatoire nécessaire à l'usage de cette technologie constituant une forme « *d'atrophie probatoire* » contrairement aux droits étrangers, notamment aux États Nord-Américains. Comme l'expérience l'a montré, il est à craindre une perte de souveraineté proche et l'appropriation des protocoles par des systèmes juridiques étrangers, à l'instar de la genèse des protocoles Internet.

[1208] G. Feuer, H. Cassan, *Droit international du développement*, Precis Dalloz, 1985, 644 p.Voir aussi : F. Chatzistavrou, **«** L'usage du soft law dans le système juridique international et ses implications sémantiques et pratiques sur la notion de règle de droit », *op.cit.*, p.5, n°21.

CONCLUSION DE LA PARTIE 1

573. Pour conclure la partie 1, il n'y aurait pas de contradiction ontologique à donner plus de force aux preuves *blockchains* faisant naître une vérité cryptographique dans notre droit pour davantage de sécurité dans l'usage de celles-ci : l'adage « *Code is law* » se transformerait ainsi en « *Code with law is security* »[1209]. La possible convergence de la pensée libertarienne et du droit sert et soutient la reconnaissance de la vérité cryptographique.

574. Pour transposer juridiquement cette vérité, notre droit commun de la preuve a montré sa constance et sa modernité à faire correspondre des règles anciennes aux mécanismes nouveaux et iconoclastes des preuves *blockchains* permettant leurs qualifications. Nous ne prônons pas, dans ce contexte, d'ajustement ou de reformulation du Code civil. Seule une proposition d'avis de droit dérivé adopté par le Parlement européen serait de nature à clarifier l'assimilation de la signature et l'horodatage *blockchain* à la signature et l'horodatage électronique simple conçu par le règlement eIDAS. Qui plus est, au renfort de l'horodatage *blockchain* perçu comme particulièrement fiable techniquement, nous suggérons la proposition d'une présomption de fiabilité de la date et de l'heure des blocs de transactions et d'intégrité de ces données.

575. Avant que ces règles ne s'étiolent et deviennent insuffisantes, un régime général des preuves *blockchains* doit en outre être construit conformément à l'architecture internationale et décentralisée de cette technologie. Notre temps est ainsi à la réflexion en vue de cette construction. Les régimes spéciaux nationaux des preuves *blockchains* sur les minibons et les titres financiers non cotés pourront coexister avec ce dernier. Des principes internationaux seront établis dans une loi type de la CNUDCI et reçus en droit national par un régime dual souple : une *lex blockchain* et une labellisation optionnelle des produits et services de la *blockchain*. L'ensemble de ces propositions pourront ainsi participer au cadre requis au soutien de la traduction de la vérité cryptographique issue des preuves *blockchains*.

[1209] A. Barbet-Massin, « Réflexions autour de la reconnaissance juridique de l'horodatage blockchain par le législateur italien », *op.cit.*, p.43.

576. Si la vérité cryptographique est particulièrement forte quant à la date qu'elle produit et l'intégrité des données qu'elle prouve, ce qui peut être perçu par notre droit, elle reste toutefois dépendante des juges et des auxiliaires de justice dans la véracité de son contenu, comme de son interprétation.

577. Portalis dans son discours préliminaire au premier projet de Code civil mentionnait que « *la science du législateur consiste à trouver les principes les plus favorables au bien commun : la science du magistrat est de mettre ces principes en action, de les ramifier, de les étendre, par une application sage et raisonnée, aux hypothèses privées (…)* »[1210]. Toute décision d'un juge au sujet des preuves *blockchains* sera l'application d'une loi à des faits donnés, une situation spécifique. Cette vision légicentriste qui vise à considérer que les juges « *ne sont que la bouche qui prononce les paroles de la loi, des êtres inanimés qui n'en peuvent modérer ni la force, ni la vigueur* »[1211] n'est plus, depuis longtemps, conforme aux réalités de l'état du droit.

578. Cette vision que le juge est une simple « *bouche de la loi* » occulte la complexité des preuves *blockchains*. Le juge n'aura pas qu'un rôle passif mais bien actif dans l'appréhension de ces preuves techniques. À tous les stades de la progression de la preuve numérique, le juge a nécessairement été impliqué dans sa reconnaissance et sa vérification[1212], ce qui doit être le cas avec la vérité cryptographique portée par les preuves générées par la *blockchain*. Le rapport De la Raudière/Mis rappelle que pour le moment *« aucun texte ne détermine la portée juridique des éléments inscrits sur un protocole blockchain. Dès lors qu'il ne fait pas partie des moyens de preuve actuellement reconnus au plan juridique, il appartient au juge de déterminer leur valeur probatoire, au vu des circonstances de l'espèce* »[1213] ce que nous envisagerons en titre 2.

[1210] J.-E.-M, Portalis, Discours préliminaire au premier projet du Code civil, présenté le 1er pluviôse an IX.
[1211] Montesquieu, *De l'esprit des lois*, 1748.
[1212] Cass. 1ère civ., 6 avr. 2016, n°15-10.732, F-D, Rejet : « *ALORS QUE dès lors qu'une partie dénie être l'auteur d'un écrit sous forme électronique, le juge est tenu de vérifier les conditions de validité de la signature c'est-à-dire que celle-ci consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache et, ainsi, que ce procédé mette bien en œuvre une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié* ».
[1213] Assemblée nationale, Rapport d'information n°1501, *op.cit.*, p.91.

PARTIE 2

L'APPREHENSION JURIDICTIONNELLE INSUFFISANTE DE LA « *VERITE CRYPTOGRAPHIQUE* » DES DONNEES ENREGISTREES DANS LA *BLOCKCHAIN*

579. L'appréhension de la vérité cryptographique par le juge français sera vraisemblablement propre à notre système latin. La culture dans notre système inquisitorial a pour but lors de tout procès d'emporter la conviction du juge afin que celui-ci soit en mesure d'établir la vérité[1214]. La tradition romano-germanique du droit cherche la substance afin d'établir un récit officiel au moyen d'un prononcé du jugement par un magistrat. Au contraire en *common law*, le juge n'est pas tenu par un devoir d'essayer d'établir la vérité en ce que la culture juridique est de tradition accusatoire[1215]. L'interprétation de la vérité cryptographique serait alors différente en *common law*.

580. La culture de *common law* organise la confrontation de deux versions pour en faire triompher une, la plus vraisemblable. Selon cette conception, la vérité doit rejaillir de la confrontation puisque les parties ont un intérêt à apporter tous les éléments au soutien de leur cause[1216]. Cette confrontation serait une bonne méthode pour arriver à la vérité[1217]. Ainsi, en *common law*, la vérité cryptographique pourrait triompher en étant confrontée à deux récits mais les juges feront volontiers l'économie d'établir sa substance, le récit officiel du jugement qui aura amené à cette vérité cryptographique.

581. L'appréhension de la vérité cryptographique à la française, qui s'instaure progressivement, à plusieurs vitesses et par des acteurs distincts de la justice, interpelle. Si le Ministère de la Justice confortait l'idée que les preuves issues des *blockchains* « *(…) peuvent aujourd'hui être légalement produites en justice* », ajoutant que le juge doit évaluer leur valeur probante « *(…) sans que celui-ci ne puisse les écarter au seul motif qu'elles existent sous forme numérique* »[1218], l'admissibilité des preuves et leur recevabilité ne représentent qu'une partie infime des opérations impliquées sur les preuves *blockchains*[1219]. Par ailleurs, la répartition classique du rôle entre le juge et les parties dans l'administration de la preuve, faisant émerger

[1214] G. Lardeux, « Preuve civile et vérité », *in* Le droit en autonomie et ouverture. Mél. En l'honneur de J.-L. Bergel, Bruylant, 2013, p.869-870.
[1215] J. A. Jolowicz, « Adversarial and Inquisitorial Models of Civil Procedure », JCLQ, vol. 52, avr. 2003, p.281-295.
[1216] F. Ferrand, Preuve, *op.cit.*, n°453.
[1217] A. Levasseur, H.W. Fontenot, « Le droit de la preuve aux États-Unis », in *La preuve : regards croisés*, *op.cit.*, p.184.
[1218] Question écrite n°22103 de D. Fasquelle, publiée au JO le 30/07/2019, réponse du Ministère de la Justice publiée au JO le 10/12/2019, p.10774. Voir annexe n°10.
[1219] Pour les opérations sur la preuve voir : O. Leclerc, J. Wigmore, *Un jalon vers une « science de la preuve ». La représentation graphique des raisonnements probatoires*, Tiré à part, Dalloz, févr. 2019.

le principe de coopération entre eux[1220], est revisitée par l'accroissement corrélatif du rôle des auxiliaires de justice dans la démystification des preuves *blockchains*. Le tribunal ne se forge plus une conviction qu'à partir des seules preuves présentées par les parties[1221]. Pourtant, lorsque des faits techniques au soutien de la manifestation de la vérité cryptographique sont apportés lors d'un procès, il convient que le juge soit à même de distinguer les différents visages des preuves *blockchains*, c'est-à-dire les données informatiques - brutes ou non - apportées par les parties, les faits constatés par un huissier de justice, et les faits qui ont impliqué une analyse en sciences informatiques par un expert.

582. Nous présenterons dans ce contexte l'intervention juridictionnelle relativement lacunaire dans la reconnaissance des preuves de données enregistrées dans la *blockchain* (titre 1). Soutenue par des auxiliaires de justice pour comprendre cette preuve particulièrement technique, nous expliquerons ensuite en quoi cette aide extra-juridictionnelle pour reconnaître la vérité cryptographique issue de ces preuves peut sembler démesurée (titre 2).

[1220] La répartition de ces rôle est d'abord observé en droit civil : L. Cadiet et E. Jeuland, *Droit judiciaire privé*, 5e éd., Litec, 2006, n°535 ; ainsi qu'en droit administratif : B. Pacteau, *Le Juge de l'excès de pouvoir et les motifs de l'acte administratif*, thèse 1971, n°91.

[1221] Remise en perspective de l'adage selon le célèbre adage d'Henri Motulsky, « *da mihi factum, tibi dabo jus* » signifiant « *donne-moi le fait, je te donnerai le droit* ».

TITRE 1

L'INTERVENTION JURIDICTIONNELLE PRUDENTE DANS LA RECONNAISSANCE DES PREUVES DE DONNEES ENREGISTREES DANS LA *BLOCKCHAIN*

583. Le pouvoir reconnu au juge dans l'administration de la preuve par les législations modernes est théoriquement proéminent et central[1222]. Les preuves *blockchains* ne s'en soustraient pas en principe. Naguère, le procès civil traditionnellement accusatoire fut construit comme un duel judiciaire entre les parties qui se plaçaient dans une situation d'« *égalité mythique* »[1223]. Ce « *libéralisme improductif* » a conduit à ralentir le cours de la justice et les législateurs ont progressivement limité la toute-puissance des parties par un renforcement des pouvoirs du juge[1224]. Nous montrerons alors dans quelle mesure les juridictions traditionnelles en matière de preuve des données enregistrées dans la *blockchain* ont un rôle cardinal (chapitre 1). Ce rôle rejoint l'office du juge, terme provenant du latin *officium* qui renvoie à la « *fonction* » ou la « *charge* » en ce qu'elle confère des pouvoirs au juge et lui impose aussi des devoirs qui sont applicables aux preuves de la *blockchain*. Pour le moment, l'office du juge étant largement insuffisant dans ce domaine, nous analyserons quelles sont les attentes dans son dépassement (chapitre 2).

[1222] Matérialisé par son pouvoir issus des articles suivants : C. pr. civ., art. 10, 11, al. 2, 132, al. 2, 138, 145, 146, al. 1er (T. Le Bars, « De la théorie générale des charges de la preuve et de l'allégation à la théorie globale des risques processuels », in Mél. G. Goubeaux, Dalloz- LGDJ, 2009, p.319 et s.).
[1223] H. Croze, *Le procès civil*, 2e ed., Dalloz, 2004, p.7.
[1224] *Ibid.*, p.7 ; G. Bollard, *Droit et pratique de la procédure civile*, Dalloz Action, 2012-2013, n°223-22 ; F. Ferrand, Preuve, *op.cit.*, n°327.

CHAPITRE 1

LE ROLE CARDINAL DES JURIDICTIONS TRADITIONNELLES EN MATIERE DE PREUVE DES DONNEES ENREGISTREES DANS LA *BLOCKCHAIN*

584. Le Professeur de droit et conseiller à la Cour de cassation Albert Tissier enseignait instructivement et avec contemporanéité que « *(…) l'objet du procès appartient aux parties ; mais la procédure ne leur appartient pas. Elles peuvent ne pas plaider ; mais si elles s'adressent au juge ; c'est à lui de diriger la marche du procès. L'État doit la justice : il la doit rapide et simple (…)* »[1225]. En tout état de cause, dans tout procès, c'est au demandeur - celui qui allègue dans le procès civil ou le Ministère Public et la partie civile dans le procès pénale - d'apporter la preuve de ce qu'il prétend[1226], mais ces demandeurs n'ont pas à eux seuls l'initiative de la charge de la preuve : le juge intervient aussi activement dans sa recherche. Un rôle central est alors accordé au juge dans la phase de recherche des preuves enregistrées dans la *blockchain* (section 1). Le juge intervient ensuite dans la phase d'appréciation de ces preuves où il détermine si ces dernières l'ont convaincu (section 2).

Section 1 : La recherche appropriée par le juge des preuves de données enregistrées dans la *blockchain*

585. Que ce soit en matière civile, comme en matière pénale, le juge dispose de forts pouvoirs d'administration dans la recherche des preuves *blockchains*. Si la preuve numérique de données est de nature volatile, la *blockchain* envisagée comme outil numérique de conservation de données de façon inaltérable[1227] devient un outil de traçabilité au soutien de preuves issues soit

[1225] A. Tissier, *Le rôle social et économique des règles de la procédure civile. Les méthodes juridiques*, *in* Leçons faites aux Collège libre des sciences sociales, Girard et Brière, 1910-1911, p.121-122.
[1226] Selon le vieil adage latin *actori incumbit probatio.*
[1227] Voir : M. Orcutt, « Some crypto-criminals think jumping across *blockchains* covers their tracks. Big mistake », MIT Technology Review, 22 août 2019 : « *Law enforcement officials can trace transactions and even identify who*

d'une faute ou d'un fait en matière civile, soit de la commission d'une infraction en matière pénale. Les preuves *blockchains* n'échappent donc pas à leur recherche par le juge, avec plus ou moins d'intensité en fonction de la nature du procès.

586. Nous déciderons alors dans les développements suivants de traiter de manière indifférenciée la recherche par le juge des preuves *blockchains* de nature civile (paragraphe 2) et celles de nature pénale (paragraphe 1). Ce choix s'explique par l'impétueuse apparition des cas d'escroquerie visant les crypto-actifs (objets d'infractions)[1228] et de blanchiment d'argent[1229] par le biais de crypto-actifs (supports d'infractions). Dès 2011, Tracfin (Traitement du renseignement et action contre les circuits financiers clandestins) proclamait que l'usage du bitcoin à des fins illégales était à l'origine de risques et d'insécurité mais que la *blockchain* présentait toutefois l'avantage de rendre accessibles les données de ce registre à n'importe quel observateur et d'identifier les protagonistes par leurs transactions publiques et leurs adresses publiques tracées[1230]. Un aparté dans les chemins du procès pénal par une analyse approfondie de ce phénomène semble particulièrement opportun.

Paragraphe 1 : La recherche de la preuve pénale parmi les données enregistrées dans la *blockchain*

587. La *blockchain* est exploitée par des cyber-délinquants pour faciliter, commettre, voire dissimuler une infraction. De plus en plus de phénomènes délictueux visent en effet des actifs numériques échangés *via* des *blockchains*, alors que d'autres phénomènes relèvent d'une adaptation d'infractions plus traditionnelles à ce domaine[1231]. La *blockchain*, porteuse de contenus illégaux constitutifs d'infractions (pornodivulgation (ou *revenge porn*), *ransomware*,

is making them ». Par exemple : en 2018, Tracfin a constitué une cellule d'enquête composée d'agents spécialisés en cybercriminalité financière qui a développé des compétences pour retracer les transactions dans le registre de la *blockchain* et identifier les flux résultant d'opérations délictueuses (Tracfin, Tendances et analyse des risques de blanchiment de capitaux et de financement du terrorisme en 2018-2019, *op.cit.*, p.61).

[1228] En 2018, l'AMF enregistrait 55 millions d'euros de pertes déclarées par des particuliers sur des crypto-actifs proposés par des plateformes frauduleuses (https://www.capital.fr/entreprises-marches/bitcoin-55-millions-deuros-darnaques-declarees-a-lautorite-des-marches-financiers-1335749 (consulté le 31/05/2020)).

[1229] En 2017, Tracfin recevait 250 déclarations de soupçon sur les crypto-actifs. Elle augmentait de 44% par rapport à 2016 mais elle représentait toutefois seulement 0,4% du total des 68 661 déclarations de soupçon en 2017 (Tracfin, Tendances et analyse des risques de blanchiment de capitaux et de financement du terrorisme 2017-2018, *op.cit.*, p.58).

[1230] Tracfin, Rapport annuel d'activité 2011, 22 août 2012, p.21-22.

[1231] Voir *supra* n°199-203.

malware) et de transactions illicites, apparait alors comme un instrument de traçabilité intéressant en vue de rechercher et d'identifier les cyber-délinquants, rassembler des preuves, et constater des infractions. À titre d'exemple, les indices qu'une plateforme d'échange de monnaie ayant cours légal en actifs numériques et inversement réalise un certain nombre de flux, quand bien même elle exercerait son activité sans l'enregistrement obligatoire requis auprès de l'AMF[1232], pourraient être retrouvés dans certains registres distribués de transactions. Le Parlement européen souligne à ce titre au point F de sa résolution du 3 octobre 2018 que la *blockchain* « *(…) peut fournir un cadre de transparence, réduire la corruption, déceler l'évasion fiscale, permettre le suivi de paiements illicites, faciliter les politiques de lutte contre le blanchiment de capitaux et détecter les détournements d'actifs* »[1233]. La recherche de la preuve pénale est réalisée pour partie par les autorités de police sur accord des autorités judiciaires dans le cadre de procédures traditionnelles (A) et nouvelles (B) applicables aux données enregistrées dans la *blockchain.*

A. Les procédures traditionnelles applicables à la recherche de données enregistrées dans la *blockchain*

588. Des procédures classiques de perquisition (1) et de saisie et confiscation (2) de données figurant dans un registre de *blockchain* sont déjà mises en œuvre efficacement par des officiers de police judiciaire, avec des particularismes tenant à cette technologie.

1. Les procédures de perquisitions applicables aux données enregistrées dans la *blockchain*

589. **L'objet de la perquisition : les paires de clés.** La procédure de perquisition de données a pour but de chercher et d'accéder à des données de contenu intéressant l'enquête. Cette phase de perquisition est une étape cardinale car elle conditionne les facultés de saisie[1234]. Elle permet la prise de connaissance des données informatiques par l'officier de police judiciaire avant de

[1232] C. mon. fin., art. L54-10-4. Le manquement à l'enregistrement est pénalement réprimé à un an ou 15 000 euros d'amende ou deux ans ou 30 000 pour une personne morale (C. mon. fin., art. L572-23).
[1233] Parlement européen, Résolution du 3 oct. 2018 sur les technologies des registres distribués et les chaînes de blocs: renforcer la confiance par la désintermédiation (2017/2772(RSP)), P8_TA(2018)0373.
[1234] « Question à Olivier Le Guen sur la perquisition et la saisie des crypto-actifs », Dossier : la justice pénale à l'épreuve des crypto-monnaies, Dalloz IP/IT n°10, oct. 2019, p.541.

procéder à leur saisie[1235]. Selon l'article 57-1 du Code de procédure pénale, les officiers de police peuvent accéder à des données intéressant l'enquête par un système informatique implanté dans les lieux où se déroule l'enquête ou dans un autre système informatique[1236]. Elles se déroulent en revanche sous le contrôle d'un magistrat du siège, soit le juge d'instruction ou un juge des libertés et de la détention[1237].

590. **L'objet de la perquisition dans une *blockchain* porterait sur les paires de clés cryptographiques attestant la possession d'actifs numériques.** Rappelons qu'un actif numérique est conservé sur une clé publique (ou adresse publique) et est contrôlé par la clé privée associée. Généralement les clés privées sont conservées selon deux grandes catégories, soit par une auto-conservation par le détenteur des actifs lui-même, soit par une conservation pour le compte de tiers (les acteurs réalisant cette activité de portefeuille numérique sont considérés en France comme des PSAN).

591. **Les difficultés pratiques de la perquisition : l'auto-conservation et la multiplicité de stockage des clés cryptographiques.** Lorsque les clés sont auto-conservées, il est très complexe voire impossible en pratique d'assurer l'effectivité de la perquisition. Lorsqu'elles ne le sont pas, la difficulté essentielle de la perquisition se situe au niveau de la multitude de portefeuilles numériques, et ainsi de modalités de stockage de clés privées. Il pourra s'agir de stockage hors ligne ou dit « *à froid* » (ou *cold wallets*) en mode *hardware* sous forme de clés USB, ou des stockages en ligne ou dits « *à chaud* » (ou *hot wallets*), c'est-à-dire des portefeuilles en ligne, installés par des logiciels en mode *software* sur ordinateur, tablette ou smartphone qui sont connectés à Internet dont les données sont stockées sur une infrastructure accessible par Internet. Ces supports sont difficilement accessibles aux officiers de police puisque, en sus de l'accès aux clés privées, des codes pin protègent les *cold wallets*, des mots de passe et identifiants de compte pour l'accès aux *hot wallets*[1238].

592. **Les contraintes de la perquisition transfrontalière.** La loi n°2014-1353 du 13 novembre 2014 relative à la lutte contre le terrorisme étend les pouvoirs des enquêteurs en cas

[1235] C. pr. pén., art. 56, al. 2.
[1236] C. pr. pén., art. 94.
[1237] M. Quemener, F. Dalle, « L'accès à la preuve numérique, enjeu majeur de toute enquête pénale : pratique et perspectives », Dalloz IP/IT, juill.-août 2018, p.420.
[1238] « Question à Olivier Le Guen sur la perquisition et la saisie des crypto-actifs », Dossier : la justice pénale à l'épreuve des crypto-monnaies, *op.cit.*, p.541-542.

de données stockées dans un système situé en dehors du territoire national. Si la perquisition est transfrontière, elle devra être néanmoins soumise aux conditions d'accès prévues par les engagements internationaux. La collecte des preuves ne peut en effet dans ce cas s'opérer que dans le respect des conventions internationales, comme la Convention de Budapest du 23 novembre 2001.

593. La dimension internationale de la *blockchain* génère des difficultés quant à la recherche de preuves pénales numériques. Les données utiles aux enquêtes se situeront quasi-systématiquement à l'étranger compte tenu de toutes les copies du registre synchronisées entre les nœuds situés en tout lieu. Un respect attentif des conventions internationales devra ainsi être mis en place.

2. Les saisies et confiscations appliquées aux données enregistrées dans la *blockchain* Bitcoin

594. **La saisie de données informatiques.** Les mesures de saisie peuvent intervenir à tout moment de la procédure, en phase d'enquête préliminaire, de flagrance ou lors de l'instruction. Elles ont pour but soit de placer sous main de justice tout objet utile à la manifestation de la vérité[1239], soit de faciliter l'usage ultérieur de la peine complémentaire de confiscation[1240], soit enfin à titre conservatoire, de garantir l'exécution d'une éventuelle condamnation pécuniaire. La saisie de données informatiques peut se faire soit en plaçant sous main de justice le support physique de ces données (comme un disque dur, une clé USB, un ordinateur, une tablette, ou un téléphone), soit en réalisant une copie en présence des personnes qui assistent à la perquisition[1241]. Dans ce dernier cas, le Procureur de la République ou le juge d'instruction peut prononcer l'effacement définitif des données sur le support physique qui n'a pas été placé sous main de justice[1242].

595. **La saisie d'actifs numériques.** L'objet de la saisie de l'instrument ou encore des produits de l'infraction concerne essentiellement pour l'heure les actifs numériques. La saisie pourra s'effectuer uniquement par leurs transferts vers un portefeuille étatique auprès de

[1239] C. proc. pén., art. 56, al. 7 et 97, al. 3.
[1240] C. pén., art. 131-21.
[1241] C. pr. pén., art. 56, al. 5 et 97, al. 3.
[1242] C. pr. pén., art. 56, al. 6 et 97, al. 4.

l'Agence de gestion et de recouvrement des avoir saisis et confisqués (AGRASC)[1243]. L'efficience de la saisie passe donc par le biais de ce transfert d'actifs numériques. Il est permis de songer que des données autres que des actifs numériques pourraient être saisies, comme celles renvoyant à des données à caractère pédopornographique. En Mars 2018, la *blockchain* Bitcoin contenait au moins huit fichiers comportant un contenu à caractère sexuel. Deux d'entre eux sauvegardaient des listes de 274 liens vers de la pornographie juvénile[1244].

596. **Les spécificités de la saisie de données enregistrées dans la *blockchain*.** Des techniciens étrangers à la commission de l'infraction pourront être amenés à intervenir notamment pour lever les obstacles à l'investigation et l'extraction dans le cas de données chiffrées[1245].

597. **L'exemple de la saisie de bitcoins.** En France, un exemple témoigne de l'effectivité de la saisie. Dans le cadre d'une instruction judiciaire, une mesure de perquisition a en effet permis la saisie d'environ 388 bitcoins sur une plateforme d'échange par la section de recherche de la gendarmerie de Toulouse, le 7 juillet 2014[1246]. Aux États-Unis aussi environs 170 000 bitcoins ont été saisis dans l'affaire dite « *Silk Road* »[1247]. En définitive, ces affaires montrent que cette procédure d'enquête est déjà appliquée essentiellement à la *blockchain* Bitcoin.

B. Les procédures récentes adaptées aux complexités de la recherche de données enregistrées dans la *blockchain*

598. Deux nouvelles procédures appliquées au monde numérique s'adaptent tout à fait à l'environnement de la *blockchain* pour la recherche de preuves pénales. L'une est créée pour

[1243] « Question à Olivier Le Guen sur la perquisition et la saisie des crypto-actifs », Dossier : la justice pénale à l'épreuve des crypto-monnaies, *op.cit.*, p.542.
[1244] R. Matzutt, J. Hiller, M. Henze, J.-H. Ziegeldorf, « A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin », *op.cit.*, fevr. 2018, p.13.
[1245] P. Roussel, « L'emploi de l'informatique dans l'administration de la preuve », Etude 11, Droit pénal n°9, sept. 2005, n°14.
[1246] https://www.latribune.fr/technos-medias/internet/20140707trib000838782/bitcoin-le-premier-trafic-demantele-en-europe-est-francais.html (consulté le 31/05/2020).
[1247] Aux États-Unis, l'affaire dite « *Silk Road* » du 2 octobre 2013 illustre le recours à la saisie. Le site de e-commerce Silk Road offrait des services illégaux sur une plateforme du web cachée (ou *deep web*) pour lesquels des paiements étaient systématiquement effectués en bitcoins. Ce site a donc été fermé par le « *Federal Bureau of Investigation* » (FBI) et une saisie et confiscation de bitcoins a eu lieu avec une vente aux enchères par les autorités judiciaires américaines. Voir : Ministre de l'Économie et des Finances, Les crypto-monnaies, Rapport au Ministre de l'Économie et des Finances Jean-Pierre Landau avec la collaboration d'Alban Genais, juill. 2018, p.37.

une nouvelle forme de criminalité qui implique la mise en place d'enquêtes spécifiques à l'identification des cyber-délinquants : c'est l'enquête sous pseudonyme (1). L'autre, la captation, s'applique au champ matériel nouveau des infractions : la donnée, puisqu'aujourd'hui, 85 % des enquêtes pénales font intervenir des données numériques (2)[1248].

1. L'enquête sous pseudonyme

599. **Le fonctionnement et les objectifs de l'enquête sous pseudonyme.** L'enquête sous pseudonyme est une enquête par laquelle les officiers ou agents de police judiciaire peuvent interagir avec les suspects par échanges électroniques afin de recueillir les éléments de preuve d'une infraction mais sans aucune provocation à la commettre[1249]. En pratique, les services de police judiciaire opèrent sur Internet en utilisant un pseudonyme dans le but de traquer les personnes qui commettent des infractions et de parvenir à pénétrer leurs réseaux. Les agents conservent leur anonymat, par le biais du recours à une identité d'emprunt, leur permettant de participer aux échanges et d'être en contact avec les auteurs de ces infractions, par exemple en créant de faux profils sur les réseaux sociaux et autres forums.

600. Elle implique ainsi la faculté pour les agents de participer à des échanges, d'extraire, d'acquérir ou de conserver des éléments de preuve et des données sur les présumés auteurs de ces infractions et même d'acquérir ou de conserver des contenus illicites[1250]. Elle permet de faciliter la constatation des infractions par les agents de police habilités, sans l'obtention préalable d'une autorisation par un magistrat[1251].

601. **L'enquête sous pseudonyme étendue à toutes les infractions commises par voie de communications électroniques.** L'article 230-46 du Code de procédure pénale issu de la loi n°2019 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice a étendu cette enquête à toutes les infractions commises par voie de communications électroniques. Cette procédure est désormais applicable pour constater les crimes et les délits punis d'une peine

[1248] https://www.consilium.europa.eu/fr/policies/e-evidence/ (consulté le 31/05/2020)
[1249] M. Quémener, Fasc. 35 : la preuve numérique dans le cadre pénal, JCl. Communication, Lexis Nexis, 18 avr. 2019, n°61.
[1250] *Ibid*.
[1251] A. Jomni, « crypto-tracking : les nouveau outils d'enquête pour les forces de l'ordre », Revue de la gendarmerie nationale n°263, dec. 2018, p.116.

d'emprisonnement commis par la voie des communications électroniques. Avant cette loi du 23 mars 2019, la Cour de cassation avait considéré pour certaines infractions déterminées que le texte qui autorisait les enquêteurs habilités à rassembler des preuves et rechercher les auteurs, en participant avec eux à des échanges de messages électroniques sous pseudonyme, sans pouvoir pour autant inciter à leur commission, n'entraînait aucune violation des droits de la défense, ni aucune intrusion dans la vie privée de la personne qui demeurait libre de répondre auxdits messages en appréciant librement le contenu de sa réponse[1252].

602. **Enquête sous pseudonyme et *blockchain*.** L'enquête sous pseudonyme dans le cadre de la *blockchain* permettra surtout de récupérer des données préalables aux infractions commises ensuite *via* une transaction en actifs numériques inscrite dans une *blockchain*. Par exemple, il pourrait s'agir d'un prétendu délinquant qui commet une escroquerie aux investissements fictifs ou n'est qu'un intermédiaire dans le commerce de produits illicites. C'est en communiquant préalablement avec celui-ci que les officiers ou agents de police pourront rassembler des indices pour identifier celui qui commet l'infraction.

2. La captation des données enregistrées dans la *blockchain*

603. **Le fonctionnement et les objectifs de la captation de données.** La technique d'enquête numérique spéciale de captation des données a été créée et introduite par la loi n°2011-267 d'orientation et de programmation pour la performance de la sécurité intérieure du 14 mars 2011 dite « *LOPPSI* 2 », connaissant moult évolutions depuis. Elle est strictement encadrée aux articles 706-102-1 à 706-102-5 du Code de procédure pénale. Ces dispositions ouvrent la possibilité, pour les officiers et agents de police judiciaire, agissant sur commission rogatoire, de mettre en place un dispositif technique, sans le consentement des intéressés, ayant pour objet d'accéder, en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre, telles qu'elles sont stockées dans un système informatique, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un STAD, telles qu'ils les y introduisent par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques[1253]. La loi n°2016-731 du 3 juin 2016 a également étendu la catégorie des données récupérables aux

[1252] Cass. crim., 7 févr. 2018, n°17-90.026 : Comm. com. électr. 2018, comm. 29, A. Lepage.
[1253] C. pr. pén., art. 706-102-1, al. 1.

données stockées dans un système informatique, ce qui permet en théorie de rechercher à distance dans le disque dur du terminal ciblé des informations utiles à la manifestation de la vérité[1254]. Par exemple, le dispositif permettra aux enquêteurs habilités de capter des données liées à des actifs numériques blanchis à distance à la suite de ventes de services illicites pour y avoir accès, les enregistrer, les conserver et les transmettre.

604. La mise en œuvre de cette enquête implique que le procureur de la République et le juge d'instruction puissent désigner toute personne physique ou morale habilitée et inscrite sur l'une des listes prévues en vue d'effectuer les opérations techniques permettant la réalisation du dispositif susmentionné[1255]. En vue de mettre en place ledit dispositif, le juge des libertés et de la détention, à la requête du procureur de la République, ou le juge d'instruction peut autoriser la transmission de ce dispositif par un réseau de communications électroniques[1256]. Ces opérations sont effectuées sous l'autorité et le contrôle du juge des libertés et de la détention ou du juge d'instruction[1257].

605. **Captation de données et *blockchain*.** Très concrètement, dans le cadre d'un environnement de réseau distribué *blockchain*, un logiciel « *espion* » pourrait prendre partiellement le contrôle du terminal informatique du prétendu délinquant réalisant du blanchiment d'argent de crypto-actifs pour entre autres blanchir le produit d'une escroquerie réalisée grâce à une identité fictive[1258]. Les enquêteurs pourraient avoir accès à tout ce qui s'affiche à l'écran de ce cyber-délinquant pour ainsi voir comment l'individu utilise son navigateur et enregistre aussi les frappes du clavier[1259]. Cette solution aura notamment l'avantage de contourner le chiffrement des communications en dehors de la *blockchain*[1260]. Notons que cet argument ne pourra pas se révéler efficace dans le cadre du chiffrement utilisé pour émettre et recevoir des transactions dans une *blockchain* publique car un « *message* » n'est pas à proprement rendu secret.

[1254] M. Quémener, Fasc. 35 : la preuve numérique dans le cadre pénal, *op.cit.*, n°69.
[1255] C. pr. pén., art. 706-102-1, al. 2.
[1256] C. pr. pén., art. 706-102-5, al. 2.
[1257] C. pr. pén., art. 706-102-5, al. 1 et 2.
[1258] Voir ce cas déjà analysé par Tracfin : Tracfin, Tendances et analyse des risques de blanchiment de capitaux et de financement du terrorisme en 2018-2019, *op.cit.*, p.66.
[1259] C. Feral Schuhl, Cyberdroit, Praxis Dalloz, 2020/2021, p.1685, n°721.151.
[1260] M. Quémener, Fasc. 35 : la preuve numérique dans le cadre pénal, *op.cit.*, n°69.

C. Les techniques de l'informatique légale et autres voies de renforcement des moyens d'enquête

606. **Les obstacles techniques à la recherche de la preuve pénale : l'anonymisation des connexions et le mixage de données.** La recherche de la preuve pénale sur un support *blockchain* semble complexe et fastidieuse corrélativement à l'esprit retors des cyber-délinquants[1261]. Même si la *blockchain* est généralement pseudonyme[1262], certains acteurs de la *blockchain* utilisent des réseaux privés virtuels (VPN) ou les réseaux TOR, des réseaux qui permettent d'anonymiser l'origine des connexions, notamment les adresses IP. Par ailleurs, les techniques sophistiquées du mixage de données constituent aussi des entraves à la recherche de données enregistrées dans la *blockchain*. Des services nommés « *mixeurs* » proposent à tout individu de mélanger ses actifs numériques - notamment issus d'activités illicites - avec les unités propres du mixeur pour ensuite les redistribuer à son titulaire originel moyennant une commission[1263]. L'idée pour ces mixeurs serait alors de « *brouiller les pistes* » quant au lien entre l'origine de l'actif numérique et le titulaire. Une action conjointe des Pays-Bas, du Luxembourg et d'Europol a permis de suspendre l'activité de l'important mixeur « *Bestmixer.io* » dont une grande partie d'actifs numériques mixés avait une origine ou une destination criminelle[1264].

607. **Des outils proposés par l'informatique légale (ou *computer forensic*) : la *blockchain forensic*.** Des outils bénéficient aux procédures d'investigation comme le *crypto-tracking* accompagné d'une veille policière classique. Le *crypto-tracking* est un outil de l'informatique légale offrant la possibilité d'analyser des flux de transactions suspectes en actifs numériques dans le but de caractériser une infraction pénale. Il repose sur une exploration des transactions en actifs numériques inscrites de manière « *indélébile* » dans les registres distribués de

[1261] Voir à ce sujet sur cette complexité de la recherche de la preuve numérique dans le secteur économique et financier : S.-M. Cabon, « L'influence du cyber espace sur la criminalité économique et financière », Etude 5, Droit pénal n°3, mars 2018, n°12-16.
[1262] Voir *supra* n°298 et s.
[1263] J. Martinon, « Crypto-actifs : la justice pénale à l'épreuve des crypto-monnaies », Dossier : la justice pénale à l'épreuve des crypto-monnaies, Dalloz IP/IT n°10, oct 2019, p.533 ; J. Martinon, « Phénomènes criminels célèbres ou exotiques dans le champ des crypto-actifs (illustrations extraites de la présentation de Patrice Réveillac, Europol) », Dossier : la justice pénale à l'épreuve des crypto-monnaies, Dalloz IP/IT n°10, oct 2019, p.540.
[1264] Europol, Press release, « Multi-million euro cryptocurrency laundering service bestmixer.io taken down », 22 mai 2019, https://www.europol.europa.eu/newsroom/news/multi-million-euro-cryptocurrency-laundering-service-bestmixerio-taken-down (consulté le 31/05/2020).

blockchain[1265]. Cet outil d'informatique légale fait partie intégrante de la famille des techniques d'investigation numérique légale ou *inforensique*. L'investigation numérique légale consiste en l'application de processus et techniques d'investigation permettant de collecter et d'analyser des éléments ayant valeur de preuves en vue d'une procédure judiciaire[1266]. Appliqués à la *blockchain*, ces nouveaux outils forment une branche de l'*inforensique* : la *blockchain forensic*.

608. **Dans l'attente d'un accès transfrontalier aux preuves pénales renforcé par la directive et le règlement dits « *e-evidence* ».** La règlementation dite « *e-evidence* » relative à la preuve électronique aménagerait un régime d'accès transfrontalier aux preuves pénales facilité et plus direct au sein de l'Union européenne. La Commission européenne a présenté le 17 avril 2018 un projet de directive établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale et un projet de règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale[1267]. D'une part, la directive obligera tous les fournisseurs de services à désigner un représentant légal dans l'Union européenne. Ce dernier sera en charge de la réception et du respect des décisions et des injonctions. Cette mesure a pour ambition de soumettre tous les fournisseurs de l'Union européenne à des obligations uniformisées concernant les preuves électroniques. D'autre part, la directive permettra aux autorités judiciaires d'accéder aux preuves électroniques stockées par les fournisseurs de services dans l'Union européenne. D'un côté, le règlement prévoit une injonction de production qui donnera un accès direct aux autorités judiciaires d'un État membre leur permettant de demander des preuves électroniques détenues par un fournisseur de services établi dans un autre État membre. Celui-ci sera tenu de répondre dans un délai de dix jours, délai ramené à six heures dans l'hypothèse d'une urgence. De l'autre côté, une injonction de conservation empêchera, durant le traitement de l'injonction de production, la suppression des preuves électroniques par le fournisseur de services[1268]. De nombreux enjeux et risques en matière de protection de la vie privée, principe de souveraineté et de territorialité sont encore en suspens[1269]. Qui plus est, ce règlement pourrait faire doublon avec la décision-cadre du Conseil relative aux équipes

[1265] A. Jomni, « Crypto-tracking, les nouveaux outils d'enquête pour les forces de l'ordre », Revue de la gendarmerie nationale n°263, déc. 2018, p.114.
[1266] C. Feral Schuhl, Cyberdroit, Praxis Dalloz, *op.cit.*, n°721.191.
[1267] Proposition de Règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, COM(2018) 225 final 2018/0108(COD).
[1268] https://www.consilium.europa.eu/fr/policies/e-evidence/ (consulté le 31/05/2020).
[1269] J.-S. Mariez, « Une nouvelle étape vers un accès transfrontalier aux preuves numériques : l'initiative européenne « e-evidence » ou la recherche d'un équilibre entre efficacité des enquêtes pénales, droit des personnes concernées et sécurité », RLDI n°146, mars 2018, p.53-61.

communes d'enquête qui fixe les règles relatives à la création et au fonctionnement des équipes communes d'enquête (ECE) au sein de l'Union européenne[1270]. La version finale de ce texte doit donc encore être discutée avec le Parlement européen.

609. À titre d'exemple, ce règlement permettrait à l'autorité judiciaire française d'introduire une injonction pour avoir accès à un ensemble de données liées à des transactions en « *Monero* » à une plateforme d'échange européenne. Aussi son utilité ne serait pas de moindre importance en vue de l'obtention plus directe des autorités des données enregistrées dans des *blockchains* privées (données hachées mais aussi les données de contenu comme des vidéos, des images, des liens hypertextes) et associées (données de connexion), très longues et difficiles à obtenir auprès de prestataires de service basés à l'étranger[1271]. Enfin, l'opportunité pourrait être saisie par les autorités de police d'accéder à des preuves situées dans le cloud des fournisseurs de BaaS, indépendamment de la localisation de celui-ci sur le territoire européen. Le règlement dit *e-evidence* se profile ainsi comme un catalyseur des enquêtes transfrontalières liées à la *blockchain*.

610. **L'appel à des moyens d'investigation renforcés.** Une circulaire de la direction des affaires criminelles et des grâces du Ministère de la Justice a requis le 18 octobre 2018 le recensement de toutes les procédures d'escroqueries aux faux investissements dans les actifs numériques en vue de regrouper les plaintes nécessitant des investigations complexes dans l'intérêt d'une bonne administration de la justice[1272]. Pour mener à bien ces investigations complexes, nous appelons de nos vœux des moyens technologiques renforcés d'investigation pour la recherche de preuves pénales dans la *blockchain*, mis à disposition des services d'enquête, c'est-à-dire des agents et officiers de police judiciaire, mais aussi de TRACFIN et des cyberdouanes concernant la lutte contre le blanchiment et le financement du terrorisme. Si les outils actuels d'investigation permettent uniquement le suivi des transactions illicites réalisées en bitcoins, il conviendrait que des instruments plus puissants soient compatibles avec d'autres crypto-actifs.

[1270] Décision-cadre du Conseil 2002/465/JAI du 13 juin 2002 relative aux équipes communes d'enquête.
[1271] M. Quémener, Fasc. 35 : la preuve numérique dans le cadre pénal, *op.cit.*, n°115.
[1272] Direction des affaires criminelles et des grâces, sous- direction de la justice pénale spécialisée, Bureau du droit économique, financier et social, de l'environnement et de la santé publique, Dépêche relative au recensement des procédures d'escroqueries aux faux investissements dans les cryptoactifs, n°2018/F/0090/FC1, le 18 oct. 2018. Voir annexe n°9.

611. Un effort d'investissement dans nos capacités technologiques est sollicité par le législateur pour ces investigations[1273]. Cette nécessité impérieuse a été entendue par le ministère de l'intérieur qui a déjà entrepris des travaux de renforcement visant à doter la gendarmerie, la police nationale et les douanes d'outils pour analyser les transactions en crypto-monnaies. Ce sont à ce stade uniquement des appels d'offre qui sont lancés[1274]. Formulons enfin le souhait que le complexe mondial Interpol pour l'innovation (CMII), chargé notamment du soutien aux enquêtes, prenne la mesure de la complexité des moyens d'enquête axés dans l'environnement de la *blockchain*.

Paragraphe 2 : La recherche de la preuve civile parmi les données enregistrées dans la *blockchain*

612. Traditionnellement, l'administration de la preuve repose sur la recherche de la vérité[1275]. Cette vérité dans la *blockchain* pourrait consister dans la recherche de preuve sur un contenu contrefaisant, des injures et diffamations, ou encore une atteinte à la vie privée. Rappelons que l'administration de la preuve est la combinaison du rôle des parties et du juge illustrée parfaitement par l'adage latin *Da mihi factum, tibi dabo jus* signifiant « *donne-moi les faits, je te donnerai le droit* ». L'administration judiciaire et les contestations afférentes sont régies par le Code de procédure civile, selon l'article 1357 du Code civil qui y fait un renvoi. Dans cette administration de la preuve, le rôle du juge est toutefois des plus conséquent, en témoigne l'article 3 du Code de procédure civile indiquant que « *le juge veille au bon déroulement de l'instance ; il a le pouvoir d'impartir les délais et d'ordonner les mesures nécessaires* ». Ce rôle justifié par l'émergence d'un véritable « *droit à la preuve* » érigé en droit fondamental, a essentiellement pour objectif de faciliter l'administration des preuves et de rapprocher la vérité juridictionnelle de la vérité des faits[1276]. L'administration de la preuve civile des données

[1273] J.-M. Mis, « Crypto-monnaie : une régulation/réglementation « contre-nature » ou « naturellement indispensable » à son développement ? », *op.cit.*, p.552.

[1274] https://www.marches-publics.gouv.fr/index.php?page=entreprise.EntrepriseDemandeTelechargementDce&refConsultation=417559&orgAcronyme=g6l&fbclid=IwAR2CdMLjvWi91QlCuHQ6MFKV5k3lSzTtZR8bvkpkx_nljcxtzrhU9Cl8E0s (consulté le 31/05/2020).

[1275] F. Terré, *Introduction générale au droit*, *op.cit.*, n°613.

[1276] Cass. 1ère civ., 5 avr. 2012, n°11- 14.177, Bull. civ. I, n°85, D. 2012. 1596, note Lardeux. Voir au sujet de l'émergence du droit à la preuve : C. Grimaldi, « Comment résoudre les conflits de droits fondamentaux relatifs à la preuve ? », *in* V. Boccara, « Du droit de la preuve au droit à la preuve, question de mots ou changement de cap ? », *op.cit.*, p. 5.

enregistrée dans la *blockchain* sera ainsi impactée par cette place centrale du juge dans cette mission de recherche de vérité. Partant, le pouvoir d'investigation du juge quant à ces données est important (B) mais ces données soutiennent, du reste, le principe dispositif (A).

A. Les données enregistrées dans la *blockchain* au soutien du principe dispositif

613. **La délimitation de la matière litigieuse par les parties.** Notre héritage du droit latin nous enseigne que « *la charge de la preuve incombe impérativement à l'accusation, mais elle échoit au défendeur chaque fois qu'il soulève une exception ou plus généralement un moyen de défense* »[1277]. Rappelons que ce sont les parties qui soumettent aux juges leurs prétentions, qui déterminent l'objet du litige tel qu'énoncé par l'article 4 du Code de procédure civile, lequel dispose que « *l'objet du litige est déterminé par les prétentions respectives des parties* ». Ces prétentions sont alors fondées sur des éléments de fait que les parties ont la charge d'alléguer, selon les articles 6 et 9 du Code de procédure civile. Dans notre droit français actuel ce sont effectivement les parties au procès qui ont la charge d'alléguer les faits propres à fonder leur prétention[1278] et de prouver les faits nécessaires à leur succès[1279]. Cette charge processuelle fait référence à la règle posée par l'article 1353 du Code civil, qui indique que « *celui qui réclame l'exécution d'une obligation doit la prouver* ». Toutes ces règles qui font du procès « *la chose des parties* » sont ainsi l'expression du principe dispositif, qui laisse aux parties seulement le soin de délimiter la matière litigieuse.

614. **Les données enregistrées dans la *blockchain* au succès des prétentions des parties.** Les données enregistrées dans la *blockchain* serviront alors, si l'occasion se présente, aux parties pour prouver les faits nécessaires au succès de leurs prétentions. Les faits propres à fonder leurs prétentions et nécessaires à leur succès pourront être basés sur des données présentes dans un registre distribué. À ce moment-là, cette preuve cryptographique participera à la découverte de la vérité cryptographique, soutien probablement important aux prétentions des parties.

[1277] De l'adage latin : « *Actorié incombit probatio, reus in excipiendo fit actor* ».
[1278] C. proc. civ., art. 6. Voir le rejet d'une demander en justice si les faits allégués ne sont pas de nature à la fonder : Cass. 2ème civ., 24 mars 1971, n°70-11.114, Bull. civ. II, n°130.
[1279] C. proc. civ., art. 9.

615. Au nom de la recherche de la vérité, le juge ne pourra pas aller, en théorie, au-delà des faits liés à la *blockchain* proposés par les parties. Un auteur écrivait à ce titre que « *le juge doit retenir du litige l'édifice de fait qu'en apportent les parties, toutes les parties ensemble* »[1280]. Le juge dispose toutefois de l'obligation de donner ou restituer leur exacte qualification aux faits et actes litigieux sans s'arrêter à la dénomination des preuves *blockchains* que les parties en auraient proposée[1281]. Or, il ne peut changer la dénomination ou le fondement juridique lorsque les parties, en vertu d'un accord exprès et pour les droits dont elles ont la libre disposition, l'ont lié par les qualifications et points de droit auxquels elles entendent limiter le débat. D'autres pouvoirs étendus d'investigation du juge interpellent et nécessitent une analyse approfondie pour la technologie *blockchain*.

B. Le pouvoir d'investigation réelle du juge quant aux données enregistrées dans la *blockchain*

616. **Pouvoir de recherche du juge dans les données enregistrées dans la *blockchain*.** L'étendu du pouvoir de recherche de la preuve de données enregistrées dans la *blockchain* par le juge lors de la phase d'instruction est large. Pour le Professeur Frédéric Ferrand, il conviendrait de reconnaître au juge « *(…) un pouvoir d'office de rechercher la vérité matérielle des circonstances de fait litigieuse, parfaire sa conviction pour rendre un jugement jugé en vérité* »[1282]. Dégager un « *office de vérité* » du juge était le sens d'une proposition du rapport publié le 30 mai 2013 de la mission de réflexion sur l'évolution de l'office du juge et son périmètre d'intervention confiée par Madame Christiane Taubira à l'Institut des hautes études sur la justice. Cet office aurait pour but d'établir la vérité des faits de façon indépendante, procédurale et argumentée[1283]. En effet, « *neutralité* » du juge ne signifie pas « *passivité* »[1284]. Le rôle actif du juge se justifierait également par le souci de tenir compte et de remédier à l'inégalité entre les parties[1285]. Le droit français rejette l'idée d'une passivité en matière de

[1280] G. Bolard, *Droit et pratique de la procédure*, Dalloz, 2014/2015, n°221.51.
[1281] C. proc. civ., art. 12, al. 2 et 3.
[1282] F. Ferrand, Preuve, *op.cit.*, n°327.
[1283] Rapport de la mission de réflexion confiée par Madame Christiane Taubira, garde des Sceaux, à l'Institut des hautes études sur la justice, sur l'évolution de l'office du juge et son périmètre d'intervention, « La prudence et l'autorité l'office du juge au XXIe siècle », mai 2013, p.20.
[1284] S. Grignon Dumoulin, « L'office du juge civil dans la recherche de la preuve », Justice & Cassation, Revue annuelle des avocats au Conseil d'État et à la Cour de cassation, Dossier la preuve, Dalloz, 2017, p.52.
[1285] R. Legeais, *Les règles de preuve en droit civil. Permanences et transformations*, *op.cit.*, p.190.

recherche de preuve[1286]. Le juge a la possibilité de prendre un ensemble de mesures très variées lui permettant de chercher des preuves et ainsi d'accéder à une certaine vérité matérielle dans une affaire impliquant la technologie *blockchain*.

617. **Les faits pertinents enregistrés dans la *blockchain*.** Le juge a précisément la faculté de prendre en considération des faits que les parties n'ont pas spécialement invoqués[1287]. Ces faits sont puisés parmi la « *masse de faits* » allégués liée au procès (conclusion ou pièces produites)[1288]. Alors même que les parties n'auraient pas mis l'accent sur certains faits, le juge peut considérer, sélectionner les faits allégués qui lui apparaissent les plus pertinents, autrement dit « *les faits pertinents* » pour trancher le litige. Dans l'hypothèse où les parties n'auraient pas versé aux débats des preuves *blockchains* pour prouver certains faits, le juge pourra tout à fait envisager de prendre en compte des faits pertinents liés à des données enregistrées dans la *blockchain*.

618. **Les explications de fait.** Le juge peut demander également des explications de fait nécessaires à la solution du litige[1289]. Cette simple invitation n'est pas un pouvoir d'injonction[1290].

619. **Les mesures d'instruction ou d'enquête.** Aussi, le juge est en capacité d'ordonner la production de pièces ou des mesures d'instructions à la demande des parties[1291]. Et au-delà de l'initiative des parties, il peut ordonner d'office des mesures d'instruction ou d'enquête[1292]. Il sera même parfois tenu d'ordonner des mesures d'instruction. À tout moment le juge peut ajouter les mesures d'instruction nécessaires à celles déjà ordonnées ou étendre les mesures prescrites auparavant[1293]. À cette occasion, le juge ne pourra pas introduire de nouveaux faits dans le débat mais cette mesure pourra tout à fait faire évoluer les débats probatoires et susciter la discussion avec les parties sur les faits issus de l'instruction, non versés aux débats initialement. Dans le cadre d'un contentieux impliquant des faits dans une *blockchain*, le juge

[1286] J.-L. Mouralis, « Preuve : règles de preuve », *op.cit.*, n°34.
[1287] C. proc. civ., art. 7, al. 2 : « *Parmi les éléments du débat, le juge peut prendre en considération même les faits que les parties n'auraient pas spécialement invoqués au soutien de leurs prétentions* ».
[1288] S. Grignon Dumoulin, « L'office du juge civil dans la recherche de la preuve », *op.cit.*, p.52.
[1289] C. proc. civ., art. 8 et 765 (pour le juge de la mise en état).
[1290] S. Grignon Dumoulin, « L'office du juge civil dans la recherche de la preuve », *op.cit.*, p.52.
[1291] C. proc. civ., art. 11, 138, 142, 143.
[1292] C. proc. civ., art. 10, 143 et 771-5° (le juge de la mise en état).
[1293] C. proc. civ., art. 148, 149, 166.

devrait être particulièrement enclin à requérir des mesures d'instruction ou des enquêtes pour relever des éléments pertinents tracés dans le registre distribué.

620. **Les limites de la vérification personnelle.** D'autres investigations diverses sont à sa disposition, comme le fait de procéder à des vérifications personnelles[1294], d'ordonner la comparution personnelle des parties[1295], de recevoir des déclarations de tiers[1296], d'ordonner une enquête[1297], de prescrire des constatations, une consultation ou encore une expertise[1298]. La vérification personnelle de données dans la *blockchain* pourra sembler complexe en raison de l'absence de fioritures des registres sans interfaces utilisateurs, ne permettant pas un accès simple à un public non averti. Le juge pourra alors prescrire une expertise ou des constatations d'huissiers[1299].

621. **Le « *bon sens procédural* ».** Enfin, la jurisprudence a affirmé une obligation incombant au juge de procéder à des investigations lorsqu'une partie ne peut par elle-même obtenir un élément de preuve utile à la solution du litige. Par exemple, la Cour d'appel avait violé l'article 146 alinéa 2 du Code civil car elle avait refusé d'ordonner une expertise pour déterminer l'étendue du préjudice auquel les demandeurs ne pouvaient pas procéder eux-mêmes et qui ne pouvait être établi que par des recherches de pièces. Alors même que la preuve de la contrefaçon alléguée était rapportée en l'espèce, la chambre mixte statue sur la violation de la loi[1300]. Cette décision propose un enseignement clé dans la recherche de la preuve, c'est une forme de « *bon sens procédural* »[1301] dont le juge doit faire preuve dans sa coopération à l'établissement de la vérité quand les parties sont au bout de leur possibilité. Il est tout à fait probable qu'une partie n'ait pas accès à des preuves enregistrées dans la *blockchain* liées à des violations de droit de propriété intellectuelle. Dans la *blockchain* Bitcoin par exemple, sept fichiers liés à des contenus contrefaisants ou mettant en avant le potentiel de la *blockchain* Bitcoin pour des violations de *copyright* ont été constatés en mars 2018 par des chercheurs[1302]. Bien que la *blockchain* Bitcoin soit ouverte à la lecture, dans l'hypothèse où les parties ne pourraient pas

[1294] C. proc. civ., art. 179.
[1295] C. proc. civ., art. 184.
[1296] C. proc. civ., art. 199.
[1297] C. proc. civ., art. 204.
[1298] C. proc. civ., art. 232.
[1299] Voir *infra* n°745 et s.
[1300] Cass. ch. mixte, 6 juill. 1984, n°80-12.965.
[1301] S. Amrani Mekki, « Vers un droit commun de la preuve processuel », *in La preuve : regards croisés*, *op.cit.*, p. 119, n°12.
[1302] R. Matzutt, J. Hiller, M. Henze, J.-H. Ziegeldorf, « A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin », *op.cit.*, fevr. 2018, p.12.

avoir accès à ces fichiers - qu'ils soient hachés ou chiffrés -, le juge se devra de procéder à davantage d'investigations, et ne pourra refuser d'ordonner une expertise de ces fichiers.

622. En définitive, dans la recherche des preuves *blockchains* par le juge, la preuve de nature pénale accorde plus de pouvoir au juge et vient dynamiser sa recherche des preuves *blockchains*. Bien que le procès civil devienne mixte, on oppose encore volontiers traditionnellement la procédure civile accusatoire[1303] à la procédure pénale inquisitoire, donnant une parfaite illustration de cette différence. La procédure pénale inquisitoire accorde nécessairement au juge un rôle plus actif dans la recherche des preuves *blockchains* dans un contexte qui n'est pas sans défi sur le plan pratique, un domaine aux prises perpétuelles des cyber-délinquants. Seul le juge pénal dispose en outre d'un pouvoir de coercition lui permettant notamment de réaliser des perquisitions et des saisies sur des preuves *blockchains*[1304]. Alors que la loi et la jurisprudence confient une place de choix grandissante dans la recherche des preuves civiles - offrant au juge des opportunités dans la recherche de données dans la *blockchain* -, celle-ci aurait le mérite d'être approfondie, tout comme l'appréciation de ces preuves. L'absence de décision illustrant ces pouvoirs ne permet pas d'affirmer les contours de leur mise en œuvre concrète.

Section 2 : L'appréciation quasi-inexistante par le juge des preuves de données enregistrées dans la *blockchain*

623. Le pouvoir d'appréciation des preuves *blockchains* par le juge consiste à les examiner minutieusement afin d'être en mesure de se déclarer convaincu ou non de l'existence de faits allégués par les parties[1305]. Nous examinerons les pouvoirs d'appréciation du juge s'agissant de la preuve des données enregistrées dans la *blockchain* en théorie (paragraphe 1) ainsi que l'absence de positionnement des juges français sur ces preuves dans les faits (paragraphe 2).

[1303] S. Guinchard, C. Chainais, F. Ferrand, *Procédure*, Dalloz, 30e éd., 2010, n°55 ; L. Cadiet, E. Jeuland, *Droit judiciaire privé*, *op.cit.*, n°12 ; J. Héron, T. Le Bars, *Droit judiciaire Privé*, 3e éd., Montchrestien-Lextenso, Domat, Droit privé, 2006, n°245.
[1304] E. Jeuland, *Droit processuel général*, *op.cit.*, n°501.
[1305] J.-L. Mouralis, « Preuve : modes de preuve », *op.cit.*, n°598, p.73.

Paragraphe 1 : Les pouvoirs d'appréciation du juge s'agissant de la preuve des données enregistrées dans la *blockchain*

624. Le juge doit décider si les preuves débattues par les parties, incluant des preuves *blockchains*, l'ont amené à se forger une conviction. Ce qui importe pour le juge c'est de vérifier que la preuve des données enregistrées dans la *blockchain* présente des garanties suffisantes de sincérité[1306]. C'est à lui seul que revient la décision de la confirmation de la réalité ou du rejet d'un fait contesté. Il a donc une obligation de procéder à l'appréciation des preuves des données enregistrées dans la *blockchain* qui lui sont présentées[1307]. Partant, le juge dispose de pouvoirs inclus dans le cadre de l'appréciation de ces preuves (A) et d'autres exclus de son appréciation (B).

A. Les pouvoirs inclus dans l'appréciation du juge s'agissant des preuves de données enregistrées dans la *blockchain*

625. Pour forger sa conviction, le juge doit disposer d'une liberté totale afin d'apprécier que des faits existent ou non. Or, notre système de preuve fixe déjà des lois déterminant la valeur des procédés de preuve, ce qui apporte des limitations à son pouvoir d'apprécier les données enregistrées dans la *blockchain*. Nous explorons ainsi les cas de liberté du juge dans l'appréciation des preuves de données enregistrées dans la *blockchain* (1) et ceux de neutralité du juge dans l'appréciation de ces preuves (2).

1. La liberté du juge dans l'appréciation des preuves de données enregistrées dans la *blockchain*

626. Si le principe de la libre appréciation de la preuve de données enregistrées dans la *blockchain* se concentre en son point névralgique sur la notion de conviction (a), des cas peuvent aussi être déclinés pour les preuves *blockchains* (b).

[1306] Cour de cassation, Rapport annuel 2012, La preuve, p.88.
[1307] F. Ferrand, Preuve, *op.cit.*, n°537.

a. La conviction du juge dans l'appréciation des preuves de données enregistrées dans la *blockchain*

627. **Libre appréciation et conviction du juge.** Lorsque la preuve n'est pas légale, c'est le principe de liberté de la preuve qui l'emporte. Le cas échéant, le juge est libre d'apprécier la force probante des éléments de preuve de données enregistrées dans la *blockchain* qui lui sont soumis. Il s'agit de son « *intime conviction* »[1308] qui va le guider en matière pénale[1309], comme en matière civile[1310]. Si la loi ne détermine pas la force probante d'un mode de preuve, le juge se fie en effet à son « *intime conviction* » pour déterminer librement la valeur des preuves *blockchains* soumises par les parties. De nombreuses fois, l'accès à la vérité par le juge est plus une question de certitude[1311], de « *certitude intérieure* »[1312], c'est-à-dire une vérité purement subjective[1313].

628. **Le débat doctrinal sur la notion d'« *intime conviction* ».** Deux courants doctrinaux s'opposent sur la définition de l'intime conviction, celui axé sur la certitude de juge et celui davantage tourné sur une forte probabilité[1314]. D'un côté, l'intime conviction impliquerait une certitude du juge[1315] en ce que la partie qui a la charge de la preuve doit prouver les faits allégués jusqu'à les rendre certains. En cela, le juge ne pourrait fonder sa décision uniquement sur des faits avérés. Cette position repose sur les idées selon lesquelles le juge est interdit de se baser sur des motifs hypothétiques[1316] et le doute est préjudiciable à la partie qui supporte la charge de la preuve[1317]. De l'autre côté, l'intime conviction impliquerait une forte probabilité fondant

[1308] J.-D. Bredin, *Le doute et l'intime conviction*, Droits, 1996, p.21, n°23.
[1309] C. proc. pén., art. 427.
[1310] Exemple : Cass. 1ère civ., 16 juin 1998 : D. 1999, p.360, note J. Massip.
[1311] V. F. Hélié, *Traité de l'instruction criminelle ou théorie du Code d'instruction criminelle*, Tome IV, 2e éd., Plon, Paris, 1866, n°1759, p.324.
[1312] E. Vergès, « Éléments pour un renouvellement de la théorie de la preuve en droit privé », *in* Mélanges J.-H. Robert, LexisNexis, 2012, p.893. 108. Voir aussi les jurisprudences en ce sens : Cass. 2ème civ., 21 janv. 1993 : Bull. civ. II, n°28 ; Cass. 2ème civ., 28 juin 2006 : Bull. civ. II, n°174 ; Cass. 2ème civ., 5 avr. 2007 : Bull. civ. II, n°76.
[1313] M. Mekki, « Vérité et preuve. Rapport français », *op.cit.*, p.827, n°23.
[1314] E. Vergès, « La réforme du droit de la preuve civile: enjeux et écueils d'une occasion à ne pas manquer », D. n°10, 13 mars 2014, p.624.
[1315] J.- D. Bredin, *Le doute et l'intime conviction*, *op.cit.*, p.21, n°23. Critère de certitude repris formellement par la jurisprudence : Cass. 3ème civ., 18 mai 2011, n°10-17.645 : D. 2011. 1483, obs. I. Gallmeister, 2089, note M. Boutonnet, 2679, chron. A.-C. Monge, 2694, obs. F. G. Trébulle, 2891, obs. J.- D. Bretzner, et 2012. 47, obs. P. Brun ; RTD civ. 2011. 540, obs. P. Jourdain.
[1316] Cass. 1ère civ., 20 mai 1981, n°79-17.171.
[1317] Cass. 2ème civ., 4 juill. 2007, n°05-11.569.

la décision du juge[1318]. Cette position repose sur une approche pragmatique du syllogisme juridictionnel conforme à la pratique[1319]. Le projet Catala a proposé en vain d'adopter une conception souple de l'intime conviction dans la réforme du droit des obligations suggérant que le juge apprécie la valeur des preuves « *en conscience* », le projet ajoutait que « *dans le doute, le juge s'en tient à la plus forte vraisemblance* ». La notion de vraisemblance est d'ailleurs mentionnée par les articles 1316-2 et 1347 du Code civil ainsi que par la jurisprudence[1320]. Cette conviction du juge ne relève pas de l'arbitraire car elle doit reposer sur une vraisemblance[1321]. La vraisemblance est basée sur une légitimité de la probabilité[1322]. Ce standard s'appuie sur une probabilité de plus de 50 % et il s'éloigne de l'intime conviction.

629. Selon la première conception de l'intime conviction, si une hypothèse implique des moyens portant sur des données enregistrées dans la *blockchain*, le juge ne pourra pas se baser sur des motifs hypothétiques. S'il se base sur ces données mathématiques de la *blockchain*, elles ne seront pas hypothétiques en soi. Dans ce cas, la deuxième conception de la forte probabilité sera *a fortiori* satisfaite. En somme, avec les données enregistrées dans la *blockchain*, il sera aisé pour le juge de se conformer à la conception la plus exigeante de l'intime conviction, c'est-à-dire la première.

b. Les cas de libre appréciation des preuves de données enregistrées dans la *blockchain* par le juge

630. **Souveraineté du juge dans la détermination de la valeur et de la portée des preuves *blockchains*.** Les cas visés par la liberté de la preuve sont déclinés limitativement en partie préliminaire (les faits juridiques et les actes juridiques d'un montant inférieur à 1 500 euros en

[1318] C. Aubry, C. Rau, *Cours de droit civil français*, t. 12, *op.cit.*, p. 58. Une conception proche, C. Tournier, L'intime conviction du juge, PUAM, 2003, n[os] 135 s. Critère confirmé par la jurisprudence qui rejette l'exigence d'une preuve scientifique et admet que la preuve puisse reposer sur un faisceau d'indices constituant des présomptions du fait de l'homme : Cass. 1[ère] civ., 22 mai 2008, n°06-10.967, n°05-10.593, n°06-18.848 et n°06-14.952 : D. 2008. 1544, obs. I. Gallmeister, et 2894, obs. P. Jourdain ; RDSS 2008. 578, obs. J. Peigné; RTD civ. 2008. 492, obs. P. Jourdain ; RTD com. 2009. 200, obs. B. Bouloc ; JCP 2008. II. 10131, note J.- L. Grynbaum.
[1319] E. Vergès, « La réforme du droit de la preuve civile: enjeux et écueils d'une occasion à ne pas manquer », *op.cit.*, p.624.
[1320] Cass. 3[ème] civ., 3 févr. 1993 : Bull. civ. III, n°14.113.
[1321] J. Carbonnier, *Droit civil, Introduction, op.cit.*, n°28, p.76 ; D. Ammar, *Preuve et vraisemblance. Contribution à l'étude de la preuve technologique*, RTD civ., 1993, p.501 et s. ; C. Puigelier, « Vrai, véridique et vraisemblable », *in* La preuve, ss. dir. C. Puigelier, Economica, 2004, p. 195 et s.
[1322] R. Perrot, obs. sous Cass. civ., 29 mai 1951 : JCP G, II, 6421 ; C. Aubry, C. Rau par E. Bartin, *Cours de droit civil français selon la méthode de Zachariae*, *op.cit.*, §749, p.84, note 19b.

matière civile, et en matière pénale). Dans toutes ces hypothèses, le juge sera libre d'apprécier la valeur et la portée d'une preuve *blockchain* relatant un fait ou un acte. Celles-ci seraient ainsi probablement admises par le juge[1323]. Le Ministère de la Justice abonde en ce sens, confirmant que ces preuves peuvent légalement être produites en justice[1324]. Le juge devra évaluer leur valeur probante, sans pouvoir les écarter au seul motif qu'elles seraient numériques[1325]. Notons que la preuve d'un fait positif enregistré dans la *blockchain* sera toujours préférable, et préférée par le juge, à celle d'un fait négatif[1326]. Il sera plus aisé d'apporter la preuve de l'antériorité par un enregistrement de la *blockchain* que de démontrer le fait qu'un prétendu contrefacteur ne dispose pas de l'antériorité. Si la souveraineté du juge est pleine dans la détermination de la valeur et de la portée des preuves *blockchains*, celles-ci n'auront pas *a priori* de force supérieure à d'autres éléments de preuve selon la magistrate Sophie Canas[1327].

631. **Présomptions judiciaires.** Le juge pourra toujours s'adonner à la pratique de la présomption judiciaire puisque dans ces cas de liberté d'appréciation, la loi admet la preuve par tout moyen en conformité avec l'article 1382 du Code civil. C'est un moyen pour celui-ci de tirer d'un fait inconnu, un fait connu dont l'existence est rendue vraisemblable[1328]. Cette présomption judiciaire sera conditionnée toutefois à sa gravité, sa précision et sa concordance.

632. **Preuves indiciaires.** Les labels projetés ci-avant[1329], une mesure d'instruction[1330], une expertise[1331], un constat d'huissier[1332], des attestations ou documents délivrés par des tiers[1333],

[1323] A propos de la preuve de la contrefaçon : « La preuve de la contrefaçon ou à l'inverse de l'authenticité du bien par la *blockchain* est parfaitement admissible devant le juge » (M. Malaurie-Vignal, « Blockchain et propriété intellectuelle », Prop. Ind. n°10 étude 20, oct. 2018, n°19).
[1324] Question écrite n°22103 de D. Fasquelle, publiée au JO le 30/07/2019, réponse du Ministère de la Justice publiée au JO le 10/12/2019, p.10774. Voir annexe n°10.
[1325] *Ibid*.
[1326] Sur le fait négatif voir : J. Larguier, « La preuve d'un fait négatif », RTD civ. 1953, p. 1 et s.
[1327] S. Canas, « Blockchain et preuve : le point de vue du magistrat », Dalloz IP/IT, févr. 2019, p.84. Voir aussi : M. Malaurie-Vignal, « Blockchain et propriété intellectuelle », *op.cit.*, n°19.
[1328] G. Cornu, *Vocabulaire juridique*, *op.cit*., Voir présomption, p.798.
[1329] Voir *supra* n°543 et s.
[1330] Cass. 2ème civ., 9 janv. 1974 : Bull. civ. II, n°12 ; Cass. 2ème civ., 30 janv. 1974 : JCP 1974, IV, 93 ; Cass. 2ème civ., 2 mai 1974 : JCP 1974, IV, 220 ; Cass. com., 4 févr. 1975 : JCP 1975, IV, 97 ; Cass. soc., 18 mars 1975 : Bull. civ. V, n°154 ; JCP 1975, IV, 154 ; Cass. 1ère civ., 22 avr. 1975 : JCP 1975, IV, 181 ; Cass. 3ème civ., 23 avr. 1975 : JCP 1975, IV, 183 ; Cass. 1ère civ., 28 mai 1975 : Bull. civ. I, n°181 ; JCP 1975, IV, 232 ; Cass. crim., 28 oct. 1975 : Bull. crim. n°228 ; D. 1975, IR, p. 247 ; Cass. 1re civ., 14 janv. 1976 : JCP 1976, IV, 76 ; Cass. com., 15 mars 1976 : JCP 1976, IV, 164 ; Cass. soc., 31 janv. 1979 : Bull. civ. V, n°90 ; Cass. 1ère civ., 14 mai 1985 : JCP 1985, IV, 260 ; Cass. soc., 8 nov. 1989 : JCP 1990, IV, 3 ; Cass. 1ère civ., 12 janv. 1994 : Bull. civ. I, n°14 ; D. 1994, p. 449, note J. Massip.
[1331] C. pr. civ., art. 263.
[1332] Cass. 2ème civ., 12 mars 1975 : Bull. civ. II, n°90 ; JCP 1975, IV, 6551, p.328.
[1333] C. pr. civ., art. 11, 138, 199 à 203.

des registres ou papiers domestiques[1334], ainsi que les traces numériques[1335], seront autant de preuves indiciaires à considérer par le juge.

633. **Données de la *blockchain* « *certaines* » et analyse scientifique.** En amont du jugement, le juge accède donc à l'intime conviction que les données de la *blockchain* sont dites « *certaines* ». Il convient pour cela qu'il fasse preuve d'une analyse scientifique afin de déterminer si ces données techniques sont certaines ou non. Cette démarche pourra sembler fastidieuse car le magistrat devra vérifier la qualité de la personne qui a enregistré ces données et le contenu qu'elle a enregistré, du moins si la *blockchain* le permet. S'agissant de la vérification du contenu, il pourra s'agir, par exemple, pour un ancrage, de s'assurer de la justesse des données ancrées dans la *blockchain* avec les données initiales. C'est donc aussi au plaideur qu'il appartiendra de redoubler d'effort dans la présentation de ses preuves pour faciliter l'analyse scientifique du juge afin qu'il accède à l'intime conviction que lesdites données de la *blockchain* sont certaines.

634. **Limites à la libre appréciation.** La liberté d'appréciation n'équivaut pas à l'arbitraire. Le juge devra notamment respecter des règles de motivation des décisions de façon logique et suffisante[1336]. Il existe d'autres limites à la libre appréciation des juges du fond établies par le contrôle de dénaturation de la Cour de cassation[1337]. En vue de vérifier l'absence d'interprétations controversées, les juges de cassation interviennent dans le dessein de déterminer d'éventuelles dénaturations commises par le juge du fond. Ces derniers doivent se garder d'interprétations dites « *dénaturantes* », en d'autres termes, les interprétations qui méconnaissent la lettre claire et précise des actes. Ce contrôle est souvent mis en œuvre par les chambres civiles[1338] et commerciales de la Cour[1339].

[1334] Cass. req., 16 mars 1909 : DP 1909, I, p. 343 ; Cass. req., 2 févr. 1927 : DH 1927, p.113 ; Cass. 1ère civ., 6 oct. 1958 : D. 1958, p.747 ; a contrario : Cass. com., 18 mars 1969 : D.1969, p.514.
[1335] Cass. 1ère civ., 28 mars 2000 : D. 2000, p.276, obs. J. Faddoul.
[1336] J.-L. Mouralis, « Preuve : modes de preuve », *op.cit.*, n°616, p.75.
[1337] Cass. civ., 15 avril 1872, arrêt Veuve Foucauld et Coulombe c. Pringault.
[1338] Cass. 1ère civ., 5 avril 2012, n°10-24.991 : concernant des documents probatoires (attestations).
[1339] Com., 19 juin 2012, n°11-13.176 : *Bull.* 2012, IV, n°132 : concernant la dénaturation des écritures des parties ; Com., 24 mai 2011, n°10-24.869 : *Bull.* 2011, IV, n°80 : concernant un rapport d'expertise.

c. Les cas de conflits de preuves *blockchains*

635. **La règle des conflits de preuve par écrit.** À la lecture de l'article 1368 du Code civil, c'est « *à défaut de dispositions ou de conventions contraires,* (que) *le juge règle les conflits de preuve par écrit en déterminant par tout moyen le titre le plus vraisemblable* ». Celui-ci pourra déterminer, hors des cas visés, le titre le plus vraisemblable entre plusieurs preuves *blockchains* ou entre une preuve *blockchain* contre une preuve non *blockchain*.

636. **Le champ du conflit de preuves *blockchains*.** Ce n'est pas la recevabilité des preuves qui sera en jeu mais « *(…) la foi due aux preuves recevables* »[1340], qu'elles soient parfaites ou imparfaites. En effet, la réforme du droit des contrats dans la formulation de ce nouvel article 1368 retient que le juge règle les conflits de preuve « *par écrit* », abandonnant la mention des conflits de preuve « *littérale* ». Cet abandon suscite l'attention puisque le législateur ne semble plus restreindre les conflits de preuve aux seuls écrits parfaits. Cette ouverture des conflits de preuve aux écrits imparfaits laisse au juge l'opportunité de se prononcer également sur les conflits de preuve impliquant un commencement de preuve par écrit. En cela, le juge pourrait être amené à régler des conflits de preuve impliquant des écrits parfaits comme une inscription de minibons, une empreinte, un acte sous-jacent à celle-ci, ou des écrits imparfaits comme des données transactionnelles quelconques (incluant des transactions complexes) ou d'autres données complémentaires.

637. **Les applications du conflit de preuves *blockchains*.** Une expertise pourra tout à fait trancher les discussions en cas de conflit entre deux écrits impliquant au moins un écrit et un support *blockchain*[1341]. Si l'un d'eux n'est pas fiable, son détenteur succombera mais si les deux écrits sont établis conformément aux exigences légales, le juge sera libre de retenir le plus vraisemblable[1342]. En pratique, plusieurs scénarii de conflit de preuves avec la *blockchain* peuvent être envisagés : une preuve *blockchain* contre une autre *blockchain* de même nature, une preuve *blockchain* contre une autre de nature différente, et une preuve *blockchain* contre preuve non *blockchain*.

[1340] A. Raynouard, « Adaptation du droit de la preuve aux technologies de l'informatique et à la signature électronique », *op.cit.*, p.600, n°19.
[1341] Voir *infra* n°793 et s. sur l'objet de l'expertise.
[1342] L. Grynbaum, Fasc. 10 : La preuve littérale, JCl. Civil Code – Art. 1316 à 1316-4, *op.cit.*, n°36.

638. **Preuve *blockchain* contre preuve *blockchain* de même nature.** L'hypothèse selon laquelle les parties produiraient des preuves *blockchains* de même nature, comme deux empreintes numériques, pourra mettre le juge à rude épreuve quant à la sélection de la plus vraisemblable. Au regard du caractère cryptographique de ces deux preuves, il y a peu de chance que celles-ci expriment un contenu contradictoire puisqu'une fonction de hachage identique appliquée aux mêmes ensembles de données produit un résultat parfaitement équivalent. En revanche, ce qui pourra peser dans l'appréciation du titre le plus vraisemblable sera le registre utilisé pour procéder à l'ancrage. Si les registres sont différents, la résilience du réseau et les algorithmes utilisés seront de nature à influer sur la fiabilité des données qui y sont enregistrées.

639. **Preuve *blockchain* contre preuve *blockchain* de nature différente.** L'hypothèse selon laquelle les preuves *blockchains* seraient de natures différentes et impliqueraient des registres différents, comme une transaction complexe et un acte sous-jacent à une empreinte, soulèvera sans doute des difficultés moindres. En fonction de la qualification retenue du mode de preuve et de sa force probante, le juge déterminera le titre le plus vraisemblable. La fiabilité des preuves *blockchains* en cause est un facteur qui entrera aussi en compte.

640. **Preuve *blockchain* contre preuve non *blockchain*.** Enfin, l'hypothèse selon laquelle une preuve *blockchain* est confrontée à une preuve sur un support autre que la *blockchain* pourrait aussi soulever moins de difficultés et la tendance à la vraisemblance de la preuve cryptographique pourrait être affichée de manière presque axiomatique. Cependant, la vigilance devra être de mise dans le cadre des réseaux peu résilients et moins fiables.

641. Par ailleurs, le juge ne pourra pas se contenter de faire prévaloir un écrit sur support physique, comme un support papier, sur un écrit sur support *blockchain* en raison uniquement de son support conformément à l'article 1366 du Code civil qui précise que « *l'écrit électronique a la même force probante que l'écrit sur support papier (…)* ». Le conflit de support de preuve plutôt que de la preuve elle-même ne peut raisonnablement être envisagé par un plaideur. Toute idée de prééminence d'un écrit sur un autre en raison de son support est donc écartée[1343].

642. Ce sont donc à première vue davantage des conflits entre deux preuves *blockchains* identiques de registres différents, ou deux preuves *blockchains* de natures différentes et de

[1343] A. Raynouard, « Adaptation du droit de la preuve aux technologies de l'informatique et à la signature électronique », *op.cit.*, p.600, n°19.

registres différents, ou encore une preuve sur support *blockchain* et l'autre sur un support extérieur à la *blockchain*, qui pourront être aisément résolus si tant est qu'un expert intervienne. Rien n'est moins sûr s'agissant des conflits de preuves *blockchains* soumis et résolus par les seules réflexions du juriste.

2. La neutralité du juge dans l'appréciation des preuves de données enregistrées dans la *blockchain*

643. **Neutralité d'appréciation des preuves *blockchains*.** La liberté du juge dans l'appréciation souveraine des faits doit être nuancée par les règles impératives encadrant l'administration de la preuve[1344]. Dans ces cas, le juge sera soumis à un principe de neutralité dans son appréciation des preuves de données enregistrées dans la *blockchain*. La conviction personnelle du juge est ici sans importance, c'est « *l'automatisme de la preuve (qui) est précisément l'effet recherché* »[1345]. La preuve *blockchain* en cause liera ainsi le juge.

644. **Le juge ne peut pas apprécier librement les données enregistrées dans la *blockchain* si la preuve est légale.** Il existe une hiérarchie légale entre les modes de preuve qui lie le juge par la force probante afférente à ces modes de preuve définis par la loi. Lorsque la loi déclare qu'un procédé de preuve fait foi sous certaines conditions déterminées, le pouvoir d'appréciation du juge se contente du contrôle de l'existence de ces conditions dans le cas d'espèce soumis[1346]. Il lui est alors interdit de rejeter la réalité d'un fait que la loi aurait réputé établie[1347]. La neutralité du juge dans l'appréciation des preuves établies par la loi permet d'être fixé définitivement sur la valeur des titres et d'être à l'abri des contestations postérieures[1348].

645. Les modes de preuve actuels ne visent pas le support de la *blockchain* pour l'heure, sauf la preuve de l'inscription des minibons dans le DEEP qui est assimilée à un écrit sous signature privée[1349]. L'inscription de minibons nécessite pour être prouvée d'apporter au juge la preuve

[1344] Cour de cassation, Rapport annuel, La preuve, *op.cit.*, p.115.
[1345] J. Normand, *Le juge et le litige*, thèse Paris, coll. Bibliothèque de droit privé, 1965, n°292.
[1346] J.-L. Mouralis, « Preuve : modes de preuve », *op.cit.*, n°612, p.75.
[1347] Cass. 3ème civ., 8 déc. 1971, Bull. civ. III, n°617.
[1348] R. Legeais, *Les règles de preuve en droit civil. Permanences et transformations*, *op.cit.*, p.94.
[1349] C. mon. fin., art. 223-13, al.1.

de cet acte. Dans cette hypothèse, le juge n'aura pas à apprécier la preuve de l'inscription mais simplement à contrôler son existence.

646. **Critiques de la preuve *blockchain* contredisant la vérité.** Certaines critiques ont pu être émises puisque « *même convaincu de la mauvaise foi du plaideur qui lui présente l'écrit probatoire, le juge doit lui donner raison ; même convaincu qu'à raison celui qui n'a pas la preuve exigée par la loi, le juge doit lui donner tort* »[1350]. Le Professeur Etienne Vergès déplore fort justement qu'une preuve inexacte ayant une force probante établie par la loi pourrait contredire la vérité[1351]. Par exemple, si tant est qu'un *smart contract* soit reconnu comme un acte sous seing privé dans une certaine situation (dans une convention de preuve par exemple), les biais, fautes, et erreurs, dans la saisie et programmation de ce *smart contract* pourraient conduire à une vérité erronée qui fera foi jusqu'à preuve du contraire et à laquelle le juge sera quand même tenu. Ce dernier devra donc donner pleine foi à cet écrit sous signature privée au détriment de la vérité. Dès lors, consacrer des modes de preuve légaux aux procédés ou aux données enregistrées dans la *blockchain* n'est pas sans risque.

647. **Appréciation en droit américain des preuves *blockchains*.** Si dans l'ensemble le juge français est soumis à une neutralité qui s'avère inflexible lorsque la preuve *blockchain* est légale, le juge américain n'est pas plus libre. Avec la marge d'appréciation serrée des textes fédéraux par le juge, la position américaine sera probablement plus rigoureuse, sauf dans les États où la loi est favorable à l'admission et à la recevabilité des preuves *blockchains*[1352].

648. La *Federal Rules of Evidence* impose comme principe de base l'usage de la « *meilleure preuve* » au procès[1353]. Ce principe de la meilleure preuve exige la production de la preuve originale au tribunal lorsque cela est pertinent. Selon l'article 1002 de la *Federal Rules of Evidence*, est exigé « *un écrit original, un enregistrement ou une photographie pour prouver son contenu, sauf si ces règles ou une loi fédérale prévoit le contraire* ». Les enregistrements dans la *blockchain* aux États-Unis pourront être considérés comme des originaux si tant est que la multiplication des registres sur le nombre de nœuds présent n'en soit pas un obstacle.

[1350] P. Stoffel-Munck, P. Malaurie, L. Aynès, *Droit des obligations*, *op.cit.*, n°558.
[1351] E. Vergès, « La réforme du droit de la preuve civile: enjeux et écueils d'une occasion à ne pas manquer », *op.cit.*, p.624.
[1352] Des auteurs sont d'avis que dans certains états, notamment celui du Vermont, les preuves *blockchains* sont admissibles sans l'application des lois fédérales (G. Autrey, G. Marchant, « Admissibility of *Blockchain* Evidence », Arizona State University - College of Law, nov. 2018, p.3).
[1353] FRE, 1002.

649. De surcroît, pour être admises par le juge américain, les preuves *blockchains* devraient pouvoir répondre à la définition de « *hearsays* » (ou preuve par ouï-dire) conformément à la *Federal Rules of Evidence*[1354], c'est-à-dire une déclaration extrajudiciaire orale ou écrite par un déclarant et rapportée pour établir la véracité de la thèse d'une partie[1355]. Il se pourrait cependant que les juges n'admettent pas la qualification de *hearsay* pour des informations produites et générées automatiquement par ordinateur[1356], en témoigne l'affaire dite « *U.S. v. Lizarraga-Tirado* » au sujet d'images satellites de Google Earth[1357]. La plupart des preuves *blockchains* pourraient ainsi ne pas être recevables par *hearsay.* Mais nonobstant leur recevabilité, elles pourraient entrer dans le cadre d'une exception de *hearsay* des registres commerciaux[1358], des registres publics[1359], ou encore des registres de souvenirs[1360].

B. Les pouvoirs exclus de l'appréciation du juge s'agissant des preuves de données enregistrées dans la *blockchain*

650. **Les règles.** Les preuves *blockchains* sont dans certains cas totalement exclues de l'appréciation du juge lorsqu'elles portent sur des faits en dehors du débat. La règle selon laquelle le juge ne peut pas se prononcer sur des faits en dehors du débat est un principe directeur du procès visé au premier alinéa de l'article 7 du Code de procédure civile précisant que « *le juge ne peut fonder sa décision sur des faits qui ne sont pas dans le débat* ». Cette règle est complétée par l'article 5 du Code de procédure civile qui expose que « *le juge doit se prononcer sur tout ce qui est demandé et seulement ce qui est demandé* ». Celui-ci peut toutefois

[1354] J. Ching, Is *Blockchain* Evidence Inadmissible Hearsay? », janv. 2016, http://www.law.com/sites/jamesching/2016/01/07/is-blockchain-evidence-inadmissible-hearsay/ (consulté le 31/05/2020) ; A. Guo, « Blockchain Receipts : Patentability and Admissibility in Court », Chicago-Kent Journal of Intellectual Property Volume n°16, Issue n°2, Article 9, june 2017, p.444 ; G. Autrey, G. Marchant, « Admissibility of Blockchain Evidence », Arizona State University - College of Law, nov. 2018, p.17.
[1355] FRE, 801 (c) (1), (2).
[1356] A. Guo, « Blockchain Receipts : Patentability and Admissibility in Court », *op.cit.*, p.445-448 ; D. J. Neally, M. L. Hodg, « Blockchain in the Courts », Center for Law, Science and Innovation, Sandra Day O'Connor College of Law Arizona State University, nov. 2018, p.11 ; G. Autrey, G. Marchant, « Admissibility of *Blockchain* Evidence », *op.cit.*, p.21.
[1357] US v. Lizarraga-tirado, Case No. 13-10530 (9th cir. 2015).
[1358] FRE, 803 (6), (7). Voir de cet avis : A. Guo, « Blockchain Receipts : Patentability and Admissibility in Court », Chicago-Kent Journal of Intellectual Property Volume n°16, Issue n°2, Article 9, le 21/06/2017, p.448.
[1359] FRE, 803 (8), (10).
[1360] FRE, 803 (5).

prendre en considération dans les éléments du débat, les faits adventices, c'est-à-dire les faits non spécialement invoqués par les parties[1361].

651. **Les raisons.** En tout état de cause, le juge ne peut pas prendre des initiatives en dehors du champ fixé par les parties[1362] car cela reviendrait à redéfinir la matière du litige et porterait atteinte à son immuabilité[1363]. Le principe dispositif guide l'idée selon laquelle seules les parties ont le soin de délimiter leur matière litigieuse. Le juge ne doit pas modifier les termes du litige que les parties lui ont soumis[1364]. Il n'est en effet pas censé intervenir dans le domaine du fait, sauf à rompre l'égalité des parties devant la justice et ainsi porter atteinte à la neutralité dont il fait preuve en principe. S'il se mêlait des faits de l'une ou l'autre partie, cela pourrait revenir à soutenir les intérêts d'une partie[1365]. Le juge ne peut pas non plus faire état d'éléments de connaissance personnelle[1366]. Il lui est interdit d'apporter de nouveaux éléments au débat[1367].

652. **L'application aux preuves de données enregistrées dans la *blockchain*.** Dans une affaire portant sur des faits précis et une matière litigieuse délimitée par les parties, quand bien même un registre de *blockchain* pourrait être public, le juge ne pourra faire état des données de ce registre, si elles portent sur des faits en dehors du débat. Celui-ci ne pourra pas non plus apporter d'éléments de connaissance personnelle sur la technologie, même s'il pense suffisamment les maîtriser.

Paragraphe 2 : L'absence de positionnement formel des juridictions françaises sur les preuves de données enregistrées dans la *blockchain*

653. Si les juges français n'ont pas eu à connaître un litige portant directement sur des preuves de données enregistrées dans la *blockchains* et n'ont pas eu en conséquence l'opportunité d'apprécier ces preuves de données enregistrées dans la *blockchain* (A), ce n'est

[1361] C. proc. civ., art. 7, al.2.
[1362] S. Grignon Dumoulin, « L'office du juge civil dans la recherche de la preuve », *op.cit.*, p.51.
[1363] *Ibid.*, p.52.
[1364] *Ibid.*, p.51.
[1365] *Ibid.*, p.52.
[1366] *Ibid.*, p.51.
[1367] Cass. 1ère civ., 21 nov. 2006, n°05-11.607 : Bull. civ. I, n°505 ; D. 2007. 152, obs. X. Delpech ; AJDI 2007. 46 ; Cass. 2e civ., 6 janv. 2012 n°10-27.737 ; Soc. 5 déc. 2012, n°11-21.113 : Bull. civ. V, n°325 ; Cass. 3e civ.,19 mai 2015, n°14-14.881.

pas le cas de certains juges chinois qui ont dû statuer sur une affaire liée à cette thématique portée devant la *Hangzhou Internet Court* (B).

A. L'absence de positionnement des juges français sur l'appréciation des preuves de données enregistrées dans la *blockchain*

654. **Absence de décision judiciaire française.** En France, aucune décision judiciaire n'est à notre connaissance recensée à ce jour tant sur la confirmation processuelle de l'admissibilité des preuves *blockchains*, que sur une prise de position au fond sur leur valeur (par une qualification juridique) et leur portée (par une détermination de leur force probante). La recevabilité de ces preuves qui auraient pu convaincre le juge n'en est pas plus abordée.

655. Les juges auraient pu néanmoins avoir à connaître et apprécier des pièces apportées à un dossier de plaidoirie, et d'autres preuves versées au débat ou rassemblées lors de la phase d'instruction du dossier qui auraient trait à un enregistrement dans la *blockchain*.

656. Vraisemblablement c'est surtout sur le manque de preuves que deux jugements du Tribunal de Commerce de Paris du 26 février 2020[1368] et du Tribunal de Grande Instance de Paris du 20 juin 2017[1369] nous orientent. Aussi, des preuves renvoyant indirectement à des données enregistrées dans une *blockchain* ou à des éléments liés à la technologie *blockchain* sont des pièces qui ont déjà été versées aux débats dans une décision dite « *Macaraja* » de la deuxième chambre du Tribunal de Commerce de Créteil en date du 6 décembre 2011[1370]. Nous ne sommes donc pas en mesure de confirmer que le juge a conforté l'admissibilité de preuves *blockchains*. En l'absence de dispositif clair d'un jugement - voire d'un attendu de principe - étayé par des motifs, il n'est pas possible de considérer avec certitude et sérieux les balbutiements d'un positionnement des juridictions judiciaires françaises sur le sujet.

[1368] T. com. Nanterre, 26 févr. 2020, n°2018F00466, BitSpread c/ Paymium : com. G. Marraud des Grottes, RLDI n°168, p.49-51 ; com. L. Costes, RLDI n°168, p.40 ; com. M. Julienne, JCP E n°19, p.41-44 ; N. Mathey, LEDB avr. 2020, p.1.
[1369] TGI Paris, Référés, 20 juin 2017, n°17/55291.
[1370] TC Créteil, 2ème ch., 6 déc. 2011, n°2011F00771. Confirmé : CA Paris, 26 septembre 2013, n°12/00161 : JurisData n°2013-024887 ; RDBF 2014, comm. 3, obs. F.-J. Crédot et T. Samin ; JCP E 2014, 1091, note Th. Bonneau.

657. **Les preuves indirectes d'enregistrement de données dans la *blockchain*.** Dans la décision du Tribunal de Commerce de Créteil du 6 décembre 2011, différentes pièces liées à des enregistrements dans une *blockchain* avaient été apportées par le demandeur, la SAS Macaraja, et le défendeur, le Crédit industriel et commercial (CIC). Dans cette affaire, la société Macaraja, qui avait pour activité la commercialisation de logiciels et plus généralement toute activité liée à l'informatique, décida d'ouvrir un compte de dépôt au CIC pour étendre ses activités. Ce nouveau champ d'activité portait sur de l'intermédiation de commerce pour la société Tibanne gérant une plateforme d'échange de bitcoins. Ce compte de dépôt ouvert au CIC permettait alors de sécuriser les opérations d'achat et de vente de bitcoins par la réception des fonds des vendeurs de bitcoins et le reversement aux acheteurs après vérification sur la plateforme d'échange de la réalisation de l'achat et de la livraison effective par le vendeur. À la suite de la constatation de nouveaux flux sur ce compte de dépôt et l'interrogation de son client, le CIC décida de mettre un terme aux relations commerciales avec la société Macaraja et clôtura son compte à l'expiration du délai de préavis de deux mois. La société Macaraja décida alors de saisir la Banque de France afin d'obtenir la désignation d'une banque dans le cadre de la procédure du « *droit au compte* ». Cette institution désigna la Société Générale avant de désigner, à nouveau, le CIC. Après une procédure en référé, le Tribunal de Créteil fut saisi par la société Macaraja sur les principales questions de nature du bitcoin (qualification ou non de monnaie électronique), de nature de l'activité de la Société Macaraja (une fourniture de services de paiements ou pas), sur la régularité de la clôture du compte par le CIC et sur son droit au compte. Au soutien des prétentions des parties, de nombreuses pièces ont été produites en lien avec la *blockchain*, c'est à ce titre que cette affaire attire particulièrement notre attention. Parmi elles, des pièces ont été communiquées par la société Macaraja au sujet des différents flux sur le compte de dépôt, notamment des e-mails et courriers justifiant ou demandant des virements effectués pour des opérations en lien avec son activité d'intermédiaire de commerce de plateforme d'échange. Le sous-jacent de ces flux n'était donc pas le bitcoin et ce n'était pas le registre directement qui était présenté comme pièce mais c'est bien l'objet de l'opération qui concernait le bitcoin. Une autre pièce qui a été versée par la société Macaraja intéresse également les preuves blockchains, un CD.R portant sur des logiciels (« *bitcoins-0.3.24-win32-setup.exe* » et « *bitcoin-0.3.21-win.32setup.exe* ») permettant de « *générer des bitcoins* », autrement dit de miner. Pour ce qui est du défendeur, de simples liens hypertextes témoignent du rapport indirect avec les preuves *blockchains* comme le site Internet « *http//bitcoin.fr* » définissant les bitcoins, « *https//fr.bitcoinit/wiki/trade* » listant les sites marchands acceptant les bitcoins, ou encore « *http//bitcoincharts.com/markets/* » regroupant

les données de marché de différentes plateformes d'échange de bitcoins dont celles de l'affaire. L'ensemble de ces pièces nous conforte sur la connaissance indirecte de ces preuves par le juge et ainsi une possible « *qualité* » des décisions de justice rendues en la matière[1371].

658. **Les preuves *blockchains* insuffisantes.** La décision du Tribunal de Commerce de Nanterre du 26 février 2020 statue en partie sur le manque de preuve d'une transaction en bitcoins[1372]. Cette affaire mettait en cause la société Bitspread, spécialisée dans le conseil en matière financière, précisément dans le domaine des crypto-monnaies, et la société Paymium exerçant une activité de plateforme d'échange de *bitcoins.* La société Bitspread avait ouvert un compte sur la plateforme de la société Paymium et celle-ci avait consenti trois contrats de prêt en bitcoins à la société Bitspread, pour un montant s'élevant à 1 000 bitcoins (avec intérêt au taux de 5 %). La société Paymium avait aussi accordé un prêt sans intérêt de 200 000 euros à la société Bitspread dans l'objectif de financer des prestations de tenue de marché en bitcoins sur la plateforme. Un contentieux apparaît entre ces deux protagonistes. La société Paymium décide de clôturer le compte de la société Bitspread. Celle-ci assigne alors la société Paymium devant le Tribunal de commerce de Nanterre. Ce Tribunal conclut en partie sur le rejet de la demande de restitution de 1 000 bitcoins à la Société Paymium, notamment faute de preuve de l'ensemble des préjudices allégués. Elle n'apportait pas non plus la preuve que 1 000 bitcoins avaient bien été transférés à Bistread lors du *hard fork* de bitcoin du 1er aout 2017. Cette décision met ainsi en exergue une position du juge du Tribunal de Commerce de Nanterre encline à recueillir et analyser des enregistrements de transactions en bitcoins dans le registre de la *blockchain* Bitcoin, mais la preuve de ces enregistrements en question faisait en l'espèce défaut. Par ailleurs, notons que ces juges ont été particulièrement attentifs à l'aménagement contractuel des parties dans l'hypothèse de *fork*, considéré dans ce cas comme insuffisant pour des professionnels avertis du secteur des crypto-actifs[1373].

659. **Les preuves *blockchains* indirectes insuffisantes.** Dans une décision du Tribunal de Grande Instance de Paris du 20 juin 2017[1374], les juges du fond ont également souligné

[1371] Sur la notion de « qualité des décisions de justice » voir : H. Colombet, A. Gouttefangeas, « La qualité des décisions de justice. Quels critères ? », Droit et et société 2013/1 n°83, p.155-176.
[1372] T. com. Nanterre, 26 févr. 2020, n°2018F00466, BitSpread c/ Paymium : com. G. Marraud des Grottes, RLDI n°168, p.49-51 ; com. L. Costes, RLDI n°168, p.40 ; com. M. Julienne, JCP E n°19, p.41-44 ; N. Mathey, LEDB avr. 2020, p.1.
[1373] Voir *infra* n°691 la proposition de contractualisation dans l'hypothèse de *fork*.
[1374] TGI Paris, Référés, 20 juin 2017, n°17/55291.

l'insuffisance de pièces concernant le caractère innovant et technologiquement avancé de la *blockchain*. Aucune pièce n'avait ici été versée au débat concernant ce caractère innovant, ce qui n'avait pas permis au juge des référés d'apprécier l'introduction de cette nouvelle technologie. Les faits de cette affaire ne portaient pas sur un contentieux informatique mais sur une question de droit social pour laquelle le comité d'établissement et le comité d'hygiène, de sécurité et des conditions de travail avaient été consultés sur le « *projet Ambition 2020* » de la Banque de France. Lors d'une réunion, le comité d'établissement avait adopté une résolution aux termes de laquelle il indiquait souhaiter recourir à un expert au sens des articles L2323-29 et L2325-38 du Code du travail et avait désigné un cabinet à cet effet. Par courrier, la Banque de France avait informé ledit cabinet qu'elle s'opposait à la mesure d'expertise et ne pouvait donc donner une suite favorable. Le comité d'établissement, autorisé par ordonnance, a par acte d'huissier de justice fait assigner la Banque de France devant le président du Tribunal de grande instance de Paris statuant en la forme des référés. Un des motifs relève qu'au regard des « *pièces versées aux débats qu'il s'agisse des procès-verbaux de réunion du comité central d'entreprise et du comité d'établissement ou des documents remis en vue de ces réunions, il n'est pas établi que le projet Ambitions 2020 constitue un projet suffisamment élaboré d'introduction de nouvelles technologies* » puisqu'en effet « *si certaines des actions du projet devant être mises en œuvre au sein des directions du siège renvoient à des notions impliquant l'utilisation de technologie, non seulement, le comité d'établissement ne rapporte pas la preuve que les technologies en cause présentent toutes un caractère de nouveauté (…) mais surtout celles-ci sont évoquées de façon générale sans précisions sur les outils ou techniques devant être utilisées et il n'est généralement fait état que de réflexions* ». S'agissant particulièrement de la technologie « *(…) « blockchain » son expérimentation est en cours au sein de la direction des services bancaires et son extension n'est pas encore décidée* ». Dans ces conditions, le Tribunal de Grande Instance a débouté le comité d'établissement de l'intégralité de ses demandes et annulé la résolution adoptée par ce dernier désignant le cabinet en qualité d'expert. En tout état de cause, aucune pièce concernant le caractère innovant et technologiquement avancé de la *blockchain* n'avait été versée au débat, ce qui n'a pas permis au juge des référés d'apprécier l'introduction de nouvelles technologies.

660. **L'audace technologique de la Cour de cassation dans la preuve électronique.** De longue date, la Cour de cassation est reconnue pour sa capacité à faire preuve « *d'audace technologique* » concernant l'évolution des preuves et leur reconnaissance. Avant l'adoption de la loi du 13 mars 2000 relative à l'écrit électronique, la Cour de cassation témoignait d'un

certain libéralisme dans la reconnaissance probatoire de la photocopie[1375], de la télécopie[1376], ou encore de la preuve électronique[1377]. Il n'est donc pas déraisonnable de penser qu'elle se montrerait une nouvelle fois entreprenante si une question sur le droit des preuves *blockchains* lui était posée.

661. **L'admission théorique des preuves *blockchains* en cas de liberté de la preuve.** Force est d'admettre que si dans un litige un plaideur bénéficie du principe de liberté de la preuve, il pourra apporter par tous moyens sa preuve et le juge français n'a pas de raison d'écarter *a priori* les preuves *blockchains*. En droit français, rien n'empêcherait dans ce contexte favorable l'admission de cette preuve *blockchain* par les juges particulièrement demandeurs, comme le confirme une réponse ministérielle du 10 décembre 2019[1378]. Malgré cette liberté d'appréciation du juge dans certains cas, ce dernier doit tout de même répondre aux conclusions qui lui sont présentées[1379]. Par exemple, avait été cassé un arrêt qui trouvait dans un enregistrement magnétique versé comme pièce aux débats la confirmation de propos attribués à l'une des parties, sans pour autant répondre aux conclusions avançant qu'un document était un faux[1380]. Les juges du fond ne sont pas tenus toutefois de répondre à tous les arguments présentés afin de combattre les éléments de preuve qu'ils considèrent comme déterminants[1381]. Ils peuvent d'ailleurs faire état d'un élément de preuve qui n'a pas été expressément visé dans les conclusions s'il a été versé aux débats régulièrement et soumis à discussion contradictoire des parties[1382]. Si un litige est porté devant la juridiction suprême, les juges du droit pourraient profiter d'un *obiter dictum* pour exprimer leur opinion - même étrangère à l'espèce - sur le droit

[1375] CA Versailles, 27 sept. 1989 : D. 1989. IR 293 ; CA Paris, 15 févr. 1990 : D. 1990. IR 72 : sur le fondement de la loi n°80-525 du 12 juillet 1980, les juges du fond ont considéré que la photocopie d'une reconnaissance de dette était fidèle et durable ; Cass. 1ère civ. 25 juin 1996 n°94.11-745 : Bull. civ. I, n°270 : la Cour de cassation a estimé que les juges avaient constatés que la photocopie qui avait été produite aux débats était une reproduction fidèle et durable du mandat confié à un commissaire-priseur et que le document ainsi produit ne valait pas seulement comme commencement de preuve par écrit, mais faisait pleine preuve du contrat de mandat.

[1376] Com. 2 déc. 1997, n°95-14.251 : D. 1998. 192 note Martin ; JCP 1998. Actu. 905, obs. P. Catala, P.-Y. Gautier ; JCP E 1998, P.178, note Boneau ; JCP 1998. II. 10097, note Grynbaum : les juges de cassation se sont prononcés sur la force probante d'une télécopie dans une affaire de borderau Dailly et les conditions nécessaires à la valeur probatoire d'un document produit par télétraitement. Il était question en l'espèce que l'acceptation de la cession puisse être donnée par le débiteur sous la forme de télécopie.

[1377] P. Catala, P.-Y. Gautier, « L'audace technologique à la Cour de cassation vers la libéralisation de la preuve contractuelle », JCP E n°23, 4 juin 1998, p.884.

[1378] Question écrite n°22103 de D. Fasquelle, publiée au JO le 30/07/2019, réponse du Ministère de la Justice publiée au JO le 10/12/2019, p.10774. Voir annexe n°10.

[1379] J.-L. Mouralis, « Preuve : modes de preuve », *op.cit.*, n°617, p.75.

[1380] Cass. 3ème civ., 15 janv. 1970, Bull. civ. III, n°39.

[1381] Cass. 3ème civ., 17 janv. 1969, Bull. civ. III, n°63 ; Cass. 1ère civ., 5 oct. 1977 Bull. civ. I, n°357.

[1382] Req. 8 janv. 1879 : S. 1880. 1. 16. ; Cass. 2e civ., 16 janv. 1957 : Bull. civ. II, n°47 ; Cass. 3e civ., 12 avr. 1972 : Bull. civ. III n°218 . 28 nov. 1972, Bull. civ. III, n°636 ; JCP 1973. IV. 16 ; Cass. 1ère civ., 5 fevr. 1991 : D. 1991. 456, note Massip.

qui entoure les preuves *blockchains* et l'évolution souhaitable de la législation, tout en participant à la portée de la décision rendue.

662. **En attente d'une pratique judiciaire sur les preuves *blockchains*.** C'est « *la pratique judiciaire (qui) pourra révéler le champ des possibles en matière de preuve blockchain* » remarquait Sophie Canas, Conseillère référendaire à la Cour de cassation[1383]. Une jurisprudence solide des tribunaux français pourra à cet égard jouer un rôle important dans la construction du régime général des preuves *blockchains*, incitant à terme une réforme pour intégrer les solutions jurisprudentielles au sein de dispositions légales (voir ci-avant la proposition de *lex blockchain*). Un droit prétorien favorable aux preuves *blockchains* contribuerait beaucoup au rayonnement de la place française comme pays attractif dans le secteur de la technologie des registres distribués.

B. L'admission de la preuve d'un ancrage de données dans la *blockchain* par les juges chinois

663. La reconnaissance de l'ancrage des données dans la *blockchain* au sein d'une décision chinoise (1) constitue une première pierre à l'édifice de l'appréciation des preuves *blockchains* par un juge. Le caractère circonstancié de cette décision chinoise doit néanmoins être mis en exergue afin de nuancer sa portée (2).

1. La reconnaissance de l'ancrage des données dans la *blockchain* au sein d'une décision chinoise

664. C'est en Chine qu'une décision sur l'ancrage de données dans la *blockchain* a été très instructive. La *Hangzhou Internet Court*, le 27 juin 2018 a reconnu un ancrage de données dans la *blockchain*[1384]. En l'espèce, il était question d'un demandeur, la société Huatai Yimei, qui invoquait la violation de ses droits de propriété intellectuelle liés à des éléments de son site Internet, produisant des captures d'écrans de son site et des codes sources ancrés dans la

[1383] S. Canas, « Blockchain et preuve : le point de vue du magistrat », *op.cit.*, p.82.
[1384] Hangzhou Internet Court, Province of Zhejiang People's Republic of China, Case No. 055078 (2018) Zhe 0192 No. 81 Huatai Yimei/Daotong, June 27, 2018. Voir annexe n°11 la decision traduite en anglais.

blockchain Bitcoin et Factom. C'est par l'intermédiaire de la plateforme tierce « *Baoquan.com* », prévue à cet effet, que les preuves avaient été ancrées. Le défendeur, la société Daotong, aurait publié un site Internet contrefaisant certains éléments des droits d'auteur de la Société Huatai Yimei sans requérir d'autorisation ou de licence auprès d'elle.

665. La *Hangzhou Internet Court* saisie devait se prononcer précisément sur trois questions : la qualité à agir de la société Huatai Yimei, la violation ou non du droit d'auteur de la société Huatai Yimei, et le montant raisonnable ou non des dommages-intérêts au regard de la violation, réclamés par la société Huatai Yimei. Nous concentrerons nos remarques sur la deuxième question qui comporte le plus d'enjeux dans la problématique de l'appréciation par le juge des preuves de données enregistrées dans la *blockchain*. Elle portait plus précisément sur le point de savoir si la titularité d'un droit d'auteur pouvait être établie par un ancrage dans la *blockchain* et s'il pouvait être admissible en justice. La *Hangzhou Internet Court* a déclaré sur cette deuxième interrogation que l'ancrage de données dans une *blockchain* Bitcoin était un moyen de preuve admissible et reçu dans cette affaire en raison de l'intégrité de la preuve *blockchain* en cause. Elle fait donc droit aux demandes de la société Huatai Yimei sur la violation de son droit d'auteur en rendant sa décision sur le fondement notamment des articles 10, 11, 48, et 49 de la loi sur le droit d'auteur de la République populaire de Chine et de l'article 8 sur la signature électronique de la République populaire de Chine, réalisant un examen minutieux de l'authenticité des messages électroniques conformément à cet article (examen de fiabilité des méthodes de génération, de stockage ou de transmission des messages électroniques, de fiabilité des méthodes pour maintenir l'intégrité du contenu, et de fiabilité des méthodes d'identification d'un émetteur).

666. Remarquons par ailleurs que les juges de la *Hangzhou Internet Court* ont étonnamment fait abstraction des règles d'admissibilité de preuve en Chine de la loi sur la procédure civile. À défaut de mention de ces règles, observons toutefois que cette affaire est conforme à cette loi qui, rappelons-le, dans sa dernière version en vigueur depuis le 1er juillet 2017, reconnaît expressément les « *données électroniques* » comme une catégorie juridique de preuves[1385]. Cependant, même si elles sont admissibles en tant que preuves, leur valeur probante reste souvent inférieure à celle d'autres catégories de preuves telles que les preuves physiques[1386]. En

[1385] LPC, art. 63, (5).
[1386] LPC, art. 63, (3). Voir : X.-G. Wang, Research on Relevant Legal Problems of Electronic Evidence, 2nd Annual International Conference on Social Science and Contemporary Humanity Development, 2016, p.380 ;

pratique, les parties ont tendance à demander une « *notarisation* » de la preuve électronique pour s'assurer de son admission[1387]. C'est pourquoi, cette décision est de taille, tant remise dans son contexte national de la preuve en Chine qui s'émancipe de la « *notarisation* », que dans le contexte international. Elle constitue semble-t-il, parmi l'ensemble des juridictions du monde, la première reconnaissance de l'admissibilité et de la recevabilité par un juge de la preuve de données ancrées dans une *blockchain*. Nous aurions tort de ne voir là qu'une simple admissibilité d'un mode de preuve quelconque. Cette décision a fait des émules et pourrait certainement susciter l'envie de reconnaître les preuves *blockchains* au sein d'autres juridictions si l'occasion se présentait. Nuançons néanmoins cette analyse en raison du caractère circonstancié de l'affaire en cause.

2. Le caractère circonstancié de la décision chinoise sur la reconnaissance de l'ancrage des données dans la *blockchain*

667. Le caractère circonstancié de la décision chinoise du 27 juin 2018 sur la reconnaissance de l'ancrage des données dans la *blockchain* doit être relevé du fait que d'une part, le faisceau d'indices était concordant avec la preuve de l'ancrage apporté (a) et d'autre part, cette décision est rendue par un tribunal spécialisé dans le contentieux de l'Internet (b).

a. Un faisceau d'indices concordant avec la preuve *blockchain* apportée

668. Le faisceau d'indices de l'espèce concordant avec la preuve *blockchain* apportée lors du litige a contribué à la réception favorable de cette reconnaissance.

669. **La vérification des données ancrées.** La *Hangzhou Internet Court* procède à un raisonnement en deux temps : elle vérifie que les données prouvant la contrefaçon avaient bien été déposées dans la *blockchain* et contrôle que ces données correspondaient à celles présentées par la partie demanderesse lors du litige. En l'espèce, le juge avait eu l'opportunité de confirmer tout d'abord la date du dépôt dans le registre, la date de la validation de la transaction dans le

X. Hong, « *Online Dispute Resolution for E-Commerce in China: Present Practices and Future Developments* », Hong Kong Law Journal, 2004, p.379-380.

[1387] S. Polydor, « Blockchain Evidence in Court Proceedings in China – A Comparative Study of Admissible Evidence in the Digital Age (as of June 4, 2019) », Stanford Journal of Blockchain Law and Policy, 5 janv. 2020, https://stanford-jblp.pubpub.org/pub/blockchain-evidence-courts-china, (consulté le 31/05/2020).

registre ainsi que l'empreinte des données en question. Puis, ce dernier avait procédé à la vérification de la conformité et de l'intégrité des données déposées dans la *blockchain* à celles présentées lors du litige. L'ensemble des examens sur ces données ancrées corroboraient la violation du droit d'auteur et abondaient dans le sens des faits invoqués par le demandeur. Elles avaient donc permis de convaincre le juge. Les données ancrées reçues pouvaient alors servir de base justificative à l'atteinte au droit d'auteur en l'espèce.

670. **La fiabilité du registre *blockchain* et de la plateforme tierce.** Par ailleurs, il est fait mention du protocole Bitcoin et de l'algorithme SHA256 pour calculer les empreintes, reconnus comme étant particulièrement sécurisés et fiables. Il n'est pas certain qu'avec une autre *blockchain*, le juge ait été en mesure de retenir cette solution. De surcroît, les juges de la *Hangzhou Internet Court* axent une partie de leur raisonnement sur la sécurité de la plateforme tierce qui avait permis l'ancrage, laquelle conservait ses données sur un *cloud computing*. L'usage de cette plateforme permettait d'avoir une garantie, d'une part, que ce cloud en particulier assurait que les serveurs n'étaient pas infectés, envahis par des virus, ou des chevaux de Troie, et d'autre part, que des certificats de classe I de sécurité et de classe III de protection du système d'information avaient été délivrés à la plateforme par un institut de recherche et le Centre national de contrôle et de test de la qualité des produits de la sécurité informatique et cybernétique. Par conséquent, cette plateforme disposait aussi d'un environnement très sécurisé de stockage des données.

671. **L'approche au cas par cas.** Cette décision ne peut prétendre être généralisable à tous les contentieux du même acabit. La Cour nuance sa décision en soutenant que « *les données électroniques sauvegardées et sécurisées par des moyens techniques tels que la blockchain doivent être analysées et qualifiées au cas par cas dans un esprit d'ouverture et de neutralité* ». En vue d'adopter cette analyse au cas par cas et de déterminer « *l'efficacité de la preuve* » de données enregistrées dans la *blockchain*, le juge chinois recommande de mettre l'accent sur « *(…) l'examen de la source des données électroniques, l'intégrité de leur contenu, la sécurité des moyens techniques, la fiabilité des méthodes, (…) le degré d'association avec d'autres éléments de preuve pour les corroborer* ».

672. Les preuves par *blockchain* ne semblent pas reconnues à ce stade comme une forme de preuve numérique admise par tous les tribunaux chinois car ce jugement du 27 juin 2018 ne

donnait pas le ton d'une décision de principe. Il n'est en effet pas à exclure qu'en fonction de la typologie de *blockchain*, le sens d'une décision soit différente.

673. Par ailleurs, la Chine est un continent central dans le marché de la *blockchain*, tant par le nombre de mineurs qui y sont établis, que par des acteurs économiques comme Alibaba qui disposent de solutions de licences basées sur la technologie *blockchain*. Nous ne pouvons occulter l'idée que cette décision circonstanciée ait eu comme objectif de placer cette technologie comme pierre angulaire d'une stratégie de promotion globale de la technologie *blockchain*.

b. Une juridiction spéciale

674. **Présentation des Tribunaux de l'Internet en Chine.** Le tribunal qui a reçu la décision du 27 juin 2018 est une juridiction spéciale à Hangzhou. C'est le premier tribunal en Chine spécialisé dans des litiges liés à Internet et au numérique[1388]. Il existe actuellement trois Tribunaux de l'Internet en Chine : la *Hangzhou Internet Court*, le premier tribunal créé en août 2017, puis la *Beijing Internet Court* et la *Guangzhou Internet Court* créés en septembre 2018[1389].

675. **Compétences des Tribunaux de l'Internet en Chine.** Ce sont des tribunaux de première instance compétents territorialement dans le ressort de leur ville. La loi de la Cour suprême populaire chinoise sur le jugement des litiges par les Tribunaux de l'Internet en vigueur depuis le 7 septembre 2018 clarifie la compétence matérielle de ces tribunaux[1390]. Le deuxième article de cette loi prévoit le type de litige que pourront traiter les Tribunaux de l'Internet : des litiges portants sur le *e-commerce*, les prêts en ligne, la titularité et la violation des droits d'auteur, des droits voisins, et des noms de domaine, la violation des droits de la personne et de

[1388] China Internet Development Report, Chinese Academy of Cyberspace Studies Editor, 2017, p.96.
[1389] S. Polydor, « Blockchain Evidence in Court Proceedings in China – A Comparative Study of Admissible Evidence in the Digital Age (as of June 4, 2019) », Stanford Journal of Blockchain Law and Policy, jan. 2020, https://stanford-jblp.pubpub.org/pub/blockchain-evidence-courts-china (consulté le 31/05/2020), p.5.
[1390] S. Xia, « China's Internet Courts are Spreading; Online Dispute Resolution is Working », China Law Blog, 23 dec. 2018, https://www.chinalawblog.com/2018/12/chinas-internet-courts-are-spreading-online-dispute-resolution-is-working.html (consulté le 31/05/2020).

la propriété sur Internet, les plaintes relatives à la responsabilité du fait des produits, et les litiges d'intérêt public sur Internet introduits par les procureurs[1391].

676. **Fonctionnement des Tribunaux de l'Internet en Chine.** Sur l'organisation de ces juridictions, le premier article de la loi de la Cour suprême populaire chinoise sur le jugement des litiges par les Tribunaux de l'Internet prévoit que ces tribunaux jugent les affaires essentiellement en ligne[1392]. L'ensemble du processus de litige dans les Tribunaux de l'Internet sera mené en ligne. Lorsqu'une affaire est traitée par le Tribunal de l'Internet, les plaintes sont tout d'abord enregistrées directement en ligne. Après une mise en état rapide, une audience est organisée en visioconférence[1393]. Les décisions du jugement sont enfin publiées sur le site Internet du tribunal. Toutes les étapes sont ainsi effectuées sur Internet : les poursuites, les pièces, le jugement, la notification des actes[1394].

677. **Usage institutionnalisé des preuves *blockchains*.** En ce qui concerne les preuves en particulier, l'article 11 de cette loi confirme que le Tribunal de l'Internet apprécie les preuves électroniques comme des signatures électroniques permettant l'authentification des parties, un horodatage, une vérification par la fonction de hachage, une *blockchain* et d'autres méthodes de vérification[1395]. La *Hangzhou Internet Court* aurait mis en place à titre de support sa propre plateforme d'ancrage de preuve déployée par la *blockchain*[1396]. L'offre de préconstitution de preuve par un tribunal pose toutefois question. Une admissibilité et recevabilité des ancrages *blockchains* pourraient être établies de façon implicite par le seul usage de cette plateforme. Le risque est qu'elle en vienne à créer une inégalité dans l'administration de la preuve entre les plaideurs, notamment ceux ne faisant pas appel à cette plateforme pour ancrer des données.

678. Par ailleurs notons que le 18 septembre 2018, le tribunal Internet de Hangzhou a lancé la première plateforme officielle de résolution des litiges par *blockchain*, développée

[1391] S. Polydor, « Blockchain Evidence in Court Proceedings in China – A Comparative Study of Admissible Evidence in the Digital Age (as of June 4, 2019) », *op.cit.*, p.6.
[1392] S. Xia, « China's Internet Courts are Spreading; Online Dispute Resolution is Working », *op.cit.*
[1393] https://www.lexpress.fr/actualite/monde/asie/la-chine-se-dote-du-premier-tribunal-sur-internet_1936345.html (consulté le 31/05/2020).
[1394] S. Xia, « China's Internet Courts are Spreading; Online Dispute Resolution is Working », *op.cit*.
[1395] S. Polydor, « Blockchain Evidence in Court Proceedings in China – A Comparative Study of Admissible Evidence in the Digital Age (as of June 4, 2019) », *op.cit.*, p.6.
[1396] http://evidence.netcourt.gov.cn/#/page (consulté le 31/05/2020)

conjointement par les Offices notariaux, l'Autorité de certification et d'enregistrement, et le Centre d'évaluation judiciaire[1397].

679. Pour l'ensemble de ces différentes raisons et circonstances favorables à l'accueil de cette décision, il n'est pas alors certain qu'elle soit étendue à tous les litiges similaires se basant sur une preuve issue d'un ancrage dans la *blockchain*, devant toutes juridictions de droit commun.

Paragraphe 3 : La gestion contractuelle du risque de preuves *blockchains* liée à l'absence d'appréciation du juge

680. Les risques immanents dans l'emploi des preuves *blockchains* trouve un écho naturel dans la notion doctrinale de risque de preuve (A). Ce risque inhérent au flou juridictionnel est maîtrisé par la possibilité d'encadrer contractuellement les preuves *blockchains* par convention de preuve (B), laquelle a des caractéristiques propres lorsque l'objet porte sur lesdites preuves (C).

A. La notion de risque de preuve *blockchain*

681. **Une notion doctrinale libre.** La notion de risque de preuve est une notion doctrinale libre et fluctuante. Selon une partie de la doctrine, ce risque est essentiellement une question de fond lié au raisonnement probatoire[1398], alors que le Professeur Cyril Grimaldi y voit un risque « *pour une personne de succomber lors d'un procès, dans sa demande ou sa défense, pour des raisons de preuve et non de fonds* »[1399]. Du reste, le risque de la preuve renvoie à trois grands concepts[1400] : celui de l'aléa inhérent à l'existence du procès, celui de la charge de la preuve, ainsi que celui du risque du doute, autrement dit, la question de savoir à qui le juge devra donner satisfaction lorsque la lumière ne sera pas faite[1401].

[1397] F. Mostert, J. Wang, « The Application and Challenges of Blockchain in Intellectual Property Driven Businesses in China », Tsinghua China Law Revue, vol. 11, dec. 2018, p.29.
[1398] J. Chevalier, *La charge de la preuve. Cours de droit civil approfondi*, Les Cours de droit, 1958-1959, p. 186 ; A. Bergeaud, *Le droit à la preuve*, thèse ss. dir. J.-C. Saint-Pau, Bordeaux, LGDJ, 2010, n°24, p.28 et p.227 ; P. Théry, « Les finalités du droit de la preuve », Droits, 1996, n°23, p.42 s.
[1399] C. Grimaldi, « La preuve en droit des contrats », *in* La preuve: regards croisés, *op.cit.*, p.79.
[1400] M. Mekki, « Regards substantiel sur le « risque de la preuve. Essai sur la notion de charge probatoire », in *La preuve: regards croisés*, *op.cit.*, p.7-8.
[1401] R. Legeais, *Les règles de preuve en droit civil. Permanences et transformations*, *op. cit.*, p. 101.

682. **Un risque quant à l'existence du procès et à l'issue du procès avec les preuves *blockchains*.** La « *zone grise* » tant légale que juridictionnelle des preuves *blockchains* génère tantôt un aléa et une crainte d'un potentiel litige, tantôt un risque du doute eu égard aux incertitudes du plaideur d'obtenir gain de cause. Ce risque de preuve *blockchain* conduit alors à s'interroger sur « *la preuve qui se joue avant la preuve* »[1402] . C'est par une convention de preuve *blockchain* que cette interrogation trouve des pistes de réponse. Dans l'objectif de maîtriser ce risque de la preuve *blockchain* pesant sur les parties[1403], celles-ci choisissent souvent d'encadrer au mieux l'aléa de la preuve judiciaire par une convention de preuve permettant de ne pas remettre en cause leurs prévisions[1404]. La gestion des risques de preuves *blockchains* par le contrat est une manière pour les parties de maîtriser l'aléa et le risque du doute, ou du moins de le réduire[1405].

B. L'admission de principe des conventions de preuves portant sur des preuves *blockchains*

683. **La convention de preuve comme instrument d'expérimentation de la preuve numérique.** C'est d'abord la loi du 13 mars 2000 qui a intégré le principe de la liberté contractuelle en matière probatoire dans le Code civil. L'ordonnance du 10 février 2016 a ensuite retenu une validité de principe de la convention sur la preuve par l'introduction du nouvel article 1356 du Code civil qui consacre fidèlement une jurisprudence constante sur la possibilité des parties de conclure des contrats sur la preuve[1406]. Par exemple, ont déjà été admis par la jurisprudence les clauses contractuelles portant sur l'objet de la preuve[1407], les modes de

[1402] Cour de cassation, Rapport annuel, La preuve, *op.cit.*, p. 139.
[1403] Voir : M. Mekki, « Réflexions sur le risque de la preuve en droit des contrats (1ère partie), Revue des contrats n°3, juill. 2008, p.681 et s. ; M. Mekki, « La gestion contractuelle du risque de la preuve (2e partie) », Revue des contrats n°2, avr. 2009, p.453-469.
[1404] G. Lardeux, « Preuve : règles de preuve », Répertoire civil, Dalloz, oct. 2018, n°246.
[1405] Voir sur la gestion des risques de nature probatoire par le contrat : J.-M. Mousseron, « La gestion des risques », RTD civ. 1988, p. 481 et s. ; M. Mekki, « La gestion contractuelle du risque de la preuve (2e partie) », *op.cit.*, p.453 et s.
[1406] Première jurisprudence : Req. 1er août 1906, D. 1909. I. 398. Jurisprudence de principe : Cass. 1ère civ., 8 nov. 1989, n°86-16.197 et n°86-16.196, affaires dites « Credicas » : Bull. civ. I, n°342 ; D. 1990. 369, note C. Gavalda, 327, obs. J. Huet, et 1991. 38, obs. M. Vasseur ; RTD civ. 1990. 79, obs. J. Mestre; RTD com. 1990. 78, obs. M. Cabrillac et B. Teyssié ; JCP 1990. II. 21576, obs. G. Virassamy ; BICC 1990, n°296, p.21, rapp. Bernard.
[1407] Cass. req., 16 févr. 1903, S. 1904, 1, p. 34 ; Cass. civ. 1ère, 24 févr. 2004, n°02-14005, FS-P, Sté CGU Courtage c/ Vacandare.

preuve admissibles[1408], leurs forces probantes[1409], ou encore la charge de la preuve pour l'attribuer ou la répartir[1410]. Le développement des techniques informatiques a permis un regain d'intérêt pour la convention de preuve[1411]. Avant même que le législateur n'intervienne ou que le juge ne soit confronté à une quelconque question, la convention de preuve est en effet un instrument contractuel parfait d'expérimentation de la preuve numérique pour régler les flous sur cette preuve technique[1412]. C'est dans ce contexte que la pratique de la convention de preuve est ouverte à l'expérimentation de la technologie nouvelle qu'est la *blockchain*.

684. **Les limites à la convention de preuve.** Deux limites à la validité des conventions sur la preuve sont à relever : l'une tenant à leur domaine, l'autre à leur contenu. Les conventions de preuve sont valables uniquement lorsqu'elles portent sur « *(…) des droits dont les parties ont la libre disposition* », selon le premier alinéa de l'article 1356 du Code civil[1413]. Elles interviennent donc seulement dans les matières où les parties ont la libre disposition de leurs droits puisqu'admettre des conventions de preuve portant sur des droits dont les parties n'ont pas la libre disposition reviendrait à des renonciations qui ont des incidences sur le fond du droit[1414]. Les conventions de preuve ne devraient pas pouvoir intervenir en droit des personnes et de la famille, surtout si elles concernent des droits extrapatrimoniaux[1415]. De plus, ces contrats ne peuvent contredire « *(…) les présomptions irréfragables établies par la loi, ni modifier la foi attachée à l'aveu ou au serment. Ils ne peuvent davantage établir au profit de l'une des parties une présomption irréfragable* » en vertu du second alinéa de l'article 1356 du Code civil.

[1408] Cass. civ., 1er juin 1893, S. 1893, 1, p. 285 ; Cass. req., 24 mars 1942, DC 1942, p. 64 ; Cass. 1ère civ., 5 nov. 1952, Bull. civ. I, n°286 ; Cass. soc., 24 mars 1964, JCP G 1965, II, 14415, note C. Lapp.
[1409] Cass. 1ère civ., 17 févr. 1838 : S. 1939, 1, p.317 ; Cass. req., 13 déc. 1911 : DP 1912, 1, p.158.
[1410] Cass. 1ère civ., 28 janv. 2003 : Bull. civ. I, n°26, p.21 ; Cass. req., 17 mai 1909, S. 1910, 1, p.185 ; Cass. com., 19 juill. 1965, Bull. civ. III, n°456 ; Cass. com., 8 nov. 1989, D. 1990, p.369, note C. Gavalda ; Cass. 1ère civ., 30 oct. 2007 : RDC 2008, p.252 et s., obs. Y.-M. Laithier ; D. 2008, p.2821, obs. P. Delebecque.
[1411] G. Lardeux, « Preuve : règles de preuve », *op.cit.*, n°249.
[1412] L. de Leyssac, « Plaidoyer pour un droit conventionnel de la preuve en matière informatique », Cahiers du Barreau de Paris, oct. 1987 p.53 ; L. de Leyssac, « Les conventions sur la preuve en matière informatique », *in* Informatique et droit de la preuve, Des Parques, 1987, p.143 ; H. Croze, « Informatique, preuve et sécurité », D. 1987, chr., p.165 ; M. Mekki, « La gestion contractuelle du risque de la preuve (2e partie) », *op.cit.*, p.454 ;
[1413] Confirmé par la jurisprudence antérieure : Cass. soc., 25 mars 2009 : Bull. civ. 2009, IV, n°85. Confirmé par une jurisprudence récente : Cass. Com. 6 déc. 2017, n°16-19.615, D. 2018. 327, note G. Lardeux, et 371, obs. M. Mekki ; AJ Contrat 2018. 37, obs. T. Douville ; RTD civ. 2018. 123, obs. H. Barbie.
[1414] A. Aynès, « Conventions sur la preuve : validité limitée », *in* dossier Réforme du droit de la preuve, Droit et patrimoine n°250, sept. 2015, p. 46.
[1415] A. Aynès, X. Vuitton, *Droit de la preuve. Principes et mise en œuvre processuelles*, *op.cit.*, p.61-62, n°93.

685. D'autre exceptions de droit commun sont applicables[1416], telles que celles de l'absence de possibilité de déroger par convention aux règles impératives, règles d'ordre public selon les articles 6, 1102 et 1162 du Code civil. Par exemple, il ne serait pas possible d'établir une convention de preuve pour déroger aux règles concernant la valeur probatoire des actes authentiques ou celles de la procédure d'inscription de faux. Par ailleurs, la convention ne doit pas créer un déséquilibre significatif entre les droits et obligations des parties relatifs à la preuve dans les contrats de consommation et d'adhésion visée à l'article 1110 du Code civil. Des clauses pourraient être qualifiées d'abusives lorsqu'elles sont un moyen pour un professionnel d'échapper à ses obligations, à l'instar d'une clause renversant la charge de la preuve[1417]. L'article R132-1-12° du Code de la consommation présume irréfragablement abusives les clauses conclues entre les professionnels et consommateurs qui imposent au consommateur la charge de la preuve qui devrait incomber au professionnel en vertu du droit applicable. L'article R132-2-9° du Code de la consommation établit, quant à lui, une présomption simple de clause abusive pour les clauses limitant indûment les moyens de preuve à la disposition du consommateur. Le cas échéant, ces clauses sont réputées non écrites[1418]. En pratique, pour que les enregistrements de données dans la *blockchain* soient admis entre un professionnel et un consommateur par convention de preuve, il est possible de mentionner que ces enregistrements font foi de preuve entre les parties mais sans le restreindre à ce seul mode de preuve. À défaut, cette clause pourrait être présumée simplement abusive.

686. **Les divergences doctrinales sur la pratique de la convention de preuve.** Même si la validité des clauses sur la preuve fait désormais l'objet d'un assentiment général de la doctrine[1419], ce ne fut pas toujours le cas[1420]. Certaines divergences doctrinales persistent au demeurant quant à la promotion ou non de cette pratique de la preuve contractuelle.

[1416] A. Aynès, J.-D. Bretzner, « Droit de la preuve juin 2015 - juin 2016 », D.2016, p. 2536.

[1417] Cass. 1ère civ., 1er févr. 2005, n°01-16733, SA Facet c/ FLCE : JCP G 2005, IV, 1531, Contrats, conc. consom. 2005, comm. 99, obs. G. Raymond ; D. 2005, p.640, obs. V. Avena-Robardet, RDC 2005, p.719, obs. D. Fenouillet.

[1418] C. conso., art. L212-1 ; C. civ. art, 1171.

[1419] P. Malaurie, L. Aynès et P. Stoffel-Munck, *Les obligations*, Defrénois, 3e éd., 2007, n°565, p.292 ; J. Flour, J.-L. Aubert, Y. Flour, E. Savaux, *Le rapport d'obligation*, Sirey, 4e éd., 2005, n°15, p.12 ; G.-M. Sescioréano, *Des conventions sur la preuve de la libération du débiteur*, thèse, Paris, 1920, p. 49 et s. ; M. Planiol, G. Ripert, *Traité pratique de droit civil français*, t.7, Obligations, 2e éd., par P. Esmein, LGDJ, 1954, p.856 et s., n°1428 et s.

[1420] R. Le Balle, *Des conventions sur les procédés de preuve en droit civil*, thèse, Paris, 1923, p. 30 et s. ; R. Legeais, *Les règles de preuve en droit civil, permanences et transformations*, thèse, Poitiers, 1954, LGDJ, 1955, p. 134 et s. ; E. Bonnier, *Traité pratique du droit des preuves en droit civil et en droit criminel*, t. 1, 3e éd., 1862, p. 220 et s.

687. Pour les Professeurs Philippe Malaurie, Laurent Aynès, et Philippe Stoffel-Munck, la preuve dite « *contractuelle* » est centrale et doit être aménagée, au moment de la conclusion du contrat avant que le droit ne soit réclamé[1421]. Elle permet de se ménager une certaine sécurité en prévention des contestations ultérieures. *A contrario*, lorsque le juge a le plein pouvoir pour administrer la preuve, la prévisibilité du droit est moindre[1422].

688. Pour d'autres, le contrat poserait une présomption de vérité au bénéfice d'une preuve dont la crédibilité n'est pas avérée et récusable. Lorsque la preuve est établie unilatéralement par le contractant à qui elle profite, la conformité de celle-ci aux principes du droit européen du procès poserait question selon la Professeure Gwendoline Lardeux[1423]. Une clause accordant force probante absolue à des modes de preuve pourrait se heurter aux droits de la défense ôtant tout moyen de contester l'existence et l'étendue d'une preuve[1424]. C'est le droit d'être entendu par un juge qui est plus encore malmené en ce qu'il n'est pas possible pour une partie de présenter sa cause, et notamment ses preuves. Il est permis de s'interroger enfin au sujet du respect de l'égalité des armes. Selon cette Professeure, il serait impératif que le juge conserve le contrôle de la force probante des preuves prévues au contrat conformément à son rôle en tant que tiers impartial[1425]. Le fait de lier conventionnellement l'appréciation du juge à la force probante des modes de preuves pourrait revenir à « *vider le débat judiciaire de son contenu et de son utilité réels par l'exclusion du regard neutre et modérateur du juge* »[1426].

689. Toujours est-il que si la convention de preuve sur la *blockchain* est suffisamment claire et précise, conformément aux règles en vigueur, celle-ci s'impose et ne pourra pas être sujette à interprétation du juge. Cette convention fait cependant l'objet de spécificités au contact de la technologie *blockchain*, de l'ordre de la technique contractuelle.

[1421] P.Stoffel-Munck, P.Malaurie, L. Aynès, *Droit des obligations, op.cit.*, n°558.
[1422] *Ibid.* , n°559.
[1423] G. Lardeux, « Preuve : règles de preuve », *op.cit.*, n°271.
[1424] *Ibid*.
[1425] *Ibid*.
[1426] G. Virassamy, JCP 1990. II. 21576, n°16.

C. Les spécificités pratiques de la convention de preuve portant sur des preuves *blockchains*

690. La convention de preuve employant une bonne technique de rédaction contractuelle facilitera la résolution d'éventuels conflits de preuves soumis au juge[1427]. Par cette convention, les parties ayant prévu de développer un usage ensemble *via* une *blockchain* auront une certaine latitude dans le choix du rôle, de la valeur et la portée qu'elles entendent accorder aux écrits du registre et aux procédés de la *blockchain*. Il pourrait s'agir d'établir une convention de preuve sur l'admissibilité et la recevabilité des procédés des preuves *blockchains*, et leur force probante. Au contraire, certaines parties pourraient préférer restreindre la portée de certains éléments de preuve issus de la *blockchain*. Or, il est permis d'éprouver des doutes sur la légalité même d'écarter la force probante de preuves *blockchains* si la loi nationale est impérative et que l'usage de cette preuve se situe dans le pays où cette loi est impérative[1428].

691. Cette convention doit être évidemment licite et précise, et sera adaptée à chaque cas de *blockchain*. Elle pourra cependant comporter des clauses précisant :

La valeur et la portée des preuves *blockchains* :

- la valeur des inscriptions de données dans la *blockchain* pourra être déterminée par les parties. Elle pourrait viser une preuve d'existence, de possession, d'origine, d'intégrité, de date certaine, par exemple ;
- les parties pourront s'engager sur la qualité des données, des documents ancrés dans la *blockchain* (la source d'information d'origine, par exemple) ;
- l'ensemble des données informatiques générées par ou inscrites dans la *blockchain* pourront faire foi entre les parties ;

[1427] L. Grynbaum, Fasc. 10 : La preuve littérale, JCl. Civil Code – Art. 1316 à 1316-4, *op.cit.*, n°36.

[1428] La restriction de la force probante de certains éléments de preuve *blockchain* a été interrogée lors du Colloque « *Blockchain et preuve* » inscrite dans le cycle de conférences intitulé « *blockchains : entre mystères et fantasmes* » co-organisé par l'Institut de Recherche pour un Droit Attractif (IRDA) et la Cour de cassation. Pour le Professeur Mustapha Mekki, il serait tout à fait envisageable de projeter une convention de preuve qui exclurait la force probante trop excessive consacrée par certains des pays. Le Professeur Augustin Aynès se questionne quant à lui sur la légalité même d'écarter cette force probante si la loi nationale est impérative (Cour de cassation, Cycle de conférences « Entre mystère et fantasme : quel avenir pour les *blockchains* ? », sous la dir. scientifique de M. Mekki, N. Blanc, B. Haftel, 2e cycle - conférence n°1 « Blockchain et preuve », modération par A. Aynès, 27 fevr. 2020).

- les parties pourront s'engager à ne pas contester l'admissibilité, la recevabilité, l'opposabilité ou encore la force probante des éléments générés et inscrits dans la *blockchain* ;
- les parties pourront prévoir les modalités d'identification des nœuds, des participants ayant des droits d'écriture et des accédants au sein des *blockchains* privées ;
- les parties pourront mentionner que l'apposition de la clé privée pourra avoir la valeur d'une signature et le degré de fiabilité afférent à cette signature ;
- les parties pourront garantir l'identité du signataire pour une signature dans une *blockchain* privée. Cette disposition aura toute sa pertinence dans une convention de preuve pour présumer l'imputabilité de l'acte que l'on enregistre dans la *blockchain* par cette identification du titulaire des clés de signature[1429] ;
- les parties pourront prévoir la gestion des délégations de pouvoir pour inscrire des données. Une partie ne pourra pas opposer à une autre le défaut de pouvoir pour faire échec à la valeur juridique de la transaction signée, horodatée ou une quelconque inscription dans la *blockchain*.

Les droits des parties :
- une ou plusieurs parties devront être habilitées à écrire dans le registre (incluant la signature, l'horodatage et l'ancrage) ;
- une ou plusieurs parties devront être habilitées à héberger un nœud, et/ou télécharger une copie du registre, et/ou lire le registre.

Les évolutions du protocole :
- Les parties pourront reconnaître et accepter que le protocole soit amené à faire l'objet d'améliorations et d'évolutions, notamment pour le maintien à l'état de l'art. Il conviendra d'organiser les modalités de ces améliorations et évolutions, surtout dans l'hypothèse de *hard fork*[1430]. Il pourra notamment être prévu que ces évolutions ne devront pas remettre en cause la valeur des inscriptions du registre initial et altérer ou risquer d'altérer le niveau de sécurité de ce registre.

Le droit applicable et la juridiction compétente : il conviendrait de choisir la loi d'un État dans lequel les inscriptions dans un registre de la *blockchain* sont reconnues ou à tout le moins

[1429] T. Douville, « *blockchains* et preuve », *op.cit.*, p.2194.
[1430] Voir *supra* n°26 la notion de *fork*.

en faveur de la reconnaissance de la force probante de ces éléments de preuve. Le Ministère de la Justice estime toutefois que la portée de la désignation conventionnelle du droit applicable dépend de la matière concernée[1431]. À titre d'exemple, l'application du droit français ne pourrait être éludée dans les conventions portant sur des biens immobiliers[1432]. Par ailleurs, le risque de l'usage de la convention de preuve pour la *blockchain* est la pratique du *forum shopping* consistant en droit international à saisir la juridiction la plus susceptible de donner raisons à ses propres intérêts.

692. **Difficultés tenant à la nature de la *blockchain*.** La convention de preuve pourra sembler complexe, voire impossible à établir au sein des *blockchains* publiques. Pour réaliser une convention de preuve, il convient en effet de pouvoir identifier les personnes exprimant leur consentement, leur volonté, ce qui n'est pas le cas des acteurs de la *blockchain* publique. Il semble en effet laborieux de vérifier l'identité et le consentement de participants intervenant pseudonymement par des adresses publiques et de validateurs, serveurs difficilement localisables[1433]. Cette difficulté trouve une issue favorable au cours de l'usage d'un protocole public par un prestataire. Si un prestataire établit des termes et conditions du service et les met à disposition par le biais d'une plateforme, il est tout à fait envisageable d'intégrer une clause sur la preuve. Cela rejoint aussi l'activité d'un prestataire de *blockchain* en mode BaaS qui pourra établir une convention de preuve avec ses clients[1434]. Pour ce qui est des conventions de preuve dans les *blockchains* privées, les parties peuvent aisément se mettre d'accord sur les termes à retenir pour rendre efficace l'usage d'un registre distribué.

693. **Contractualisation des preuves *blockchain* et réalités pratiques.** Force est de remarquer que les parties sont enclines à préférer une convention de preuve sur les preuves *blockchains* et ses procédés, qui facilite le travail du juge dans l'appréciation de la force probante des preuves *blockchains*, plutôt que de le laisser se livrer à une hypothétique recherche minutieuse d'une vérité technique complexe à déceler[1435]. Le juge sera lié par cette convention de preuve au nom de sa force obligatoire[1436]. Le rapport Toledano met cependant en évidence

[1431] Assemblée nationale, Rapport d'information n°1501, *op.cit.*, p.88.
[1432] C. civ., art. 3, al. 2.
[1433] Voir *supra* n°133.
[1434] M.-A. Ledieu, « La Baas démocratise la blockchain », *op.cit.*, p.367.
[1435] Voir dans le même sens pour l'appréciation des preuves électroniques : M. Cocural, *Étude théorique et jurisprudentielle des conventions des parties en matière de preuve, en droit civil français*, thèse, Toulouse, 1933, p. 29 et s.
[1436] Cass. 1ère civ., 4 juin 1991, n°89-21.147 : Bull. civ. I, n°181 ; RTD civ. 1992. 403, obs. P.-Y. Gautier.

les travers d'une convention mal rédigée aux clauses disproportionnées et imprécises, précisant qu' « *en cas de litige, le juge statuera sur la validité de la convention de preuve judiciaire et sur sa portée. Cela signifie qu'il suivra en principe les stipulations de la convention de preuve mais pourra, le cas échéant, être amené à apprécier lui-même la portée des éléments de preuve soumis par les parties* »[1437].

694. **Position de la doctrine.** Une partie de la doctrine, à l'instar notamment de la Professeure Fabienne Jault-Seseke, est en faveur de la contractualisation des preuves *blockchains*. Selon elle, les parties ayant prévu de développer un usage ensemble *via* la *blockchain* « *doivent choisir le rôle qu'elles entendent accorder à la blockchain mais aussi de choisir la loi applicable à leur contrat* »[1438].

695. **Conclusion du chapitre 1.** En conclusion de ce premier chapitre, malgré de vastes pouvoirs reconnus au juge dans la recherche des preuves *blockchains*, c'est essentiellement le terrain pénal qui l'affaire, ce domaine s'émancipant par la nécessité conjoncturelle de la recherche de preuves pénales dans ou sur la *blockchain*. Sont mises en œuvre les procédures de perquisition des paires de clés, de saisie confiscation des crypto-actifs transférés sur les portefeuilles de l'AGRASC, l'enquête pseudonyme généralement sur les réseaux du *darkweb* avant l'infraction, la captation de données sur l'écran du cyber-délinquant, et les techniques d'informatique légale par le *crypto-tracking* anlysant les flux de transactions suspectes. Pour autant, les moyens d'investigation restent insuffisants. Il s'agirait d'accorder davantage de moyens technologiques d'investigation (et compatibles avec d'autres crypto-actifs que bitcoin) aux services d'enquête. Ces moyens seront mis à disposition des agents et officiers de police judiciaire, mais aussi de TRACFIN et des cyberdouanes pour la lutte contre le blanchiment et le financement du terrorisme. Le CMII chargé du soutien aux enquêtes pourrait être l'organisation internationale désignée pour l'établissement et la coordination de ces moyens à l'échelle internationale.

696. Bien que demandeur de preuves *blockchains* (sollicitées à deux reprises), le juge français ne laisse transparaître aucun indice en filigrane sur leur appréciation, contrairement à son homologue chinois qui reconnait l'ancrage dans une décision du Tribunal de Hangzhou du 27 juin 2018. Il n'est pas certain toutefois que cette décision puisse être généralisable à tous les

[1437] F. G'sell, « Preuve et signature numérique », *op.cit.*, p.100.
[1438] F. Jault-Seseke, « La blockchain au prisme du droit international privé, quelques remarques », *op.cit.*, p.546.

litiges similaires devant toutes juridictions de droit commun car elle était circonstanciée, tant par son faisceau d'indices concordant à l'ancrage dans la *blockchain* de l'espèce, que par la juridiction spéciale du tribunal de l'Internet de Hangzhou. Cela étant, le juge français pourra avoir plus ou moins de latitude d'interprétation en fonction de la liberté ou de légalité des preuves *blockchains* ; et de difficultés à trancher et démêler de potentiels conflits de preuves. Force est d'admettre cependant que si dans un litige un plaideur bénéficie du principe de liberté de la preuve, il pourra apporter la preuve qu'il souhaite au soutien de ses prétentions et le juge français n'aurait pas de raison en principe d'écarter les preuves *blockchains*. Néanmoins, cette absence de précisions des contours de l'admissibilité et de la recevabilité, de la valeur et de la portée juridique de ces preuves ne permet pas de garantir une prévisibilité satisfaisante au justiciable. Il en résulte un encouragement au recours à des conventions de preuve, faisant émerger un véritable risque de « *preuve contractuelle blockchain* » laissée aux parties.

CHAPITRE 2

LE DEPASSEMENT ATTENDU DES JURIDICTIONS TRADITIONNELLES EN MATIERE DE PREUVE DES DONNEES ENREGISTREES DANS LA *BLOCKCHAIN*

697. L'attitude du juge face à l'appréhension des preuves d'un nouveau genre générées par une technologie peu connue traduit une certaine réserve et un immobilisme. Cela n'est pas sans risque (section 1) puisque cette inertie place le justiciable dans une insécurité et une expectative qui ne lui permettent pas d'asseoir sa posture, tant sur de nouveaux projets liés à la technologie *blockchain a priori*, que lorsque le litige survient *a posteriori* sur des éléments de preuve produits par cette technologie. Un dépassement des juridictions est alors attendu. Le renforcement de l'office du juge est, dans ces circonstances, bienvenu. Nous présenterons des propositions adaptées dans les développements qui suivront (section 2).

Section 1 : Les risques de l'attentisme du juge quant aux preuves de données enregistrées dans la *blockchain*

698. Le certain statisme du juge engendre des risques à deux niveaux : pour les justiciables, comme pour les institutions juridictionnelles. L'attentisme du juge dans la recherche de la preuve en matière pénale ou civile et dans son appréciation, liées à une affaire qui traite de la technologie *blockchain*, peut être attentatoire à la condition du justiciable (paragraphe 1) et le pousse à se tourner vers d'autres juridictions, des juridictions arbitrales (paragraphe 2), instaurant une concurrence aux juridictions traditionnelles.

Paragraphe 1 : Les risques d'atteintes aux droits des justiciables

699. En l'absence de grille de lecture claire du juge sur les preuves *blockchains*, le plaideur pourrait être placé en insécurité et ses droits s'en trouveraient atteints. D'un côté, le plaideur ne pourra pas prévoir sa stratégie probatoire de contentieux, entraînant de fait une insécurité

juridique (B) et, de l'autre, le traitement du justiciable pourra être différent pour un même problème de droit lié aux preuves *blockchains*, ce qui constituera une rupture d'égalité des citoyens devant la justice (A).

A. La rupture d'égalité des citoyens devant la justice

700. **Le principe d'égalité.** Le principe d'égalité est un principe au soutien des citoyens devant la loi, consacré à l'article 6 de la Déclaration des droits de l'homme et du citoyen de 1789 précisant que « *La loi est l'expression de la volonté générale. (…) Elle doit être la même pour tous, soit qu'elle protège, soit qu'elle punisse. Tous les citoyens étant égaux à ses yeux sont également admissibles à toutes dignités, places et emplois publics, selon leur capacité, et sans autre distinction que celle de leurs vertus et de leurs talents* ». Depuis la célèbre décision du 16 juillet 1971 du Conseil constitutionnel[1439], cet article 6 de la Déclaration des droits de l'homme et du citoyen de 1789 fait partie du bloc de constitutionnalité. Par l'application de ce principe, la loi est « *aveugle* » à toutes les caractéristiques de sexe, religion, race, etc[1440].

701. **Égalité des citoyens devant l'application de la loi.** L'égalité devant la loi implique tant une égalité des citoyens face au contenu de la loi, que face à l'exécution de celle-ci[1441]. De ce principe d'égalité devant la loi découle une égalité de tous les citoyens devant l'application de la loi par l'institution juridictionnelle, et ainsi une égalité devant la justice[1442]. Le principe d'égalité des citoyens devant la justice a une valeur constitutionnelle depuis la décision du Conseil constitutionnel du 23 juillet 1975[1443]. Cette décision admet que tous les justiciables, quelles que soit leur nationalité ou leur condition, doivent être traités de manière identique par les juridictions françaises.

[1439] Cons. Constit., du 16 juillet 1971, n°71-44 DC

[1440] D. Chagnollaud de Sabouret, *La constitution de la Ve république. Droit constitutionnel contemporain*, t.2, Cours Dalloz, 8e éd., sept. 2017, p.56, n°15.

[1441] M. Lascombe, X. Vandendriessche, C. de Gaudemont, Code constitutionnel et des droits fondamentaux 2017, annoté et commenté, Code Dalloz Universitaires et Professionnels, 6e édition, nov. 2016, p.100-101.

[1442] Voir les décisions selon lesquelles le principe d'égalité devant la justice est inclus dans le principe d'égalité devant la loi : Cons. const., 23 juillet 1975, n°75-56 DC : RD publ. 1975, note L. Favoreu ; JCP E 1975, note C. Franck ; GDCC 1984, note C. Franck ; D. 1977, note L. Hamon ; AJDA 1976 note J. Rivéro ; GDCC 1979 p.323-344, note L. Favoreu, L. Philip ; Comparative Constitutional Law 1975, note J.E. Beardsley ; Cons. const. 19 janv. 1981, n°80-127 ; Cons. const. 20 janv. 1981 : ibid. ; Cons. const. 18 janv. 1985, n°84-183.

[1443] Cons. const., 23 juillet 1975, n°75-56 DC : RD publ. 1975, note L. Favoreu ; JCP E 1975, note C. Franck ; GDCC 1984, note C. Franck ; D. 1977, note L. Hamon ; AJDA 1976 note J. Rivéro ; GDCC 1979 p.323-344, note L. Favoreu, L. Philip ; Comparative Constitutional Law 1975, note J.E. Beardsley.

702. **Égalité des citoyens devant la justice.** Derrière cette « *intuition énigmatique et insaisissable* » d'égalité décrite par le Doyen Vedel[1444], se profilent désormais des règles parfaitement opératoires[1445]. L'égalité devant la justice se traduit concrètement aussi par la reconnaissance d'un droit au juge naturel. Depuis lors, les privilèges de juridiction, qui permettaient à des citoyens d'être jugés dans certaines conditions plus favorables, ont été anéantis par la loi du 4 janvier 1993[1446]. Les justiciables qui se trouvent dans une situation identique sont dorénavant jugés par un même tribunal selon les mêmes règles de procédure et de fond.

703. **Preuves *blockchains* et risques de rupture d'égalité devant la justice.** La mise en perspective de ce principe d'égalité des citoyens devant la justice dans le cadre des preuves *blockchains* suscite des interrogations sur la possibilité de juger de manière identique plusieurs affaires impliquant ces preuves selon des règles de procédure et de fond qui, soit n'existent pas au cas particulier, soit ne sont pas confirmées. En effet, les règles de droit commun qui seraient visées par les preuves *blockchains* ne sont pas confortées dans leur application. Il est permis en cela de s'interroger quant à la possibilité du juge d'appliquer de la même manière des lois aux justiciables, dans cette situation de flou et d'incertitudes juridiques.

704. **Connaissance technique des magistrats et égalité des citoyens devant la justice.** Afin d'œuvrer dans le sens de l'égalité des citoyens face à la justice, le Conseil constitutionnel se réfère à ce principe pour s'assurer de la qualité du recrutement des magistrats[1447], en particulier des compétences juridiques des personnes nommées et de leur aptitude à juger. C'est le plus souvent pour s'assurer que tous les justiciables sont placés dans la même situation et disposent des mêmes garanties que ce principe est invoqué. Il semblerait que la technicité de ce contentieux ne se satisfasse pas de la seule compétence juridique des magistrats. Celle-ci n'est plus la seule requise pour dire le droit, compte tenu de l'ultra-spécialité de la branche du contentieux informatique et de la technicité devenue inextricable du droit. L'hétérogénéité du niveau de connaissance de cette technologie et des preuves qui en sont issues entre les juges impliquerait dans ce contexte une application différente de la loi. Cette rupture d'égalité du

[1444] G. Vedel, « L'égalité », *in* La déclaration des droits de l'homme et du citoyen de 1789, ses origines, sa pérennité, La documentation française, 1990, p.172.
[1445] F. Melin-Soucramanien, « Le principe d'égalité dans la jurisprudence du Conseil constitutionnel. Quelles perspectives pour la question prioritaire de constitutionnalité ? », Cahiers du conseil constitutionnel n°29, Dossier : la question prioritaire de constitutionnalité, 2010, p.1-2.
[1446] Loi n°93-2 du 4 janvier 1993 portant réforme de la procédure pénale.
[1447] Cons. const. 19 févr. 1998, n°98-396.

traitement des citoyens devant la justice dont la responsabilité serait imputée à l'État ne doit pas être minimisée.

B. L'insécurité juridique du plaideur dans sa stratégie probatoire contentieuse

705. **Technique probatoire.** La stratégie de tout plaideur dans un litige, quelle qu'en soit la matière, consiste à se fixer des objectifs et des moyens tactiques pour essayer de les atteindre. Une partie des moyens tactiques d'une stratégie contentieuse est cristallisée par la technique probatoire[1448]. Les parties au procès n'ont pas l'obligation d'apporter la preuve de tout élément de fait qu'elles entendent porter aux débats. Il est dans leur intérêt de ne produire qu'un nombre limité d'éléments de preuve qui seraient suffisants et pertinents pour permettre aux juges d'avoir la représentation la plus vraisemblable de la réalité. Il est à ce titre possible qu'une partie obtienne gain de cause dans une affaire grâce aux seules pièces produites par l'adversaire ou à l'absence de communication d'autres pièces.

706. **Démonstration complexe de la preuve.** En tout état de cause, la collecte, la sélection et la production des preuves est une véritable question stratégique d'une importance capitale. Pour autant, plus la démonstration de la preuve est complexe en ce que le procédé est technique, moins elle aura de chance d'emporter la conviction du juge. En effet, quand bien-même le procédé serait reconnu et éprouvé par des techniciens, le juge pourrait - par manque de compréhension - écarter les preuves *blockchains*. La technicité des preuves *blockchains* pourra ainsi avoir un effet négatif sur sa recevabilité mais, également, sur sa force probante. Le plaideur à qui il incombe de prouver, supportera en conséquence le risque qu'une preuve *blockchain* ne soit pas retenue, ou qu'elle ne soit pas considérée comme convaincante au fond par le juge[1449]. Les enregistrements de données par la *blockchain* impliquent donc une insécurité juridique pour le plaideur quant à la sélection des pièces à verser aux débats et possiblement quant à l'issue du procès au fond.

[1448] K. Haeri, Stratégie et tactique en matière de contentieux : éléments clefs, tvdma, UNJF, https://www.tvdma.org/video/strategie-et-tactique-en-matiere-de-contentieux-elements-clefs (consulté le 31/05/2020).
[1449] Ce risque est canalisé dans certains cas par une convention de preuve : voir *supra* n°683 et s.

Paragraphe 2 : Les risques de concurrence des juridictions traditionnelles avec le recours aux juridictions arbitrales

707. L'attentisme du juge face aux preuves *blockchains* génère une certaine concurrence des juridictions traditionnelles par des juridictions arbitrales. La *blockchain* attire des acteurs familiers du numérique, il semblerait logique que la résolution d'un litige associé empreinte la voie de la justice par des canaux similaires, comme l'arbitrage en ligne, un nouveau mode de résolution des litiges. L'arbitrage est reconnu pour « *son mode de résolution des litiges plus souple, lequel pourrait a priori, par sa dimension souvent internationale, par les moyens dont il profite parfois et par son adaptabilité, offrir le terreau d'expérimentation idéal du numérique dans la justice* »[1450]. Or, celui-ci constitue aussi un risque de concurrence des juridictions traditionnelles à deux niveaux : par son champ d'application matériel large (A) et sa mise en œuvre souple (B).

A. Le champ d'application matériel large de l'arbitrage international

708. **Définition moderne de l'arbitrage.** Si l'arbitrage n'est pas légalement défini[1451], il est possible de l'envisager comme « *l'institution par laquelle un tiers règle le différend qui oppose deux ou plusieurs parties, en exerçant la mission juridictionnelle qui lui a été confiée par celles-ci* »[1452]. À partir de cette définition, trois éléments doivent être dégagés de la notion d'arbitrage : c'est une institution visant à faire trancher un litige de manière définitive, par un ou plusieurs arbitres, qui tiennent leurs pouvoirs et statuent sur la base d'une convention privée sans être investis de cette mission par un État.

709. D'origine conventionnelle, l'arbitrage est concrètement une forme de justice privée, à laquelle des parties choisissent de recourir en lieu et place de la justice étatique[1453]. Cette « *justice privée* » est toutefois encadrée principalement par les articles 1442 à 1527 du Code de procédure civile, issus du décret n°2011-48 du 13 janvier 2011 portant réforme de l'arbitrage,

[1450] Club des Juristes, Rapport sur l'arbitrage en ligne, Commission ad hoc, Groupe de travail présidé par T. Clay, avr. 2019, p.6.
[1451] C. Jarrosson, *La notion d'arbitrage*, LGDJ, 1987, p. 368 ; J.-B. Racine, *Droit de l'arbitrage*, Thémis droit, Puf, 2016, p. 3.
[1452] C. Jarrosson, *La notion d'arbitrage*, *op.cit.*, p.372
[1453] Club des Juristes, Rapport sur l'arbitrage en ligne, *op.cit.*, p.7.

et offre des garanties dues par toute justice, celles du procès équitable. Notons que de plus en plus de formes d'arbitrage en ligne émergent comme mode juridictionnel privé de résolution des litiges par le numérique[1454].

710. **Objet large de l'arbitrage.** L'objet de l'arbitrage, matière litigieuse que l'on peut soumettre à l'arbitrage, est étendu. Selon l'article 2059 du Code civil « *toutes personnes peuvent compromettre sur les droits dont elles ont la libre disposition* ». Il y a en revanche des limites imposées par l'article 2060 du Code civil, qui ne permettent pas de « *(…) compromettre sur les questions d'état et de capacité des personnes, sur celles relatives au divorce et à la séparation de corps ou sur les contestations intéressant les collectivités publiques et les établissements publics et plus généralement dans toutes les matières qui intéressent l'ordre public. Toutefois, des catégories d'établissements publics à caractère industriel et commercial peuvent être autorisées par décret à compromettre* ».

711. Certaines matières sont traditionnellement considérées comme non-arbitrables comme les litiges de droit pénal, de droit de la famille, de droit administratif, de droit social, et ceux relatifs aux procédures collectives[1455].

B. La mise en œuvre souple de l'arbitrage international

712. L'une des trois caractéristiques saillantes de l'arbitrage, selon une étude de la *Queen Mary University of London* et *School of International Arbitration*, est sa décentralisation[1456], ce qui attire précisément les usagers d'une technologie de nature distribuée et décentralisée. La mise en œuvre de l'arbitrage appliquée à la technologie *blockchain* sera en ce sens particulièrement souple et adaptée, d'un côté par la flexibilité de la convention d'arbitrage (1), de l'autre côté, par la transnationalité de la sentence arbitrale (2).

[1454] Club des Juristes, Rapport sur l'arbitrage en ligne, *op.cit.*, p.7.
[1455] C. Jarrosson, B. Le Bars, JCl. Notarial Formulaire, Fasc. 10 : Arbitrage - Arbitrage commercial - Droit interne, Lexis Nexis, oct. 2013 (maj mars 2017), n°54-60 ; E. Loquin, Fasc. 1024 : Arbitrage - Conventions d'arbitrage - Conditions de fond. Litige arbitrable, JCl. Procédure civile, Lexis Nexis, mai 2016, n°50-64, n°81-112.
[1456] Queen Mary University of London, School of International Arbitration, International Arbitration Survey: Improvements and Innovations in International Arbitration, White and Case, 2015, p.6.

1. La flexibilité de la convention d'arbitrage

713. **Absence de condition de forme.** La convention d'arbitrage - visée aux articles 2059 à 2061 du Code civil - exige un écrit *ad validitatem* conforme au droit des contrats mais qui n'est soumis à aucune condition de forme[1457]. À titre illustratif, cet écrit peut exister sous forme électronique uniquement.

714. **Libre choix des règles de l'institution d'arbitrage, des règles de procédure, et des arbitres.** Les parties disposent d'une liberté contractuelle totale dans l'institution d'arbitrage, les règles de procédure, et les arbitres. Cette convention ne vise donc pas des droits substantiels mais le droit d'action : son objet est processuel[1458].

715. Il est possible de choisir le forum de l'arbitrage (siège et institution) ainsi que les règles applicables. L'article 19 des règles de la loi type de la CNUDCI sur l'arbitrage commercial international de 1985 précise que les « *(…) parties sont libres de convenir de la procédure à suivre par le tribunal arbitral. Faute d'une telle convention, le tribunal arbitral peut, sous réserve des dispositions de la présente Loi, procéder à l'arbitrage comme il le juge approprié. Les pouvoirs conférés au tribunal arbitral comprennent celui de juger de la recevabilité, de la pertinence et de l'importance de toute preuve produite* ». *A contrario,* les juridictions nationales semblent rigides au côté de l'arbitrage, dans la mise en œuvre de procédures qui se déroulent selon des règles de procédure fixes prédéfinies par le Code de procédure civile.

716. La convention d'arbitrage peut, enfin, directement ou par référence au règlement d'arbitre ou à des règles de procédure, désigner le ou les arbitres adéquats[1459]. La compétence technique des arbitres dans le droit et/ou dans le secteur concerné est choisie par les parties. Ce choix étant libre, celles-ci pourraient aisément désigner un ou plusieurs arbitres spécialisés (trois maximum) dans les sciences informatiques pour résoudre leurs litiges liés à la technologie *blockchain*. Des arbitres spécialisés dans le développement informatique pourraient également

[1457] C. pr. civ, art. 1507, al. 1. Voir aussi : J.-B. Racine, Fasc. 191 : Convention d'arbitrage - Formation, JCl. Contrats Distribution, Lexis Nexis, janv. 2012, n°5.
[1458] N. Coipel-Cordonnier, *Les conventions d'arbitrage et d'élection de for en droit international privé*, LGDJ, 1999, 431 p. ; J.-B. Racine, Fasc. 191 : Convention d'arbitrage - Formation, JCl. Contrats Distribution, Lexis Nexis, janv. 2012, n°2.
[1459] C. pr. civ, art. 1507, al. 2.

comprendre le langage du code des *smart contracts,* les rendant aptes à déterminer les intentions des parties.

2. La transnationalité de la sentence arbitrale

717. **Nature de la sentence arbitrale**. L'arbitrage est détaché des contraintes des lois nationales. Les sentences arbitrales internationales ne font pas partie de l'ordre juridique national mais constituent des décisions judiciaires internationales[1460]. À ce niveau, l'arbitrage parait adapté face à l'absence de point d'ancrage de la *blockchain*. C'est le cas pour une *blockchain* publique qui ne peut pas être localisée sur un point fixe mais en de multiples points, par les nœuds du réseau localisés partout dans le monde. Cet écheveau de circonstances permet difficilement de déterminer des règles de rattachement de droit national[1461].

718. **Support de la sentence arbitrale**. La sentence arbitrale pourra être rendue sur un support dématérialisé. Le nouvel article 4-2 de la loi Justice du XXIème siècle, modifié par l'article 4 de la loi n°2019-222 de programmation 2018-2022 et de réforme pour la justice du 23 mars 2019 énonce que « *la sentence arbitrale peut être rendue sous forme électronique, sauf opposition de l'une des parties* », ce qui favorise nettement l'arbitrage en ligne.

719. **Caractère exécutoire de la sentence arbitrale.** Les sentences arbitrales sont exécutoires dans les 159 pays ayant ratifié de la Convention pour la reconnaissance et l'exécution des sentences arbitrales étrangères de 1958, dite « *Convention de New York* ». La possible exécution de ces sentences arbitrales dans 159 pays différents emporte l'avantage d'être moulé à la nature transfrontalière de la *blockchain*. La facilité d'exécution des sentences était d'ailleurs une caractéristique essentielle mise en avant par l'étude de la *Queen Mary University of London* et *School of International Arbitration*[1462].

720. En somme, l'arbitrage a crû avec l'internationalisation des échanges commerciaux et des investissements à l'étranger pour toutes les raisons citées. Il se pourrait alors que l'arbitrage

[1460] Cass. civ. 29 juin 2007, n°05-18.053.
[1461] Voir *supra* n°162 et s.
[1462] Queen Mary University of London, School of International Arbitration, International Arbitration Survey: Improvements and Innovations in International Arbitration, *op.cit.*, p.6.

qui se veut « *coloré par la technologie et plus adapté à l'air du temps* »[1463] attire logiquement les acteurs de la *blockchain* par rapport aux juridictions judiciaires ordinairement compétentes.

Section 2 : Les propositions d'aide au renforcement de l'office du juge quant aux preuves de données enregistrées dans la *blockchain*

721. Pour anticiper les risques précités, il convient de les canaliser par un renfort de l'office du juge[1464]. L'office du juge est un terme très emprunté dans le domaine juridique mais peu défini précisément[1465]. Le rapport de l'Institut des hautes études sur la justice, sur l'évolution de l'office du juge et son périmètre d'intervention intitulé « *La prudence et l'autorité : l'office du juge au XXI*^{ème} *siècle* », rendu en mai 2013 au ministère de la justice, définit négativement l'office du juge qui « (…) *ne se confond ni avec son statut, ni avec sa légitimité, ni avec son rôle dans le procès, ni avec son périmètre d'action (même s'il en découle), ni avec l'acte de juger, ni enfin avec les différentes fonctions spécialisées qui se sont multipliées ces dernières décennies (par exemple le juge des enfants, le juge de l'application des peines ou le juge aux affaires familiales)* »[1466]. Le rapport ajoute que « *L'office est tout cela mais aussi plus que cela : il est le foyer de sens de la fonction de juger* »[1467]. Positivement, l'office du juge se fond dans l'acte juridictionnel qui « *traduit la fonction judiciaire dans son essence* »[1468], et se distingue de tout autre acte public, notamment l'acte administratif. L'acte juridictionnel même pourrait

[1463] L. Sinclair, « Arbitrage et nouvelles technologies : « rien ne se perd, rien ne se crée, tout se transforme » », Journal de l'arbitrage de l'Université de Versailles - Versailles University Arbitration Journal n°1, étude 5, janv. 2019.
[1464] Idée notamment soulevée aussi dans le Rapport sur les « *chantiers de la Justice »* qui prône en ce sens le renforcement de l'office du juge et vise à repenser les droits et devoirs des acteurs du procès (Rapport « Amélioration et simplification de la procédure civile », *in* J.-F. Beynel et a. (dir.), Rapport sur les « Chantiers de la Justice », Documentation française, 2018, p. 81 et s. (rapport remis au ministère de la Justice en janvier 2018 et ss. dir. F. Agostini (présidente du TGI de Melun) et N. Molfessis (Professeur)). Voir les commentaires : C. Brenner , « La réforme de la procédure civile : un chantier de démolition ? », D. 2018, p.361 ; S. Amrani-Mekki, « Les chantiers de la justice numérique, procédure civile et réseau des juridictions : le rationnel est-il toujours raisonnable ? », Gaz. Pal., 6 févr. 2018, n°312x8, p. 67 ; J. Théron, « Améliorer et simplifier la procédure civile : comment regagner la confiance des justiciables ? Aperçu rapide », JCP G 2018, p.237 ; C. Chainais, X. Lagarde (dir.), « Réformer la justice civile : séminaire de droit processuel – actes du colloque du 6 février 2018 », JCP G 2018 ; G. Guerlin, « La procédure civile en chantier », RLDC 2018, p.32-36, n°158.
[1465] Rapport de l'IHEJ, La prudence et l'autorité l'office du juge au XXIe siècle, *op.cit.*, p.15.
[1466] *Ibid*.
[1467] *Ibid*.
[1468] L. Cadiet, E. Jeuland, *Droit judiciaire privé*, Paris, LGDJ, 6^{e} éd., 2009, n°75 et s.

être défini, d'une part, d'un point de vue formel par la méthode propre suivie de l'acte de juger[1469], et d'autre part, d'un point de vue substantiel, par sa fonction[1470].

722. L'office du juge peut être classifié méthodiquement de trois façons : selon sa source (office légal, office principiel, office consciencieux), son objet (office processuel, office de vérité, office sanctionnateur, office libéral, office tutélaire), ou encore son intensité (office virtuel, office autorisation, plein office)[1471]. Aider au renfort de l'office consciencieux guidé par la conscience de juge et l'office de vérité lui permettrait d'établir pendant l'instance l'exacte qualification et de déclarer la vérité juridictionnelle au moment de la décision, dans le secteur de la *blockchain*. Il est pertinent que le juge soit à même d'appliquer pleinement son pouvoir, tant par un seuil de connaissances et compétences relatif à la technologie *blockchain* (paragraphe 1), que dans le cadre d'une infrastructure juridictionnelle dédiée, telle qu'une juridiction numérique pilote pour les contentieux concernant la technologie *blockchain* (paragraphe 2).

Paragraphe 1 : La pertinence d'un seuil de connaissances et compétences des juges concernant la technologie *blockchain*

723. En vue d'harmoniser les connaissances et les compétences des juges, un soutien et un accompagnement dans l'acculturation à cette technologie sera projeté par la dispense de formation professionnelle continue concernant les technologies *blockchains* (A) dans la juste lignée d'une « *adaptation du service public de la Justice à la culture numérique* »[1472] d'une part, et un devoir de compétences techniques concernant cette technologie (B) d'autre part.

[1469] Dans ce cas, l'office reposerait sur trois critères : l'organe, la procédure et l'indépendance du juge. Serait juridictionnel l'acte émanant d'un juge étatique statuant au terme d'une procédure contradictoire (Rapport de l'IHEJ, La prudence et l'autorité l'office du juge au XXIe siècle, *op.cit.*, p.15-16).

[1470] La fonction distingue la fonction de juger et celle de dire droit. La fonction de juger est la mission de trancher un litige, c'est-à-dire de décider entre des prétentions contraires juridiquement argumentées (Rapport de l'IHEJ, La prudence et l'autorité l'office du juge au XXIe siècle, *op.cit.*, p.16). La fonction juridictionnelle de dire droit, pour Stéphane Rials, « *se borne au dire (jurisdictio) obligatoire (imperium) du droit* » (S. Rials, « Ouverture. L'office du juge », Droits. Revue française de théorie juridique, n°9, « La fonction de juger », PUF, 1989, p.6). Selon Duguit, la *juridictio* comporte deux opérations indivisibles, celle de constatation initiale d'un droit subjectif ou d'une violation de la loi, qui fera découler celle la sentence judiciaire (L. Duguit, « L'acte administratif et l'acte juridictionnel », RDP, 1906, p.413-471).

[1471] Rapport de l'IHEJ, La prudence et l'autorité l'office du juge au XXIe siècle, *op.cit.*, mai 2013, p.18.

[1472] Ministère de la Justice, Rapport « Transformation numérique de la justice » ss. dir. J.-F. Beynel et D. Casas, *in* Rapport sur « les chantiers de la justice », janv. 2018, p.6.

A. La dispense de formation professionnelle continue aux juges concernant les technologies *blockchains*

724. **Formation continue des magistrats.** Contrairement à la formation initiale - première formation obtenue au terme d'un cycle d'étude -, la formation continue permet à tout individu d'acquérir des savoirs lorsqu'il a déjà intégré la vie active. La formation continue des magistrats, instaurée par le décret n°72-355 du 4 mai 1972 relatif à l'École nationale de la magistrature[1473], leur permet classiquement de renforcer leurs compétences techniques et de se spécialiser tout au long de leur vie professionnelle. Elle revêt un caractère obligatoire pour tous les magistrats depuis le 1er janvier 2008[1474].

725. **« *Crypto-alphabétisation* » des magistrats.** Si sept axes de formation très complets sont déjà fixés par la formation continue de l'École nationale de la magistrature pour répondre aux exigences d'une démocratie moderne et aux attentes des justiciables, il n'en demeure pas moins que deux d'entre eux mériteraient d'être revalorisés. Le concours à l'ouverture du corps à son environnement économique, social et culturel, et le travail de l'approche pluridisciplinaire des thèmes[1475] se prêtent ainsi à la dispense d'une unité d'enseignement dans la culture numérique et à l'approfondissement particulier de la technologie *blockchain*, qui serait une forme de « *crypto-alphabétisation* » des magistrats. Cette notion rejoint celle de « *data-alphabétisation* » ou *data literacy* signifiant littératie des données ou culture des données, qui est la capacité d'identifier, de collecter, de traiter, d'analyser et d'interpréter des données afin de comprendre les phénomènes, les processus, les comportements qui les ont générées[1476]. Dans la crypto-alphabétisation, il serait question de développer des capacités pour l'identification, la collecte, le traitement, l'analyse et l'interprétation de différentes preuves cryptographiques liées à la *blockchain* dans l'objectif de comprendre ces preuves pour soit les utiliser, soit les interpréter. Selon, l'*EU blockchain observatory* dès lors que les tribunaux seront plus sensibilisés et informés au sujet de la *blockchain*, ils seront mieux placés pour évaluer si les solutions

[1473] Décret n°72-355 du 4 mai 1972 relatif à l'Ecole nationale de la magistrature.
[1474] http://www.enm.justice.fr/formation-continue-francais (consulté le 31/05/2020).
[1475] *Ibid*.
[1476] https://www.lesechos.fr/idees-debats/cercle/cercle-166504-la-data-literacy-ou-la-culture-de-la-donnee-le-prochain-enjeu-de-nos-societes-2066367.php consulté le 31/05/2020).

d'horodatage *blockchains* pourront être admissibles, au regard du règlement eIDAS par exemple[1477].

726. **Illustration du besoin des juges fédéraux de Duke.** Un sondage a été mené aux États-Unis par l'Université de droit de Duke en 2019 auprès des juges fédéraux de Duke sur leur satisfaction du niveau de connaissance technologique et pratique concernant la procédure d'*e-discovery* relative à la recherche et de la communication des preuves électroniques. Alors que sur 260 juges auditionnés, 30% se déclaraient satisfaits de leur niveau de connaissance relatif à la technologie de l'*e-discovery* et à sa pratique et ne pensaient pas avoir besoin de formations professionnelles et théoriques supplémentaires, 63% déclaraient en avoir besoin. En ce sens, 70% des juges souhaitent une augmentation raisonnable de ces formations, alors que 22% des juges ne considéraient pas celles-ci indispensables[1478]. Un parallèle avec le niveau de connaissances et de compétences des juges français dans la recherche de la preuve numérique et le besoin de formation y afférent peut être opéré. Ces formations continues ont assurément vocation à renforcer la confiance des plaideurs en nos juridictions. Celles-ci permettraient par ailleurs d'impliquer davantage les institutions judiciaires françaises dans la connaissance fine de la technologie *blockchain*, parfois indispensable en matière pénale[1479].

B. Le devoir de compétences techniques des juges concernant la technologie *blockchain*

727. **Obligation de compétence technique minimale.** La technologie s'introduit ubiquitairement dans la pratique du droit et imprègne de fait le travail des juges. Pour faire face à ce phénomène, une obligation de compétence technique minimale en matière de technologie, et plus spécifiquement concernant la technologie *blockchain* à la charge des juges, semble à propos.

[1477] EU Blockchain Observatory and Forum, Legal and regulatory framework of *blockchains* and smart contracts, le 28 sept. 2019, p.12 : « *As authorities, including regulators and the courts, become more aware and knowledgeable about blockchain, they will be in a better position to evaluate whether blockchain-based timestamping solutions can qualify under the eIDAS framework. We believe they should be enabled and encouraged to continue to deepen their understanding in this area* ».
[1478] Externo and EDRM/Duke Law, Judges survey 2019, A survey of industry trends, practices, and /challenges faced, 2019, p.14
[1479] Voir *supra* n°586 et s.

728. La compétence dans l'exercice des fonctions judiciaires exige des connaissances juridiques, la rigueur et la préparation raisonnablement nécessaires à l'exercice des fonctions judiciaires d'un juge. Désormais c'est un vernis de compétence technique qui devient utile pour faire face à un contentieux complexe enchevêtré à la technologie. Qui plus est, le juge doit pouvoir évaluer le poids du rapport d'expertise en fonction de sa propre expertise et de son expérience[1480]. Sa compétence technique est ainsi au cœur de la réflexion du renforcement de son office.

729. **Influencer par ricochet les pratiques éthiques.** Il n'y a pas cependant formellement de mention ou de suggestion sur le devoir de compétence technologique pour les juges français. Nonobstant son utilité certaine pour les questions au fond posées aux juges impliquant des interrogations techniques liées à la technologie de registres distribués parfois très complexes, ou encore les détections d'usages illicites, bien au-delà, ce devoir pourrait permettre de comprendre les implications culturelles et sociologiques de cette technologie. Considérant ces implications, les juges - *via* leur office - pourraient alors influencer par ricochet les pratiques éthiques liées à son utilisation.

730. **Illustration du devoir de compétence technique dans les Codes de déontologie aux États-Unis.** En 2012 aux États-Unis, l'*American Bar Association* a révisé son *Model Rules of Professional Conduct*, un modèle de Code de déontologie des avocats intégrant un devoir compétence des avocats non seulement en droit et dans la pratique, mais aussi technique. Le « *comment 8 to Model Rule 1.1* » inclut désormais que les avocats ont la responsabilité de se tenir informés des changements dans la loi et la pratique, « *y compris les avantages et les risques associés à la technologie en question* ». Trente-six États fédérés auraient adopté cette règle[1481]. Dans le Code sur la déontologie judiciaire, le corollaire de la *Model Rule 1.1* sur la compétence des avocats est la règle 2.5 qui dispose que « *le juge exerce ses fonctions judiciaires et administratives avec compétence et diligence* »[1482]. Ce devoir de compétence des juges est moins abouti que celui des avocats. Le commentaire relatif à la règle 2.5 est large mais n'intègre pas littéralement la compétence technologique. Il précise que « *la compétence dans l'exercice*

[1480] K. Favro, M. Lobé Lobas, J.- P. Markus (ss. dir.), *L'expert dans tous ses états.* À *la recherche d'une déontologie de l'expert*, coll. Thèmes et commentaires, Dalloz, nov. 2016, p.113. Voir aussi les développements *infra* n°869 et s.

[1481] https://www.lawsitesblog.com/tech-competence (consulté le 31/05/2020).

[1482] https://www.americanbar.org/groups/professional_responsibility/publications/model_code_of_judicial_conduct/ (consulté le 31/05/2020).

des fonctions judiciaires exige les connaissances juridiques, la compétence, la rigueur et la préparation raisonnablement nécessaires à l'exercice des fonctions judiciaires d'un juge ».

731. En 2018 toutefois, un juge basé à New York a démissionné alors qu'il faisait face à plusieurs chefs d'accusation portés par la *New York State Commission on Judicial Conduct* sur le fondement de manquements à des obligations judiciaires, administratives et financières[1483]. Entre autres, deux accusations relatives à son incompétence technologique portaient sur l'absence de consultation et réponse aux courriels de sa boîte e-mail officielle du tribunal pendant plus de trois ans, et également l'absence d'activation et d'usage d'un ordinateur et d'un logiciel fournis par le Bureau de l'administration des tribunaux pour l'administration financière et des affaires du tribunal, pendant plus d'un an. Cet exemple américain particulièrement éloquent prouve que les juges doivent répondre de leurs compétences techniques pour assurer le maintien du service public.

Paragraphe 2 : La pertinence d'une juridiction numérique pilote pour les contentieux concernant la technologie *blockchain*

732. Le sujet n'est pas d'avancer et d'imaginer des modèles de tribunaux intégralement solubles dans le numérique. Le Secrétaire général du ministère de la justice française en 2018, Stéphane Verclytte, exprimait que les outils numériques, et ainsi un tribunal pilote, ne doivent pas de toute évidence se substituer à l'indépendance et prééminence de l'intervention du juge lui-même[1484]. Il est ici question pour cette expérimentation de transposer un tribunal traditionnel avec l'adoption d'une « *logique numérique* ». Le Rapport sur la transformation numérique de la justice propose des changements par le numérique au sein des tribunaux (phase initiale dans laquelle les parties discutent librement par voie numérique, phase pré-contentieuse qui se caractériserait par le dépôt d'une saisine par voie numérique, phase contentieuse durant laquelle les écritures et les pièces numérisées seraient versées à un dossier numérique unique[1485]). Or, même si des propositions sont réalisées durant la phase contentieuse pour une audience civile

[1483] News release, New York State Commission on Judicial Conduct, Dec. 13, 2018, http://cjc.ny.gov/Press.Releases/2018.Releases/Scolton.Bruce.S.Release.2018-12-13.pdf (consulté le 31/05/2020).
[1484] S. Verclytte, « Les pré-requis du tribunal numérique », Conférence internationale sur la Justice de Marrakech, 3 avr. 2018.
[1485] Ministère de la Justice, Rapport « Transformation numérique de la justice », *op.cit.*, p.11, 12, 15.

facilité et interactive, elles sont essentiellement d'ordre matériel se tournant uniquement - mais non sans utilités - sur les outils numériques à mettre à disposition des juridictions[1486].

733. Il conviendrait dans le cadre de notre proposition de s'inspirer du modèle des Tribunaux de l'Internet chinois traitant de contentieux sur le numérique. Afin d'anticiper ces technologies de rupture, il serait possible d'importer et d'adapter ce modèle par un tribunal au départ à compétence nationale, puis de ressort international en fonction de son succès, avec une composition (A) et une compétence matérielle (B) bien particulières.

A. La composition de la juridiction numérique pilote

734. **Juges spécialisés dans le domaine du numérique.** La juridiction pilote projetée serait composée de juges spécialisés en numérique aux confins du droit et de la technique. Au-delà d'être imprégnés d'une culture socio-professionnelle forte du numérique, les juges qui y siègeraient, auraient un socle de connaissances techniques en numérique, incluant la technologie *blockchain*, leur permettant de rendre leur jugement avec discernement et clairvoyance. À titre d'illustration, le grand projet de Juridiction Unifiée du Brevet (JUB) - encore à l'avenir incertain[1487] - prévoit la nomination de magistrats dans les différentes chambres de la juridiction, lesquels devront avoir une expérience en matière de brevets d'invention. Si certains juges auront une formation exclusivement juridique, d'autres auront également une formation technique et participeront, dans certains cas, aux décisions. Les décisions rendues par une formation de magistrats plutôt mixte et hautement spécialisée en matière de brevets harmoniseraient la jurisprudence en matière de contrefaçon et de validité des brevets[1488]. En définitive, l'idée de la composition de cette juridiction numérique n'est pas de constituer un cénacle d'experts en vase clos qui n'ont pas officiellement la *juridictio* car cette dernière est entre les seules mains d'un juriste qui connaît le droit. Mais elle serait tournée vers des magistrats ayant, en plus du droit, un socle de base de savoirs en numérique.

[1486] Ministère de la Justice, Rapport « Transformation numérique de la justice », *op.cit.*, p.18.
[1487] C. Meiller, V. Chapuis, « Brevet : sale temps pour la juridiction unifiée du brevet », Dalloz actualité, 8 avr. 2020, p.1-2.
[1488] https://www.epo.org/law-practice/unitary/upc_fr.html (consulté le 31/05/2020).

735. **Modalité des nominations des juges de la juridiction numérique.** Cette juridiction serait accessible sur concours et sur dossier selon les mêmes modalités traditionnelles à l'exception que seuls les profils ayant une double compétence (une compétence majeure et une mineure) seraient admis. Il conviendrait qu'ils aient été reçus sur une formation juridique validée de second cycle (majeure) et une formation en sciences informatiques validée de premier cycle (mineure) ou inversement une formation de second cycle en sciences informatiques validée (majeure) et une formation juridique de premier cycle validée (mineure). L'idée de cette double compétence alternative serait de créer une complémentarité et une synergie entre les deux profils de magistrats.

736. **Formation initiale de la juridiction numérique.** La formation initiale de la juridiction numérique pilote serait accordée sur une promotion identique à celle existante d'une vingtaine de magistrats détachés à l'École nationale de la magistrature[1489]. Si l'objectif de la formation initiale est d'acquérir les compétences communes fondamentales classiquement requises à toutes les fonctions de magistrat[1490], la différence résiderait dans les enseignements dispensés pour développer d'autres connaissances techniques, comme la parfaite maîtrise des techniques du droit des nouvelles technologies, et la capacité essentielle à appréhender les enjeux humains et de sociétés générés par les nouvelles technologies. Au-delà d'une simple culture numérique, il s'agira de développer de nouvelles compétences adaptées au monde des nouvelles technologies : un esprit d'anticipation, de logique et d'analyse technique.

Ce projet pilote original permettrait d'articuler le numérique autour de la justice et dans la justice pour résoudre les litiges portant sur le numérique. C'est une projection de juridiction très spécialisée en soi.

B. L'objet des litiges portés devant de la juridiction numérique pilote

737. **Contentieux liés au numérique.** Il serait question pour les magistrats de rendre des décisions réservées à un certain contentieux spécifique, portant sur des litiges avec un niveau de technicité élevé dont les faits auraient trait à des activités liées au numérique incluant la technologie *blockchain*. Le juge se devra de trancher tous les points en conflit conformément

[1489] https://www.enm.justice.fr/formation-initiale-francais (consulté le 31/05/2020).
[1490] http://www.enm.justice.fr/Pedagogie-ENM (consulté le 31/05/2020).

aux règles de droit des nouvelles technologies et d'autres branches du droit. Les contentieux uniquement civils impliquant exclusivement des éléments sur des technologies avancées seront les critères d'attribution permettant de déterminer lorsqu'un litige est du ressort ou non de cette juridiction. Le numérique étant un secteur transversal mobilisant différentes branches du droit (droit des contrats, droit commercial, droit de la concurrence, droit pénal, droit de la santé, droit social, droit administratif etc), cette compétence matérielle précise de la juridiction pilote permettra d'éviter l'engorgement de cette dernière.

738. Pour reprendre l'exemple de la JUB, qui semble être celui le plus parlant, cette Cour a été créée au titre de l'Accord du 19 février 2013 relatif à une Juridiction unifiée du brevet[1491] pour connaître exclusivement des affaires de contrefaçon et de validité des brevets unitaires ainsi que des brevets européens[1492]. Seuls les litiges relatifs à des actions en contrefaçon, en constatation de non-contrefaçon, les mesures provisoires, les actions en nullité, en dommages et intérêts ou en réparation devront être portés devant cette juridiction[1493].

739. **Maîtrise du contentieux sur les technologies de rupture.** En conséquence, l'action de traiter les litiges axés sur l'environnement du numérique par des magistrats formés et issus de ce secteur permettra d'avoir une bonne maitrise du contentieux sur les technologies très pointues de rupture afin de mieux les appréhender. Plus encore, elle offrira la possibilité de mettre notre service public compétent à disposition du numérique, renversant la logique habituelle consistant à *« placer l'innovation au service d'une Justice moderne, au bénéfice des usagers, des magistrats et des fonctionnaires du ministère et des partenaires* »[1494].

740. **Conclusion du chapitre 2.** En conclusion de ce deuxième chapitre, des risques manifestes quant à l'attentisme du juge dans l'appréciation des preuves de données enregistrées dans la *blockchain* exposent d'un côté le justiciable à une rupture d'égalité devant la justice et une insécurité juridique dans sa stratégie probatoire, et de l'autre côté les juridictions à la concurrence de l'arbitrage. Des mesures de formation professionnelle continue des juges et des devoirs de compétences techniques concernant la technologie *blockchain* seraient de nature à renforcer l'office du juge quant à ces données enregistrées dans la *blockchain*. Qui plus est,

[1491] JO OEB 2013, 287.
[1492] https://www.unified-patent-court.org/ (consulté le 31/05/2020).
[1493] A. Michelet, « La juridiction unifiée du brevet : où en sommes-nous ? », Popr. Indus. n°3, étude 5, mars 2018, p.5, n°4.
[1494] Ministère de la Justice, Rapport « Transformation numérique de la justice », *op.cit.*, p.6.

l'expérimentation d'un tribunal numérique pilote ayant compétence pour les contentieux civils impliquant exclusivement des éléments sur des technologies avancées, et composé de juges spécialisés en numérique aux confins du droit et de la technique pourrait permettre d'anticiper ces technologies de rupture. Ces propositions sont autant de solutions préconisées en amont pour pallier les nombreux risques, alors que ce type de contentieux n'envahit pas encore les prétoires.

741. **Conclusion du titre 1.** En définitive, ce premier titre a permis de mettre en relief l'intervention prudente d'un juge démuni dans la reconnaissance des preuves de données enregistrées dans la *blockchain*. La recherche de preuves support d'infractions souffre de manque de moyens matériels, alors que l'appréciation des preuves par le juge français est quasi-inexistante. Même si le plaideur, au bénéfice duquel le principe de liberté de la preuve serait accordé, se placerait sur un terrain plus favorable à la réception de ces preuves par le juge, seule la pratique judiciaire pourra permettre de révéler ces preuves blockchains (incluant l'*obiter dictum* devant les juridictions suprêmes). Cette appréciation prudente exposerait tantôt la personne jugée que l'institution qui juge, à des risques. Le « *bras séculier* » pourrait s'en trouver ainsi ébranlé. L'approche prophylactique étudiée permet de mettre en avant des propositions venant prévenir ce danger.

742. Spécifiquement en matière pénale, des moyens technologiques d'investigation renforcés, compatibles avec de nombreux crypto-actifs, devront être mis à la disposition des services d'enquête (agents et officiers de police judiciaire, TRACFIN, et cyberdouanes) pour chercher les preuves. Afin d'établir et coordonner ces mesures au niveau international, le CMII pourrait être désigné.

743. De façon générale, des moyens visant à prévenir et outiller les juges semblent adéquats pour asseoir leur légitimité. Il s'agirait d'un côté, de renforcer les connaissances et compétences des juges et de l'autre côté, d'établir un tribunal numérique pilote pour le contentieux civil hautement spécialisé sur des technologies avancées.

744. Néanmoins, les juges ne possèdent pas pour le moment toutes les connaissances techniques nécessaires à la compréhension de ces preuves. Or, ils se reposent pour l'heure sur la possibilité qui leur est offerte de faire intervenir les huissiers et les experts. Sur des questions aussi techniques que ces preuves *blockchains*, les juges pourraient se retrouver confrontés à des

interrogations sur des faits dont la résolution dépasse leurs compétences professionnelles et personnelles. Les juges font et feront dans ce cadre appel à des spécialistes et des auxiliaires de justice.

TITRE 2

L'INTERVENTION EXTRA-JURIDICTIONNELLE DEMESUREE DANS LA RECONNAISSANCE DES PREUVES DES DONNEES ENREGISTREES DANS LA *BLOCKCHAIN*

745. La première phase de construction politique de la *blockchain* avait pour but de désintermédier pour supprimer le tiers de confiance, mais l'entrée dans la seconde phase de structuration des activités de *blockchain* a sonné le glas d'une nécessaire identification des tiers de confiance dont l'intervention s'avère primordiale pour démystifier les preuves *blockchains*.

746. De longue date, le droit a prévu l'intervention des experts et des huissiers de justice. Depuis l'ordonnance civile de 1667 - unifiant et codifiant pour la première fois les règles de procédure civile -, le recours aux experts est possible[1495]. Avant la réforme de la procédure civile de 1973, l'expertise était le seul mode de recours aux spécialistes des questions de fait[1496]. La pratique judiciaire a vu se développer les « *constats d'audience* ». Très usités, ils consistaient à confier à l'huissier de justice chargé de la police de l'audience le soin de procéder à des constatations[1497]. Cette pratique fut consacrée par un décret du 20 mai 1955 modifiant le statut des huissiers de justice et intégrant par ailleurs dans le Code de procédure civile deux autres mesures d'instruction : la constatation et la consultation[1498].

747. Les auxiliaires de justice aident encore très souvent à notre époque le juge à la collecte et à la traduction des preuves complexes. Le juge peut en effet prescrire une mesure d'instruction telle que des constatations, consultations, voire des expertises. Les parties ont aussi l'occasion par elles-mêmes de prendre l'initiative d'une constatation ou d'une mesure d'expertise. Cette intervention extra-juridictionnelle peut sembler démesurée à certains égards

[1495] Ordonnance de Louis XIV, avril 1967. Voir : T. Moussa, F. Arbellot, F. Delbano, D. Loriferne, J.-P. Martin, P. Matet, V. Vigneau, *Droit de l'expertise 2016/2017*, ss. dir. de T. Moussa, 3e ed., Dalloz action, dec. 2015, p.78, n°211-16.
[1496] *Ibid*.
[1497] *Ibid*.
[1498] Décret n°55-604 du 20 mai 1955 relatif aux officiers publics ou ministériels et à certains auxiliaires de justice.

dans la reconnaissance des preuves des données enregistrées dans la *blockchain*. Les preuves cryptographiques considérées comme particulièrement techniques sur ces réseaux décentralisés nouveaux feraient intervenir des experts ou huissiers de justice en appui - probablement excessif - du juge (chapitre 1). Nous exposerons alors des palliatifs aux risques d'atteinte à l'indépendance de la justice (chapitre 2).

CHAPITRE 1
LES ATTENTES EXCESSIVES DU JUGE ET DES PARTIES ENVERS LES HUISSIERS ET EXPERTS DE JUSTICE EN MATIERE DE PREUVES DES DONNEES ENREGISTREES DANS LA *BLOCKCHAIN*

748. Les huissiers et les experts de justice prêtent main forte au juge aidant au déchiffrage des preuves auprès des juridictions[1499]. Si cette tâche n'est pas des moindres, les attentes qu'ils suscitent en matière de preuves *blockchains* pourront être excessives. Face à ces attentes et projections excessives, le rôle des huissiers de justice mobilisés par les acteurs économiques au soutien du constat de ces preuves en amont d'un litige se révèle en pratique subsidiaire (section 1). À l'inverse, celui des experts informatiques à requérir au soutien de la traduction de ces preuves par le juge en cours de procédure est significatif (section 2).

Section 1 : Le rôle subsidiaire des huissiers de justice mobilisés par les acteurs économiques au soutien du constat des preuves de données enregistrées dans la *blockchain* en amont d'un litige

749. L'intervention de l'huissier de justice dans les preuves de données enregistrées dans la *blockchain* est - pour partie - mobilisée en amont des litiges par des acteurs économiques au soutien du constat de ces preuves. Il sera avant tout opportun d'établir le régime juridique du constat des enregistrements de données dans la *blockchain* (paragraphe 1), pour ensuite en dégager sa portée probatoire, semble-t-il moindre (paragraphe 2).

[1499] Le Professeur Mustapha Mekki perçoit les professionnels du droit non comme des « *ouvriers numériques* » au service de la *blockchain* mais comme des « *oeuvriers du numérique* » dans leur interaction avec la technologie *blockchain* (M. Mekki, « Blockchain et métiers du droit en questions », Dossier « Blockchain et métiers du droit : une force vive ou subversive ? », *op.cit.*, p. 89.

Paragraphe 1 : Le régime juridique du constat des enregistrements de données dans la *blockchain*

750. Le constat est défini comme l'hypothèse où l'huissier de justice est requis à titre principal ou exclusif, pour relater en principe dans un écrit, et conserver à titre de preuve un certain nombre d'éléments de faits susceptibles d'entraîner des conséquences de droit à l'occasion d'un procès[1500]. Le régime juridique du constat des enregistrements de données dans la *blockchain* sera somme toute similaire à d'autres constats, comme le constat portant sur un site Internet. Nous présenterons alors ce régime en deux temps avec, tout d'abord, la forme du constat des enregistrements de données dans la *blockchain* (A), puis l'objet du constat des enregistrements de données dans la *blockchain* (B).

A. Les typologies des constats des enregistrements de données dans la *blockchain*

Une *summa divisio* doit être dressée entre les constats des enregistrements de données dans la *blockchain* en fonction de l'origine de la demande (1) et en fonction du moment de leur intervention (2).

1. Les types de constats d'enregistrements de données dans la *blockchain* en fonction de l'origine de la demande

751. **L'huissier commis par la justice ou à la requête des parties.** Selon le deuxième alinéa de l'article 1 de l'ordonnance n°45-2592 du 2 novembre 1945 relative au statut des huissiers, c'est commis par la justice ou à la requête des parties que l'huissier de justice peut effectuer des constatations purement matérielles, exclusives de tout avis sur les conséquences de fait ou de droit qui peuvent en résulter. Les constats peuvent ainsi être de deux ordres, soit le constat est réalisé sur commission du juge, soit le constat est établi sur réquisition directe du justiciable. Cette distinction entraîne des conséquences sur le contexte qui les entoure[1501]. Lorsque le constat est diligenté sur ordonnance d'un juge, il ne pourra être dressé que par un huissier de

[1500] R. Perrot, « Le constat d'huissier de justice », CNHJ, 1985, p.7.
[1501] S. Dorol, Fasc. 30 : Constat d'huissier de justice, JCl. encyclopédie des Huissiers de Justice, Lexis Nexis, avr. 2015 (maj 27 dec. 2018), n°6.

justice, alors que s'il est diligenté à la requête d'un particulier, il peut être réalisé par un huissier de justice ou son clerc habilité[1502].

752. **La requête de personnes morales ou physiques en pratique.** Pour l'heure, ce sont surtout les constats à la requête de personnes morales ou physiques qui sont établis dans les activités de données enregistrées dans la *blockchain*. Ce constat est par nature destiné à constituer des éléments de preuve pour le requérant, qui pourront être produits lors d'un litige[1503].

753. **Les constats utiles dans les contentieux en contrefaçon, diffamation et informatique.** Il est certain qu'en matière de contentieux en contrefaçon - indépendamment d'une éventuelle preuve *blockchain* -, le constat sur requête du particulier est très utile puisqu'il permet d'accorder en toute objectivité la preuve de l'œuvre contrefaisante. C'est également le cas dans le contentieux en diffamation dont le contenu est susceptible d'être rapidement supprimé ou perdu, alors que les risques réputationnels peuvent être considérables en peu de temps. Si dans le contentieux informatique, les écrits électroniques vivants et en perpétuelle évolution ne peuvent être saisis que par des « *photographies* » horodatées[1504], il n'en demeure pas moins que celui qui portera sur la *blockchain* semble différent.

754. **La critique du constat *blockchain*.** Le registre de la *blockchain* n'est pas amené à se transformer, sauf à ajouter de nouvelles transactions, mais l'ensemble des transactions déjà validées reste immuable : le registre est donc stable. De ce fait, il n'y a très peu de risque de perdre des données enregistrées. L'usage du constat d'huissier sur demande d'un particulier n'est donc pas exempt de critiques tant il sert à « *légitimer* » l'activité économique de certains nouveaux acteurs souhaitant réaliser des prestations de service sur les ancrages dans la *blockchain*[1505]. Ce constat matériel peut alors sembler artificiel faisant émerger une « *double preuve* » superficielle et présentant davantage les caractéristiques d'un argument commercial, que ceux d'un acte nécessaire.

[1502] S. Dorol, Fasc. 30 : Constat d'huissier de justice, JCl. encyclopédie des Huissiers de Justice, Lexis Nexis, avr. 2015 (maj 27 dec. 2018), n°7-8.
[1503] J. D. Lachkar, « La force probante de l'acte d'huissier de justice », JCP N n°5, févr. 2013, p.42 ; S. Dorol, « Blockchain et métiers du droit : la fin des tiers de confiance ? », Dossier « Blockchain et métiers du droit : une force vive ou subversive ? », Dalloz IP/IT n°2, févr. 2020, p.94.
[1504] H. Croze, « La preuve par huissier de justice », Gaz. pal. n°148, mai 2013, p.9.
[1505] Voir un avis contraire : P. Sannino, « « Disruption », Justice prédictive, Blockchain, legaltech : de nouvelles opportunités pour la profession ? », Procédure n°12, entretien 1, dec. 2017, p.3.

2. Les types de constats d'enregistrements de données dans la *blockchain* en fonction du moment de leur intervention

755. **Le constat avant tout procès.** Conformément à l'article 145 du Code civil, « *s'il existe un motif légitime de conserver ou d'établir avant tout procès la preuve de faits dont pourrait dépendre la solution d'un litige, les mesures d'instruction légalement admissibles peuvent être ordonnées à la demande de tout intéressé, sur requête ou en référé* ». Généralement, le constat est ordonné sur requête quand le contradictoire est impossible ou inopportun[1506]. Le constat est dressé sur ordonnance de référé en dehors de cette première hypothèse.

756. **Le constat d'audience en cours de procès.** Le juge peut diligenter des constations dans le cadre de mesures d'instruction[1507], et plus généralement à tout moment de l'instance (y compris en conciliation ou délibéré)[1508]. Pour ce dernier cas, l'article 259 du Code de procédure civile indique que le juge peut « *charger la personne qu'il commet de procéder à des constatations* ». Il ne précise pas strictement qu'un huissier peut être la personne qui procède à ces constatations. La jurisprudence apporte des éclaircissements à ce sujet en autorisant que soit désigné un huissier de justice audiencier, comme constatant au sens de cet article, mais pas en qualité d'officier ministériel, dès lors que l'objet de la mesure prescrite est limité[1509].

757. **Un constat des enregistrements de données dans la *blockchain* avant tout litige.** En pratique, le constat de données enregistrées dans la *blockchain* est souvent exigé à la requête d'une personne morale, un prestataire de solutions *blockchains* au soutien du constat des preuves de données enregistrées dans la *blockchain* pour ses clients. Il sera donc usuellement réalisé en amont d'un litige. Il a pour but de se ménager une preuve « *sûre* » dressée par un huissier en amont, mais elle se révèle être une preuve chimérique à terme puisque le registre distribué d'une *blockchain* et le constat assurent des fonctions quasi-similaires d'enregistrement et de conservation[1510]. En revanche, de manière à éviter l'effet négatif de ces preuves lié à leur complexité, le plaideur aura tout intérêt à se ménager ce constat en amont afin d'être en mesure d'expliquer les preuves techniques de la *blockchain*.

[1506] C. pr. civ., art. 812.
[1507] C. pr. civ., art. 232.
[1508] C. pr. civ., art. 250.
[1509] Cass. 2ème civ., 23 juin 2011, n°10-18.540, inédit : Procédures 2011, note L. Lauvergnat.
[1510] Voir la place de la fonction d'enregistrement et de conservation probatoire de l'huissier : H. Croze, « La preuve par huissier de justice », *op.cit.*, p.11.

B. L’objet du constat des enregistrements de données dans la *blockchain*

758. L’absence de définition légale du constat mais seulement de son objet est révélatrice de l’unique constatation matérielle possible d’un fait juridique enregistré dans la *blockchain* par l’huissier.

759. **Constatations purement matérielles.** Seul l’objet du constat est défini par l’ordonnance du 2 novembre 1945 et les articles 249 et suivants du Code de procédure civile. En effet, selon le premier article de l’ordonnance du 2 novembre 1945, cet acte ne doit porter que sur des « *constatations purement matérielles, exclusives de tout avis sur les conséquences de fait ou de droit qui peuvent en résulter* ». Si les termes « *constatations purement matérielles* » sont relativement obscurs[1511], la notion de matérialité est plus explicite mais ne saurait s'apparenter à l’unique existence physique de l’objet à constater car cela exclurait les constatations sur Internet. La doctrine éclaire cette notion de « *constatation matérielle* ». Selon le Professeur Roger Perrot, elle comprend « *(…) tout ce qui peut être perçu directement par les* (différents) *sens* »[1512] : la vue, le toucher, l’ouïe, l’odorat ou encore le goût. L’huissier de justice Sylvian Dorol ajoute qu’elle représente « *(…) toute situation personnellement constatée par l'huissier de justice au moyen de ses sens, et qu'il n'a pas provoquée par une opération intellectuelle de nature à troubler sa qualité de tiers neutre, indépendant et impartial* »[1513]. Cette précision sur l’exclusion d’une opération intellectuelle est complétée par la jurisprudence, il apparaît que cette notion proscrit la volonté juridique, établissant l’huissier de justice en un acteur neutre et impartial. Par exemple, il n'est pas possible pour lui d'acheter un produit pour en constater la vente[1514].

760. **Faits enregistrés dans la *blockchain* fixés et relatés.** Ainsi, le constat *blockchain* ne pourra consister qu’en celui des différents enregistrements de données dans le registre et écarterait toute autre opération intellectuelle qui rendrait l’huissier de justice non neutre et impartial. Ces faits enregistrés dans la *blockchain* seront fixés et relatés dans le constat, objectivement, sans pour autant réaliser des observations sur d’éventuelles conséquences de fait

[1511] En ce sens : R. Perrot, « Constatations purement matérielles », Procédures n°5, mai 2014, p.12.
[1512] R. Perrot, « Le constat d'huissier de justice », *op.cit.*, p.33.
[1513] S. Dorol, Fasc. 30 : Constat d’huissier de justice, JCl. encyclopédie des Huissiers de Justice, Lexis Nexis, avr. 2015 (maj 27 dec. 2018), n°4.
[1514] Cass. 1ère civ., 20 mars 2014, n°12-18.518.

ou de droit. Il aurait pour objet de contextualiser les données enregistrées dans la *blockchain*[1515]. L'extraction ou encore l'achat d'actifs numériques seraient impossibles pour l'huissier. L'usage des procès-verbaux de constat dans la pratique du numérique est courant et répond aux nécessités de fixer, à date certaine, un état de fait susceptible d'être modifié ou de disparaître[1516]. Le constat *blockchain* ne poursuivra pas le même objectif puisqu'un registre distribué n'est pas sujet à modification ou disparition sauf les cas mentionnés ci-avant lors d'une attaque ou de blockchains spécifiques. L'objectif de ce constat *blockchain* pourra se situer dans la constitution d'une seconde preuve par un auxiliaire constatant matériellement un fait juridique enregistré dans le registre distribué.

761. **Outil de précaution.** Si le constat matériel ne se présente pas comme indispensable puisqu'il n'apporte pas d'analyse technique des preuves *blockchains* ou de valeur démonstrative quelconque, il se révèle être un outil de précaution nécessaire à l'amorce de la démocratisation de ces nouvelles preuves issues de la *blockchain*. La démonstration de ces procédés techniques étant complexe, elles auraient moins de chance d'emporter seules la conviction du juge. La conseillère référendaire à la Cour de cassation Sophie Canas se montrait d'ailleurs favorable à la réception de constat des conditions matérielles par huissier de justice[1517].

C. La mise en œuvre du constat des enregistrements de données dans la *blockchain*

762. **Modalités du constat.** Le procès-verbal d'un enregistrement de données dans une *blockchain* qui pourrait autrement être appelé « *constat blockchain* » est un acte par lequel un huissier de justice ou un clerc habilité (si la requête est initiée par un particulier), accèdent au registre d'une *blockchain* en suivant un protocole spécifique, dans l'objectif d'y constater des éléments, voire de procéder à des captures écran. Le constat sera en théorie conservé par l'huissier de justice sous réserve d'une interdiction législative[1518].

[1515] S. Dorol, « Blockchain et métiers du droit : la fin des tiers de confiance ? », Dossier « Blockchain et métiers du droit : une force vive ou subversive ? », *op.cit.*, p.94.
[1516] O. Blanchet, X. Bariani, Fasc. 10 : huissiers de justice, JCl. Encyclopédie des Huissiers de Justice, Lexis Nexis, avr. 2011 (maj 5 juill. 2019), n°182.
[1517] S. Canas, « Blockchain et preuve : le point de vue du magistrat », *op.cit.*, p.82.
[1518] Voir : CPC exéc., art. L152-3.

763. Ce constat *blockchain* peut être rapproché du constat Internet consistant à dresser un procès-verbal d'une page Internet parmi des réseaux internationaux. Le support technologique sera néanmoins différent. Il convient de rester conscient que deux constats ne sont jamais identiques, aucune assimilation exacte n'est possible car chaque protocole précis à suivre est distinct. Le Professeur Roger Perrot, rapportait à cet égard que « *les conditions d'élaboration d'un constat varient sensiblement selon les cas d'espèce. À la limite, on pourrait presque dire qu'il n'y a pas deux constats qui se ressemblent. Une réglementation légale, précise, minutieuse et uniforme, aurait donné au constat une rigidité difficilement compatible avec son avantage majeur qui est d'être une mesure souple (…)* »[1519].

764. Dans le cadre du constat internet, la jurisprudence a pour autant établi des critères génériques de recevabilité de ces constatations. La Cour d'appel de Paris a édicté des règles instituant une méthodologie[1520]. Le constat doit décrire le matériel ayant servi aux constatations, indiquer l'adresse IP de l'ordinateur ayant servi aux constations, les caches de l'ordinateur doivent être vidés préalablement aux constatations, la connexion doit être désactivée par proxy et l'ensemble des fichiers de navigations temporaires, cookies, et historiques de navigation doivent être supprimés. La force probante d'impression écran est souvent écartée au motif que le processus d'obtention n'est pas décrit précisément, la réalisation du constat ne fait pas intervenir un huissier de justice ou tiers assermenté, le matériel, l'adresse IP, le mode de navigation et le réseau de connexion utilisés n'ont pas été précisés[1521]. Dans le contexte de la *blockchain* la maîtrise des outils par l'huissier sera aussi essentielle, passant effectivement par la maîtrise de son ordinateur avec un espace de stockage suffisamment important pour télécharger les registres distribués volumineux en poids, une adresse IP, ou encore l'absence de serveur proxy.

765. Une norme AFNOR NFZ67-147 du 11 septembre 2011 définit *en sus* une méthodologie consultative pour le constat internet[1522]. Elle constitue un recueil des bonnes pratiques[1523], ne

[1519] R. Perrot, « Le constat d'huissier de justice », *op.cit.*, p.18.
[1520] CA Paris, pôle 5, ch. 1, 27 févr. 2013, n°11/11785.
[1521] CA Paris, pôle 5, ch. 2, 2 juill. 2010, n°09/12757, Sté Moissanite France et Sté Laval c/ Home Shopping Service (HSS) : Com. com. élec. n°11 nov. 2010, com. E. A. Caprioli. Confirmé : CA Paris, 7 janv. 2014, n°13/06238.
[1522] C. Duparc, « L'adaptation de l'huissier de justice à l'économie digitale », AJCA, avr. 2016, p.187.
[1523] CA Lyon, 28 nov. 2013, n°12/01964 ; CA Paris, 27 févr. 2013, n°11/11785.

disposant pas d'une valeur contraignante[1524]. Il n'est pas exclu qu'une norme AFNOR soit aussi prévue prochainement pour le constat *blockchain*, compte tenu du développement de cette norme dans le cadre des protocoles.

766. **Date et heure.** En principe, selon l'article 664 du Code de procédure civile « *aucune signification ne peut être faite avant six heures et après vingt et une heures, non plus que les dimanches, les jours fériés ou chômés, si ce n'est en vertu de la permission du juge en cas de nécessité* ». Toutefois, cette disposition ne s'applique pas à tous les cas de constatation. Si le constat est effectué dans un lieu public, l'impératif d'horaire ne s'impose pas à l'huissier de justice[1525]. Or, un constat réalisé dans un lieu privé non ouvert au public et sans avoir été requis par son occupant légitime se voit appliquer l'article susmentionné. Ainsi, de prime abord, seuls dans les cas où des constats seront réalisés dans des registres distribués fermés au public, dans les *blockchains* privées, les dates et heures imposées devront être respectées par l'huissier, alors que dans les *blockchains* publiques, ouvertes au public, cette contrainte ne sera pas applicable. Cependant, l'huissier de justice Thierry Guinot a pu considérer qu'il apparaissait logique que les constatations effectuées sur Internet ne soient pas concernées par ces limitations horaires[1526], ce qui suscite aussi des interrogations quant au lieu spécifique des saisies dans les registres dématérialisés des *blockchains*.

767. **Lieu du constat.** L'huissier est compétent pour réaliser des constatations dans le territoire national[1527]. Des problématiques se posent néanmoins lorsque le lieu de la saisie est dématérialisé et ne comporte pas de frontières territoriales. Par le passé, l'huissier de justice compétent pour effectuer les constatations était celui où se situait la juridiction devant laquelle était porté le litige[1528]. Il est désormais admis - indépendamment de la juridiction - que tout huissier de justice puisse réaliser des constats sur Internet. Tout huissier de justice est donc en mesure, dans le cadre d'une *blockchain*, réseau distribué international, de réaliser un constat.

[1524] Doute sur le caractère obligatoire : CA Aix-en-Provence, 15 sept. 2016, n°13/22133, inédit : Gaz. pal. oct. 2016 com. S. Dorol ; Procédures 2017, note N. Bouche et O. Hubert. Confirmation du caractère non obligatoire : CA Toulouse, 15 mai 2017, n°15/02964 ; CA Aix-en-Provence, 15 févr. 2018, n°15/02822, inédit.

[1525] R. Perrot, « Le constat d'huissier de justice », *op.cit.*, 1985, p. 61. En ce sens : « *aucun texte ne prévoit la nullité d'un constat dressé par un huissier de justice en dehors des heures légales sur la voie publique (…)* » (Cass. civ., 22 avr. 1977 : DS 1977, inf. rap. p.294). Jurisprudence récente : CA Aix-en-Provence, 21 nov. 2013, n°2013/566.

[1526] T. Guinot, *L'huissier de justice : normes et valeurs*, EJT, coll. Droit et Procédures, mars 2017.

[1527] Ordonnance n°45-2592 du 2 novembre 1945 relative au statut des huissiers, art. 3.

[1528] S. Dorol, Fasc. 30 Constat d'huissier de justice, JCl. encyclopédie des Huissiers de Justice, Lexis Nexis, avr. 2015 (maj 27 dec. 2018), n°82.

768. Pour un site public, aucune autorisation du titulaire du site Internet n'est requise puisque comme l'analysait le Professeur Pierre-Yves Gautier « *si l'agent assermenté obtient légalement l'adresse du serveur, non confidentielle, et que comme tout usager, de « clic en clic », il parvient aux œuvres mises en ligne, sans barrière, ni « mot de passe » (équivalent du verrou ou de la clé de la porte d'entrée du site), il semble que ce ne puisse être que du consentement de son propriétaire qui a ouvert sa porte sur le « Web » à un public indéterminé, la planète entière* »[1529]. En conséquence de quoi, dans l'hypothèse où le registre est public de sorte qu'un droit d'accès n'est pas requis pour lire les transactions, aucune autorisation ne sera nécessaire à l'huissier car le registre est accessible à tous par l'opération du téléchargement.

769. À l'inverse, sur un site privé fermé au public, et dont l'accès est restreint par une identification et un mot de passe ou une inscription préalable, une autorisation expresse du propriétaire est exigée[1530]. Dans le contexte d'une *blockchain* où le registre privé et un droit d'accès spécifique est requis, l'autorisation expresse des membres ou de la personne morale sera une condition préalable pour l'huissier à la réalisation de son constat.

Paragraphe 2 : La portée probatoire moindre du constat des enregistrements de données dans la *blockchain*

La charge probatoire et la force probante du constat d'huissier sont des représentations topiques des difficultés que pose de façon générale l'acte d'huissier de justice. La portée probatoire de la constatation de données enregistrées dans la *blockchain* doit faire l'objet d'une analyse circonspecte puisque, par sa nature complexe, la force probante des constats peut prêter à discussion. La constatation instaure une présomption des faits enregistrés dans la *blockchain* au bénéfice du plaideur (A) et l'acte de constat des enregistrements de données dans la *blockchain* dispose d'une dualité probatoire (B).

[1529] P.-Y. Gautier, « Les œuvres du crooner dans la « maison » de l'internaute : promenade collective, mais non autorisée, sur un site numérique », D. 1996, p.490.
[1530] S. Dorol, Fasc. 30 : Constat d'huissier de justice, JCl. encyclopédie des Huissiers de Justice, *op.cit.*, n°105.

A. Une présomption simple des faits constatés d'enregistrements de données dans la *blockchain*

770. **Nature de la présomption.** Depuis la loi Béteille du 22 décembre 2010, l'article 1 modifié de l'ordonnance n°45-2592 du 2 novembre 1945 relative au statut des huissiers permet aux faits constatés par un huissier de justice ou son clerc de faire « (…) *foi jusqu'à preuve contraire* ». Cette loi a créé une présomption simple ayant pour effet de renverser la charge de la preuve au bénéfice du demandeur.

771. **Mise en œuvre de la présomption.** Ces constatations de données enregistrées dans la *blockchain* feront donc foi jusqu'à preuve du contraire. Il existe ainsi une présomption des faits constatés des enregistrements de données dans la *blockchain* qui supporte la preuve contraire. La présomption de ces enregistrements sera réfragable par le contradicteur apportant la preuve contraire. Cette preuve contraire sera particulièrement difficile à apporter, surtout si elle n'est pas de nature cryptographique. La double garantie de la preuve *blockchain* et de son constat sera instaurée au bénéficiaire de la présomption. Le titulaire de la charge de la preuve aura alors une preuve particulièrement difficile à apporter.

B. Une dualité probatoire de l'acte de constat des enregistrements de données dans la *blockchain*

772. La force probante de l'acte de constat d'huissier de justice a fait l'objet de réflexions doctrinales même si l'opinion sur sa force est désormais relativement unanime[1531]. La dualité probatoire de l'acte de constat se manifesterait par une valeur partiellement authentique[1532]. Si les constatations matérielles des enregistrements de données dans la *blockchain* n'ont pas de valeur authentique (1), les mentions relatives à l'huissier, la date et le lieu de l'acte auraient semble-t-il, quant à eux, cette valeur (2).

[1531] J. D. Lachkar, « La force probante de l'acte d'huissier de justice », *op.cit.*, p.42-45.
[1532] *Ibid.*, p.45, n°16.

1. L'absence de valeur authentique des constatations matérielles des enregistrements de données dans la *blockchain*

773. **Avant la loi dite « *Béteille* ».** Avant la loi du 22 décembre 2010 n°2010-1609 relative à l'exécution des décisions de justice, aux conditions d'exercice de certaines professions réglementées et aux experts judiciaires dite « *Béteille* », les constatations n'avaient la valeur que de simples renseignements selon le deuxième alinéa de l'article 1 de l'ordonnance du 2 novembre 1945. Le constat n'avait pas la même force probante que les autres actes d'huissier de justice et ne valait pas jusqu'à inscription de faux[1533].

774. **Souveraineté du juge.** Les juges étaient en conséquence en mesure d'apprécier souverainement ces simples renseignements. Ils pouvaient les écarter ou les soumettre à un débat contradictoire entre les parties, à leur discrétion[1534]. Ils n'étaient pas liés en somme par ces constatations qui leur étaient présentées.

775. **Évolution jurisprudentielle.** Progressivement, la jurisprudence a eu tendance à accorder aux constatations dressées par huissier de justice une force probante plus importante que celle accordée par l'ordonnance du 2 novembre 1945[1535]. C'est la nature particulière de l'auteur, l'huissier de justice, qui permettait de rendre « *digne de foi* » les éléments matériels du constat[1536]. Allant plus loin encore dans des contentieux spécifiques comme celui de l'Internet, le caractère objectif du constat d'huissier de justice le rendait difficilement réfutable par l'adversaire[1537].

776. **Depuis la loi dite « *Béteille* ».** La valeur des simples renseignements a donc été abandonnée depuis la loi Béteille du 22 décembre 2010, ce qui permettra aux enregistrements dans la *blockchain* constatés par huissier de faire foi jusqu'à inscription de faux par le jeu de la présomption simple des faits constatés. Notons cependant que dans le cadre de constatations de délits en matière pénale[1538], la valeur de simple renseignement est maintenue.

[1533] J. Legrain, « Le constat d'huissier sur Internet », JCP G n°39, sept. 2010, p.1814.
[1534] J. D. Lachkar, « La force probante de l'acte d'huissier de justice », *op.cit.*, p.45, n°16.
[1535] *Ibid.*, p.45, n°17.
[1536] *Ibid*.
[1537] *Ibid*.
[1538] C. pr. pén., art. 430.

777. **Absence de valeur authentique des constations matérielles et carence.** Toutefois, les constatations matérielles établies dans un constat d'huissier de justice ne disposent pas d'une valeur authentique, contrairement aux mentions relatives à l'huissier et à l'opération elle-même. L'article 2 de la loi Béteille nous le rappelle en indiquant que les constatations purement matérielles « (…) *font foi jusqu'à preuve contraire* ». Or, c'est justement le contenu de l'enregistrement et la qualité de la personne qui enregistre qui ne sont pas couverts dans le cadre des enregistrements de données dans la *blockchain*. Ils auraient mérité d'être confortés par acte d'huissier de justice. De toute évidence, cette carence dans la force probante de l'acte d'huissier de justice ne sera pas de nature à présenter une valeur ajoutée dans l'aide au déchiffrage des preuves *blockchains* par le juge.

2. La valeur authentique des mentions relatives à l'huissier, la date et le lieu de l'acte de constat des enregistrements de données dans la *blockchain*

778. **Nature et raisons des mentions ayant valeur authentique.** Seules certaines mentions relatives à l'huissier et à l'opération, comme son nom, la date, le lieu du constat, ont une valeur authentique. Les mentions de l'huissier ont une valeur authentique indiscutable, une force probante renforcée, alors que les constations matérielles sont dénuées de cette force. Le seul cas de contestation de ces mentions admis est le recours à la procédure de l'inscription de faux. L'une des raisons justifiant que ces mentions soient dotées d'une valeur authentique tient en la nature particulière de l'auteur de l'acte : l'huissier de justice est un officier public et ministériel[1539]. La valeur de ces mentions contenues dans les constatations sont en raison du statut de l'huissier dotées d'une force authentique, alors que les éléments factuels seront nécessairement soumis à l'épreuve du contradictoire.

779. En principe, la date dans un enregistrement de la *blockchain* est un des éléments particulièrement certain[1540]. Il se peut néanmoins que la date d'un ancrage de données ne soit pas ajustée à celle de validation des blocs, laquelle ferait office de date officielle selon notre approche[1541]. Le constat peut donc avoir un intérêt s'il est instrumentalisé au même moment que l'ancrage. Cet intérêt sera avéré dans l'hypothèse selon laquelle un fait juridique devra être

[1539] J. D. Lachkar, « La force probante de l'acte d'huissier de justice », *op.cit.*, p.42, n°4.
[1540] Voir *supra* n°135.
[1541] Voir *supra* n°531.

daté avec une certitude indiscutable, à l'instar d'une antériorité d'une œuvre de l'esprit. La date du constat ayant valeur authentique ne pourrait pas toutefois garantir avec objectivité la date de l'ancrage mais celle du constat de données enregistrées dans la *blockchain*.

780. Si le lieu constitue un point d'enracinement difficile à évaluer dans le cadre d'une *blockchain* publique, le lieu du constat établit incontestablement par sa valeur authentique des pistes et indices quant aux problématiques de détermination du droit applicable[1542].

781. Compte tenu de cette démonstration, le constat de données enregistrées dans la *blockchain* n'aura en définitive qu'une valeur partiellement authentique ce qui pourrait à certains égards soutenir la preuve *blockchain*.

782. En définitive, le constat ne sera pas indispensable en raison de son champ limité et de sa portée probatoire moindre, mais un outil de précaution à l'amorce de la démocratisation de ces nouvelles preuves. La démonstration des procédés techniques issus de ces preuves étant complexe, elle aurait moins de chance dans un premier temps d'emporter la conviction du juge sans ce constat. Pour l'heure, afin d'éviter l'effet négatif de ces preuves lié à leur complexité, le plaideur aurait ainsi intérêt à les faire constater.

Section 2 : Le rôle significatif des experts informatiques à mobiliser au soutien de la traduction des preuves de données enregistrées dans la *blockchain*

783. Les experts informatiques jouent un rôle cardinal dans les contentieux complexes, nécessitant une connaissance technique dans le domaine du numérique, pour permettre leur résolution[1543]. Ils endossent un rôle d'interface entre la logique scientifique et la logique judiciaire[1544]. Les experts ont toujours été d'un soutien certain en pratique, un lieutenant en la Sénéchaussée de Montpellier écrivait déjà en 1667 que « *les experts sont les juges de la question du fait, lorsqu'il s'agit de la vérification d'une chose qui ne peut être connue que par la pratique journalière de l'art qu'ils exercent* »[1545]. Les experts continuent de s'ériger progressivement en

[1542] Voir *supra* n°162 et s.
[1543] F. Ferrand, Preuve, *op.cit.*, n°440.
[1544] M. Mekki, « Vérité et preuve. Rapport français », *op.cit.*, p.821.
[1545] Bornier, Conférences des ordonnances de Louis XIV Roy de France et de Navarre, nouvelle édition, corrigée et augmentée, t. I, 1755, p.171.

« *partenaire de justice souvent incontournable* »[1546], partenaire qui se rendra nécessairement utile dans la traduction des preuves de données enregistrées dans la *blockchain*. C'est pourquoi nous étudierons, premièrement, le régime juridique de l'expertise de la preuve des données enregistrées dans la *blockchain* (paragraphe 1) et, deuxièmement, la portée probatoire subordonnée au juge de l'expertise des enregistrements de données dans la *blockchain* (paragraphe 2).

Paragraphe 1 : Le régime juridique de l'expertise des enregistrements de données enregistrées dans la *blockchain*

784. L'expertise est une mesure d'instruction consistant pour un technicien commis par le juge, c'est-à-dire un expert, à examiner une question de fait qui requiert ses lumières et sur laquelle des constatations ou une simple consultation ne pourraient suffire à éclairer le juge[1547]. Dans ce cas, c'est une expertise judiciaire qui est visée. Si l'action de l'expert s'inscrit souvent dans le cadre d'une action judiciaire, l'expertise peut néanmoins être non judiciaire (amiable ou privée). Elle est effectuée dans cette hypothèse à la seule initiative des parties, contradictoirement ou non[1548]. Cette expertise pourra être diligentée avant, pendant le cours du procès, ou en dehors de tout litige[1549]. Elle aura essentiellement pour but en pratique d'accompagner les plaideurs au rassemblement de leurs preuves numériques ou d'analyser les données dans la *blockchain* afin par exemple de révéler les données effacées dans une *blockchain* privée. Les développements à venir porteront davantage sur l'expertise judiciaire comportant le plus d'enjeux pour les preuves *blockchains*, puisque les cas où les juges commettront des experts seront les plus courants. Nous procéderons tout d'abord à la présentation du choix par le juge de la mesure d'expertise appropriée aux enregistrements de données dans la *blockchain* (A) puis de l'objet de cette mesure d'expertise (B).

[1546] Cour de cassation, Colloque « La vérité... sans doute. Vérité scientifique, vérité judiciaire » (commémorant le trentenaire de la Compagnie des experts agréés par la Cour de cassation), Discours de Monsieur B. Louvel, premier président de la Cour de cassation, le 2 oct. 2015.
[1547] G. Cornu, *Vocabulaire juridique*, *op.cit.*, Voir expertise sens n°1, p.439. Voir aussi : C. pr. civ., art. 263.
[1548] V. Vigneau, *Droit de l'expertise*, Dalloz action, 2016/2017, n°212.11.
[1549] *Ibid*.

A. Le choix par le juge de la mesure d'expertise appropriée aux enregistrements de données dans la *blockchain*

785. Le juge a le choix de la mesure d'expertise pour les enregistrements de données dans la *blockchain* en deux points : par le choix de l'opportunité de la mesure d'expertise (1) et celui de l'expert spécialisé en sciences informatiques (2).

1. Le choix de l'opportunité de la mesure d'expertise

786. **Objectifs de la mesure d'expertise.** L'expertise est ordonnée par l'ordre judiciaire en cours de procès mais a un caractère facultatif pour le juge, qui n'est pas dans l'obligation d'avoir recours à un expert[1550]. Le magistrat fait appel à un expert lorsqu'il a besoin de s'appuyer sur des connaissances techniques ou scientifiques nécessaires à la solution du litige qu'il doit trancher[1551]. Rappelons que l'expert est celui qui exerce à titre principal une profession à caractère technique. Il n'est pas un réel auxiliaire de justice mais davantage un « *collaborateur occasionnel du service public de la justice* »[1552], conduit à exécuter des missions confiées par des magistrats[1553]. Il est fort probable que le juge exige le recours à un expert - considéré comme le véritable « *œil du juge* »[1554] ou encore l'« *éclaireur de la conscience du juge* »[1555] - pour pénétrer techniquement les preuves *blockchains* usitées par un plaideur et les expliquer[1556].

787. **Mesure d'expertise et preuves *blockchains*.** Il nous apparaît opportun, voire incontournable, de faire intervenir un expert dans le cadre de dossiers particulièrement complexes de technologie *blockchain* pour traduire des enregistrements de données du registre, comme pour rendre intelligibles des données codées à l'instar d'*un smart contrat* ou rendre lisibles des données chiffrées et des données hachées. L'exemple le plus significatif nous est fourni par celui d'une empreinte *blockchain* du langage haché qui doit être traduite en langage

[1550] Com. 8 déc. 1981, n°81-14.157 : Bull. civ. IV, n°428.
[1551] J. Boulez, *Expertises judiciaires*, Encyclopédie Delmas, 17e ed., 2016, p.10.
[1552] CE 26 févr. 1971, req. n°77459, Aragon, Lebon 172 : AJDA 1971. II. 177. Voir aussi : V. Perruchot- Triboulet, « Le nouveau statut des experts judiciaires », D. 2005, p.3046.
[1553] J. Boulez, *Expertises judiciaires*, *op.cit.*, p.10.
[1554] P. de Bornier, Conférences des nouvelles ordonnances de Louis XIV avec celles des rois prédécesseurs de Sa Majesté, le droit écrit et les arrêts, 1693.
[1555] René Garaud cité dans Cour de cassation, Colloque « La vérité... sans doute. Vérité scientifique, vérité judiciaire » (commémorant le trentenaire de la Compagnie des experts agréés par la Cour de cassation), Discours de Monsieur B. Louvel, premier président de la Cour de cassation, le 2 oct. 2015.
[1556] S. Canas, « Blockchain et preuve : le point de vue du magistrat », *op.cit.*, p. 82.

lisible par l'homme. C'est généralement la vérification des données originelles par un recalcul de l'empreinte qui permet de vérifier qu'elles n'ont pas été modifiées. Si cette manipulation technique est à la portée de tout initié usant des propriétés de la fonction de hachage classique employée par la *blockchain*[1557], le juge n'est pas censé être éclairé par défaut sur ces pratiques. Faire appel à un expert pour procéder au recalcul de l'empreinte est alors en principe requis de manière propice.

788. **Caractère subsidiaire de la mesure d'expertise.** Le juge doit en principe recourir à un technicien seulement dans la mesure du nécessaire. Par-delà les conceptions des différents rédacteurs des réformes de la procédure civile - qui se sont succédées depuis 1973 -, l'idée que l'expertise doit rester subsidiaire demeure[1558]. La mesure d'expertise ne peut pas être ordonnée à tout prix. Ne peuvent être ordonnées des mesures d'instruction pour suppléer la carence des parties dans l'administration de la preuve[1559] ou encore concilier et dire le droit[1560]. La décision qui ordonne ce type de mesure pourrait être frappée d'un recours immédiat, contrairement aux autres mesures d'instruction[1561]. L'une des raisons de ces limitations réside dans le constat que l'expertise judiciaire est une cause majeure de lenteur et de coût reprochés à la justice civile[1562], coût d'ailleurs supporté par une partie au procès[1563], sauf en matière pénale où l'État les prend en principe en charge[1564]. L'expertise intervenant pour une étude technique liée au décryptage des preuves *blockchains* sera ainsi de nature à aggraver les coûts et ralentir le traitement d'un litige, tel que le mentionne très justement le rapport Toledano[1565].

[1557] Voir un avis favorable à l'intervention d'un tiers certificateur : F. G'sell, « Preuve et signature numérique », *op.cit.*, p.107.
[1558] M. Francès-Magre, « Caractère subsidiaire de l'expertise par rapport aux mesures d'instruction exécutées par un technicien », JCP, 1975 ; T. Moussa, F. Arbellot, F. Delbano, D. Loriferne, J.-P. Martin, P. Matet, V. Vigneau, *Droit de l'expertise 2016/2017*, *op.cit.*, p.79, n°211-17.
[1559] C. pr. civ., art. 146, al. 1.
[1560] C. pr. civ., art. 240.
[1561] C. pr. civ., art. 272.
[1562] Circ. garde des Sceaux n°83.06, 2 août 2003 ; Rapport de la commission de réflexion sur l'expertise remis au garde des Sceaux, le 31 mars 2011 ; L. Cadiet, et Y. Jeuland, *Droit judiciaire privé*, Lexis Nexis, 17e ed., 2013, n°572 ; K. Favro, M. Lobé Lobas, J.- P. Markus (ss. dir.), *L'expert dans tous ses états*. À la recherche d'une déontologie de l'expert, *op.cit.*, p.113.
[1563] F. Loyac, « Les frais d'expertise », Rev. jur. Ouest 1991, p.167-190.
[1564] C. pr. pén., art. 800-1.
[1565] F. G'sell, « Preuve et signature numérique », *op.cit.*, p.108

2. Le choix de l'expert spécialisé en sciences informatiques appliquées à la *blockchain*

789. **La spécialité de l'expert et autres qualités.** Le juge ne peut désigner en théorie qu'un seul expert, à moins qu'il estime nécessaire d'en nommer plusieurs[1566]. Le choix de l'expert est à la libre appréciation du magistrat[1567], n'oublions pas qu'expert du latin *expertus* signifie aguerri. Le juge aura donc intérêt à choisir un expert aguerri et spécialisé avec un champ de connaissances en sciences informatiques (mathématiques-informatique) et un exercice en tant qu'ingénieur ou développeur dans le secteur du numérique. Pour l'expertise non-judiciaire, la désignation de l'expert sera libre ou contractuelle[1568]. Malgré tout, la partie qui diligente l'expertise a tout intérêt à choisir un homme de l'art hautement qualifié qui est régulièrement choisi comme expert par la juridiction devant laquelle l'action sera introduite et dont le rapport aurait moins de risque d'être discuté[1569]. *In fine*, les seules connaissances acquises accessibles à tous ne font pas forcément un bon sachant, c'est un savoir brut et une expérience solide qui constitueront sa compétence. Par-delà ces connaissances et cette expérience de l'expert, un triptyque incontournable fonde sa légitimité : compétence, objectivité et pédagogie[1570].

790. **Listes d'experts.** Dans le ressort de chaque Cour d'appel, les experts judiciaires sont inscrits sur des listes et une liste nationale est aussi dressée auprès de la Cour de cassation[1571]. Elles ne procèdent pas de simples initiatives juridictionnelles mais elles sont le résultat d'une obligation imposée par l'article 2 de la loi n°71-498 du 29 juin 1971 relative aux experts judiciaires. Cette loi - qui a fait l'objet de nombreuses modifications[1572] -, est complétée par un décret n°2004-1463 du 23 décembre 2004 relatif aux experts judiciaires[1573]. À titre d'exemple,

---

[1566] C. pr. civ., art. 264.
[1567] C. pr. civ., art. 232.
[1568] V. Vigneau, *Droit de l'expertise*, *op.cit.*, n°212.11.
[1569] J. Boulez, *Expertises judiciaires*, *op.cit.*, p.37, n°15.17.
[1570] V. Vigneau, Synthèse générale du colloque « Le futur de l'expertise judiciaire civile dans l'Union européenne », Bruxelles, 16-17 mars 2012, https://experts-institute.eu/wp-content/uploads/2018/03/actes-du-colloque-fr.pdf (consulté le 31/05/2020), p.59.
[1571] P. Schultz, « L'élaboration des listes d'experts de justice », *in* K. Favro, M. Lobé Lobas, J.- P. Markus (ss. dir.), *L'expert dans tous ses états.* À *la recherche d'une déontologie de l'expert*, *op.cit.*, p.36.
[1572] Loi n°2004-130 du 11 février 2004 réformant le statut de certaines professions judiciaires ou juridiques, des experts judiciaires, des conseils en propriété industrielle et des experts en ventes aux enchères publiques (publiée au JO, le 12 févr. 2004, p.2847) ; Loi n°2010-1609 du 22 décembre 2010 relative à l'exécution des décisions de justice, aux conditions d'exercice de certaines professions réglementées et aux experts judiciaires (publiée au JO le 23 décembre 2010, p.22552) ; Loi n°2012- 409 du 27 mars 2012 de programmation relative à l'exécution des peines (publiée au JO 28 mars 2012, p. 5592).
[1573] Décret n°2004-1463, du 23 décembre 2004 relatif aux experts judiciaires (publié au JO 30 déc. 2004, p.22351) ; modifié par Décret n°2006-1319 du 30 octobre 2006, modifiant le décret n°2004-1463 du 23 décembre 2004

dans la liste d'experts près la Cour d'appel de Paris, les nomenclatures du secteur e-industries des activités électroniques et informatiques (E.01) : Internet et multimédia (E.01.02), logiciels et matériels (E.01.03) et systèmes d'information (E-01.04) répertorient certains experts travaillant déjà précisément sur les sujets de technologie *blockchain*[1574]. La nomenclature télécommunications et grands réseaux (E.1.5) des activités électroniques et informatiques (E.1) du secteur e-industries de la liste d'experts de la Cour de cassation compte également des experts spécialisés[1575]. Ces professionnels sont reconnus mais une mission d'expertise pourrait aussi être attribuée à des experts non-inscrits[1576]. Sur le plan de son expertise technique, le choix de l'expert approprié est cardinal puisqu'avec le juge ils formeront un couple indissociable[1577], un véritable binôme tout au long de la mission de l'expert leur permettant d'avoir recours l'un à l'autre[1578].

791. **Sapiteur technique.** Lorsque la mission confiée à l'expert dépasse sa spécialité technique, celui-ci peut décider de solliciter l'avis d'un autre technicien : un sapiteur technique[1579]. Ce dernier peut être, comme l'expert lui-même, choisi sur une liste officielle ou hors liste[1580]. Un lien par une convention de droit privé de prestation de services est établi avec l'expert. Il n'est pas exigé de lui de connaissance procédurale particulière[1581]. D'ailleurs, il sera présent dans les actes procéduraux de l'expertise sous l'autorité de l'expert et non à titre personnel[1582]. Il convient donc de ne pas exclure l'hypothèse selon laquelle le contentieux portant sur les preuves *blockchains* dépasse les compétences de l'expert désigné, lequel pourrait dans ce cas solliciter l'avis d'un sapiteur.

---

relatif aux experts judiciaires (publié au JO 31 oct. 2006, p.16107) ; Décret n°2007-1119, du 19 juillet 2007, modifiant le décret no 2004-1463 du 23 décembre 2004 relatif aux experts judiciaires (publié au JO 21 juill. 2007, p.12352) ; Décret n°2011-1173 du 23 septembre 2011, portant diverses dispositions relatives à certaines professions judiciaires et juridiques réglementées (publié au JO 25 sept. 2011, p.16074) ; Décret n°2012-1451 du 24 décembre 2012 (publié au JO 27 déc. 2012, p.20504).

[1574] https://www.cours-appel.justice.fr/sites/default/files/2020-03/Annuaire%20Experts%202020.pdf (consulté le 31/05/2020).

[1575] https://www.courdecassation.fr/IMG///2019_liste_national_experts_maj0102.pdf (consulté le 31/05/2020).

[1576] J. Boulez, *Expertises judiciaires*, *op.cit.*, p.10.

[1577] M. Caratini, « Experts et expertise dans la législation civile française. Principes généraux », Gaz. pal., 22 janv. 1985, p.44.

[1578] M. Olivier, « Aspects juridiques et déontologiques du rapport d'expertise vétérinaire », *in* De l'expertise civile et des experts, t.2, Berger-Levrault, 1995, p.40.

[1579] C. pr. civ., art. 278.

[1580] A. Gaillard, « Le sapiteur ou l'assistance technique », CNECJ, janv. 2007, p.3.

[1581] *Ibid*.

[1582] F. Pinchon, « Point de procédure expertale concernant les sapiteurs », Gaz. Pal. 11 févr. 2003, n°gp20030211001, p. 3 et s.

B. L'objet de la mesure d'expertise des enregistrements de données dans la *blockchain*

792. L'expert fournit un avis tranché de praticien. La mesure d'expertise n'a néanmoins qu'un caractère technique (1), l'expert ne portant pas d'appréciations juridiques. Lors de son appréciation technique, l'expert pourra être confronté régulièrement à la problématique de la migration, perte ou destruction de données faisant obstacle à son expertise (2).

1. Le caractère uniquement technique de l'expertise des enregistrements de données dans la *blockchain*

793. **Questions techniques, réponses techniques, éléments techniques examinés.** L'expertise a un caractère uniquement technique car les experts ne disent pas le droit. L'expert ne doit jamais porter d'appréciation d'ordre juridique[1583]. La mission de l'expert est délimitée par le juge qui pose les questions techniques auxquelles l'expert doit répondre[1584], conformément au serment qu'il a prêté d'accomplir sa mission, de faire son rapport et donner son avis en « *honneur et conscience* »[1585]. Les questions techniques pourraient vraisemblablement avoir trait à la fiabilité de la preuve *blockchain* utilisée, l'intégrité de la preuve ancrée par la *blockchain*, l'identification du plaideur qui prétend s'être constitué une preuve par la *blockchain*, l'imputabilité de faits délictueux enregistrés dans la *blockchain* ou tout simplement la traduction en langage lisible des preuves *blockchains*. L'objet de l'expertise de la *blockchain* aura donc pour but d'apporter les éléments techniques de la fiabilité de la preuve, de traduire, voire extraire des enregistrements de données chiffrées, hachées, ou simplement enregistrées en clair dans une *blockchain* mais non d'apporter des éléments de droit à ces preuves *blockchains*. Seront immanquablement examinés par l'expert, dans son analyse, la nature des protocoles, les standards techniques de certains protocoles comme l'ERC, ou encore les référentiels techniques existants comme l'ISO[1586].

794. **Exemple de la fiabilité d'un algorithme.** Prenons l'exemple précis de la fiabilité d'un algorithme. Un expert sera certainement amené à trancher des problématiques de fiabilité d'un

[1583] C. pr. civ., art. 238, al.3.
[1584] C. pr. civ., art. 238, al.1.
[1585] Serment prescrit par la : Loi n° 71-498 du 29 juin 1971 relative aux experts judiciaires, art. 6.
[1586] Voir *supra* n°547-554.

algorithme de signature *blockchain*. La fiabilité d'un algorithme est étudiée corrélativement à la durée de vie des clés. La question de la durée de vie des clés dans un procédé de chiffrement s'est déjà posée dans le contexte de l'ancien régime européen des signatures électroniques issu de la Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques. Les réflexions avaient abouti à la conclusion dans le cas d'un contentieux afférent à la période d'espérance de vie de la clé, que la signature apposée sur un document devait être présumée authentique de manière quasi-irréfragable par le juge, puisque la clé est sensée être quasi-inviolable[1587]. Si toutefois un contentieux intervenait sur un document contenant une signature électronique dont la clé serait devenue violable, le document perdrait sa valeur d'originale et serait ainsi considéré juridiquement comme une copie, selon une partie de la doctrine. Pour d'autres, le document garderait toujours son caractère original quel que soit l'état de l'art puisqu'un original doit nécessairement exister au préalable avant d'envisager une copie[1588]. Par ailleurs, cet algorithme devra être étudié par l'expert en fonction de ses évolutions projetées. Par exemple, le projet de substitution de l'algorithme de signature électronique dans le protocole Bitcoin par un algorithme semblerait-il plus fiable nommé « *Schnorr* », est à l'étude[1589].

2. Les problématiques techniques spécifiques en tant que frein à l'expertise d'enregistrements de données dans la *blockchain*

795. **Hypothèses d'expertises impossibles.** L'hypothèse d'une « *expertise impossible* »[1590] est malencontreuse en cours de procès mais n'est pas inexistante. Elle correspond à des cas dans lesquels des difficultés d'ordre technique sont rencontrées par l'expert[1591], et le placent dans l'impossibilité de conclure. Or, l'expert doit faire mention dans son rapport d'expertise des questions posées restées sans réponse ou des différentes alternatives de réponses possibles. Cette hypothèse d'expertise impossible ne permettant de répondre à la question posée par le

[1587] L. J. Khalil, Signature électronique : le cadre juridique d'une autorité de certification, Thèse ss. dir. X. Linant De Bellefonds, Univ. upec, 2002.
[1588] L. J. Khalil, « Signature électronique : certificats qualifiés « publics » ou certificat qualifiés « privés », Com. Com. élec. n°4, avr. 2003, p.8.
[1589] Séminaire de « Cryptofinance » organisé par R. Pérez-Marco et C. Grunspan, intervention de Y. Seurin « Les signatures de Schnorr et de leurs applications dans Bitcoin », le 14 mars 2018.
[1590] J.-F. Schmauch, « L'expertise "impossible" », *in* K. Favro, M. Lobé Lobas, J.- P. Markus (ss. dir.), *L'expert dans tous ses états. À la recherche d'une déontologie de l'expert*, *op.cit*., p.127.
[1591] H. Bitan, *Droit et expertise du numérique*, Wolters Kluwer, coll. Lamy Axe Droit, 2015, p.497.

juge se retrouve dans la *blockchain* avec la disparition (en cas de migration ou de perte)[1592] et la destruction volontaire de données stockées en dehors du registre de la *blockchain* ou encore l'obfuscation de données stockée dans ce registre[1593].

796. **Exemple de migration ou perte dans la vérification d'une empreinte *blockchain*.** Par exemple, il serait impossible de mener une expertise technique sur la vérification d'une empreinte *blockchain* dans l'hypothèse de migrations (notamment par l'archivage du fichier initial), mais surtout de pertes du fichier initial. La migration ou la perte pose en effet des difficultés particulières car elle ne permet plus à l'expert de vérifier l'intégrité de ces données. Si l'objet de l'expertise a pour but de vérifier l'intégrité d'un ensemble de données, la migration et la perte feront obstacle techniquement à cette mission confiée à l'expert. Il est donc de nature impérative pour le plaideur de disposer d'une sauvegarde sécurisée des données initiales au-delà de la préconstitution de preuve établie par son ancrage dans le registre de la *blockchain*[1594]. En l'absence du fichier original permettant de vérifier l'empreinte, il n'a plus de preuve à administrer.

797. **Exemple de destruction volontaire de données liées à une infraction.** La destruction volontaire de données extérieures au registre constituant des preuves relatives aux infractions sont d'autres pratiques brouillant la mise en œuvre et les résultats de l'expertise. Il pourrait s'agir de la destruction de données concernant l'achat de produits ou services illicites permis grâce aux actifs numériques. Avant de se résoudre à admettre l'impossibilité de la conclusion de son expertise, l'expert doit se montrer d'une grande rigueur et rechercher toute trace, notamment de connexion, qui aurait permis de se débarrasser des données.

[1592] La migration de données est le processus par lequel un ensemble de données sont transférées d'un système à un autre impliquant un changement de stockage et de base de données ou d'application. Alors que la perte des données est la situation par laquelle des données disparaissent momentanément ou de manière permanente. Dans les deux cas, les données initiales ne seront plus stockées à l'endroit où elles ont été enregistrées originairement.
[1593] L'obfuscation est une action consistant à publier des fausses informations ou imprécises de manière à dissimuler les informations pertinentes dans un but de protection de la vie privée. Voir : F. Brunton, H. Nissenbaum, *Obfuscation : A user's guide for privacy and protest*, MIT Press, sept. 2015, 136 p. ; Rapport OPECST (par V. Faure-muntian, C. De Ganay, R. Le Gleut), Les enjeux technologiques des *blockchains* (chaînes de blocs), *op.cit.*, p.92.
[1594] Voir *supra* n°395-396.

Paragraphe 2 : La portée probatoire de l'expertise des enregistrements de données dans la *blockchain* subordonnée au juge

798. La portée probatoire du rapport d'expertise de données enregistrées dans la *blockchain* sera limitée à une certaine force probante (A). Elle sera en outre subordonnée à la libre appréciation de ce rapport d'expertise par le juge (B).

A. La force probante du rapport d'expertise des enregistrements de données dans la *blockchain*

799. **Rapport d'expertise combattu par la preuve contraire.** Les conclusions du rapport d'un expert peuvent être combattues par la preuve contraire. Cette position sur la force probante du rapport d'expertise a fait suite à de nombreux débats divisant jurisprudences et doctrine[1595]. La jurisprudence a ensuite pris le soin de trancher la valeur du rapport d'expertise : le rapport du technicien ne constitue pas un acte authentique[1596].

800. **Valeur moindre de l'expertise non judiciaire.** Pour ce qui est des expertises non judiciaires, elles auraient une valeur moindre à l'expertise judiciaire. Ces expertises de « *second ordre* »[1597] peuvent toutefois valoir à titre de preuve si elles sont soumises à la libre discussion des parties et même si l'expertise n'a pas été réalisée contradictoirement[1598]. Tranchant sur des divergences entre les chambres civiles, la chambre mixte est venue statuer dans un arrêt de principe du 28 septembre 2012 sur la valeur probante des rapports d'expertises amiables ou « *privés* ». Elle a consacré l'idée que le juge ne peut refuser d'examiner ces expertises établies non contradictoirement dès lors qu'elles sont soumises à la libre discussion des parties. Elle précise néanmoins que le juge ne pourra « *se fonder exclusivement sur une expertise réalisée à*

[1595] M. Olivier, « L'expertise en matière civile », *in De l'expertise civile et des experts*, t.2, Berger-Levrault, 1995, p.20 ; M. Olivier, « Mesures d'instruction confiées à un technicien », Répertoire de procédure civile, Dalloz, 2004, n°566 ; M. Redon, « Mesures d'instruction confiées à un technicien », Répertoire de procédure civile, Dalloz, 2012 (mis à jour 2015), n°567.
[1596] Cass. civ. 1ère, 13 janv. 1998, n°96- 14.239 ; Cass. 1ère civ., 19 janv. 1999, n°97- 14.194 : Bull. civ. I, n°22 ; Gaz. pal. oct. 2000, n°16.
[1597] T. Moussa, F. Arbellot, F. Delbano, D. Loriferne, J.-P. Martin, P. Matet, V. Vigneau, *Droit de l'expertise 2016/2017*, ss. dir. de T. Moussa, *op.cit.*, p.83, n°212.13.
[1598] Cass. 1ère civ., 13 avr. 1999, n°96-19.733, Bull. civ. I, n°134, JCP 1999. IV. 2091 : RTD civ. 1999. 671, obs. Patarin ; Cass. com. 30 oct. 2000, n°98- 12.671, Bull. civ. IV, n°172 : D. 2000. AJ 438 ; Cass. 2ème civ., 7 nov. 2002, n°01- 11.672 : Bull. civ. II, n°246 ; JCP 2002. IV. 3060 ; Gaz. pal. 6- 7 août 2003, 20, obs. du Rusquec. Solution identique pour un constat amiable non contradictoire : Cass. 1ère civ., 12 avr. 2005, n°02- 15.507, Bull. civ. I, n°181.

la demande de l'une des parties »[1599]. En d'autres termes, l'expertise amiable ou privée devra être corroborée par d'autres éléments de preuve.

801. **Possible dépendance économique de l'expert non judiciaire.** Ajoutons que dans le cadre de l'expertise non judiciaire, l'expert ne rend compte qu'à ses mandants et ne sera pas soumis aux mêmes exigences d'impartialité que celles de l'expert judiciaire. Il n'est donc pas rare qu'une situation de dépendance économique de l'expert soit établie vis-à-vis du mandant[1600]. *A contrario*, dans l'expertise judiciaire, les opérations sont réalisées sous le contrôle du juge, garantie de son impartialité. Il aura aussi librement décidé ou non de retenir les conclusions de cet expert, et le constat est soumis obligatoirement au respect du principe du contradictoire.

802. Si dans ce contexte le rapport d'une expertise judiciaire dresse un certain état technique d'une preuve *blockchain*, celui-ci ne sera pas incontestable et pourra être combattu par une preuve contraire apportée par la partie adverse. Dans l'hypothèse où le juge n'aurait pas demandé de mesure d'expertise pour des preuves *blockchains*, l'opportunité de l'expertise amiable est toujours ouverte. Même si son admissibilité n'est pas contestée, elle aura toutefois une force probante *a priori* moins importante, et devra ainsi être idéalement complétée par d'autres éléments de preuves.

B. La libre appréciation par le juge du rapport d'expertise des enregistrements de données dans la *blockchain*

803. **La liberté d'appréciation des conclusions de l'expert.** Les juges sont libres d'apprécier souverainement les conclusions de l'expert et ne sont pas liés par celles-ci[1601]. L'appréciation souveraine concerne la valeur et la portée du contenu de l'expertise[1602] mais à condition de ne pas la dénaturer[1603]. Les juges peuvent ainsi rejeter les conclusions de l'expert,

[1599] Cass. ch. mixte, 28 sept. 2012, n°11-18.710 : D. 2012. 2317, 2013. 269, obs. N. Fricero, et 2802, obs. J.- D. Bretzner ; RTD civ. 2012. 769, obs. R. Perrot ; JCP 2012. 1200, note S. Amrani Mekki.
[1600] V. Vigneau, *Droit de l'expertise, op.cit.*, n°212.11.
[1601] C. pr. civ., art. 246. confirmé : Cass. 1ère civ., 19 févr. 2013, n°11-24.453 : D. 2013. 1041, note Garaud.
[1602] Cass. 1ère civ., 12 mai 2004, n°02-13.959.
[1603] Cass. 2ème civ., 15 mai 2008, n°06-22.171.

les entériner purement et simplement, n'adopter que certaines conclusions[1604] ou encore adopter ses conclusions sans suivre le détail des parties dans leur argumentation[1605].

804. **La limitation aux motifs de rejet des conclusions de l'expert.** Cependant, la libre appréciation est limitée par la Cour de cassation, qui impose, lorsque le juge du fond n'adopte pas les conclusions de l'expert, d'énoncer les motifs qui ont conduit à ce choix[1606]. Un arrêt a même retenu que les solutions d'un expert ne pouvaient être écartées par le Tribunal que sur le fondement de la constatation et d'avis techniques extérieurs régulièrement produits au débat et discutés contradictoirement entre les parties[1607]. Généralement la jurisprudence considère cependant que les juges du fond ne sont pas tenus de s'expliquer sur les éléments de preuve qu'ils décident d'écarter[1608].

805. **La contre-expertise.** Le juge pourra aussi décider de ne pas retenir les conclusions expertales et solliciter une contre-expertise[1609]. Les conclusions de l'expertise non-judiciaire ne lient pas non plus le juge, mais il peut y puiser des renseignements à condition qu'il ait veillé au respect du principe de la discussion contradictoire entre les parties[1610].

806. **L'appréciation des conclusions de l'expert en fonction du domaine du litige.** En fonction du domaine du litige, en matière civile ou pénale, les juges ont tendance à se sentir plus ou moins liés par le rapport d'expertise. En matière civile, le juge s'estime souvent implicitement lié par le contenu du rapport d'expertise, central pour résolution du litige et commander l'action, notamment dans les conflits familiaux[1611]. À l'inverse, en matière pénale, les juges décideraient en fonction de différents facteurs, comme le désir de prononcer de bonnes décisions au fond, le respect de leurs pairs et de la société, les facteurs idéologiques, le nombre d'informations à leur disposition, etc[1612].

[1604] Cass. com. 6 avr. 1993, n°91-14.523 ; Cass. civ. 1ère, 14 nov. 2006, n°04-15.276 : Bull. civ. I, n°470.
[1605] Cass. 2ème civ., 20 mars 2003, n°00-18028.
[1606] Cass. 1ère civ., 8 mai 1961 : Bull. civ. I, n°231 ; Cass. 3e civ., 25 mars 1971, n°70-10.434 : Bull. civ. III, n°222 ; Cass. 1ère civ., 7 juin 1996 : Bull. civ., I, n°346.
[1607] Cass. 2ème civ., 29 oct. 1980 : Gaz. pal. 1981.
[1608] Civ. 1ère, 14 nov. 2006, n°04- 15.276, Bull. civ. I, n°470.
[1609] C. pr. civ., art. 245, al.3 ou C. pr. pén., art. 167.
[1610] T. Moussa, *Dictionnaire juridique expertise – Matières civile et pénale*, 2e éd., Dalloz, 1988, 401 p. ; T. Moussa, « L'expertise judiciaire et les autres expertises au regard du principe de la contradiction », Rencontres université – Cour de cassation, BICC hors-série, 23 oct. 2004, n°3, p.51.
[1611] L. Dumoulin, *L'expert dans la justice. De la genèse d'une figure à ses usages*, Economica, 2007, p.138.
[1612] M. Herzog-Evans, « La perception de l'expertise par les JAP : une recherche empirique », AJ pénal, 2014, p. 516.

807. **Les réalités pratiques.** Ces différences de culture en fonction du domaine du litige ne peuvent être généralisées et systématisées puisqu'un pouvoir de contrainte de l'expertise s'exerce souvent[1613]. Dans la pratique, le juge retient généralement les conclusions de l'expert qu'il a désigné[1614]. Dans l'hypothèse d'un litige en matière de contentieux informatique ou pénal notamment, il n'est pas déraisonnable de penser que l'avis de l'expert sur une preuve *blockchain* particulièrement technique sera suivi par le juge.

808. **Conclusion du chapitre 1.** En conclusion de ce premier chapitre, le constat matériel des données enregistrées dans la *blockchain* par l'huissier semble constituer un acte superfétatoire dont les usagers de ces preuves peuvent en théorie se passer. En effet, même si la charge probatoire sera plus facile pour celui au bénéfice duquel la présomption de faits enregistrés issue du constat est adressée, le contenu et l'identification de la partie à l'enregistrement ne seront pas assurés, ce qui relaie ce constat à un rôle assez artificiel et subsidiaire pour le juge. Seul le lieu du constat ayant une valeur authentique sera propre à aider les problématiques de détermination du droit applicable. Bien que le constat ne soit pas un outil indispensable pour le plaideur, il sera toutefois une précaution à l'amorce de la démocratisation de ces nouvelles preuves *blockchains*. *A contrario*, l'expertise est d'un secours indéniable du simple apport de traduction en langage lisible des preuves *blockchains*, jusqu'à celui de l'intégrité des données, d'identification de l'enregistreur, voire celui de fiabilité des preuves *blockchains*. Si les bienfaits de l'expertise seront certains, le coût et les délais rallongés pourraient lui en ôter tout avantage. L'expertise pourrait de surcroît instaurer un rapport de dépendance avec le juge, lequel reprendra souvent ses conclusions techniques sur la preuve de données enregistrées dans la *blockchain*.

809. Intuitivement, le droit, par son cadre normatif étroit, minimise en apparence l'influence des auxiliaires dans le domaine des nouvelles technologies et de la *blockchain*. Les auxiliaires ne sauraient déborder de leur mission et s'immiscer dans l'édifice judiciaire, le « *sanctuaire de la justice* »[1615] sans « *altérer la pureté de la fonction juridictionnel*le »[1616]. Mais

[1613] K. Favro, M. Lobé Lobas, « La distanciation à l'égard de l'avis de l'expert », *in* K. Favro, M. Lobé Lobas, J.-P. Markus (ss. dir.), *L'expert dans tous ses états.* À *la recherche d'une déontologie de l'expert*, *op.cit.*, p.297.
[1614] J. Moury, « Les limites de la quête en matière de preuve : expertise et *jurisdictio* », RTD civ. n°4, oct. 2009, p.665-676.
[1615] L. Dumoulin, « L'expertise judiciaire dans la construction du jugement : de la ressource à la contrainte », Droit et Société n°44-45, Persée, 2000, p.205.
[1616] B. Oppeti, « Les rôles respectifs du juge et du technicien dans l'administration de la preuve en droit privé, *in* Institut d'Etudes Judiciaires, *Les rôles respectifs du juge et du technique dans l'administration de la preuve*, Puf, 1976, p.62.

discursivement, la place réelle des auxiliaires pourrait déborder de ce cadre et porter atteinte à l'indépendance de la justice dans ce domaine. Des palliatifs à ces risques seront ainsi suggérés (chapitre 2).

CHAPITRE 2
LES PALLIATIFS AUX RISQUES D'ATTEINTES A L'INDEPENDANCE DE LA JUSTICE EN MATIERE DE PREUVE DES DONNEES ENREGISTREES DANS LA *BLOCKCHAIN*

810. La liberté du juge se voit parfois résumée à ce questionnement : « *le chemin à plusieurs ou décider de tout en n'étant spécialiste de rien* »[1617]. Si cette question manichéenne semble quelque peu simpliste, le risque d'une dépossession de la fonction juridictionnelle - détenue jadis en propre par le magistrat - n'en n'est pas moins négligeable. Nous évoquerons donc ces risques de dépossession de la justice traditionnelle par les auxiliaires de justice en matière de preuve des données enregistrées dans la *blockchain* (section 1). L'influence exogène de ces auxiliaires sur les juges pourrait être de nature à affecter son indépendance. Alain Girardet, conseiller à la première chambre civile de la Cour de cassation et Professeur, proclamait en 2007 « *L'indépendance est en devenir ; elle a un passé et un avenir* »[1618]. L'avenir de l'indépendance du juge à bâtir se situe alors dans des propositions de son renforcement en matière de preuve des données enregistrées dans la *blockchain* (Section 2).

Section 1 : Les risques de dépossession de la justice traditionnelle par les auxiliaires en matière de preuve des données enregistrées dans la *blockchain*

811. L'auxiliaire comme substitut du juge est une question ancienne soulevée par les développements croissants des expertises judiciaires dans l'ensemble des domaines[1619]. Elle réinterroge les fondements de la justice dans le cadre des preuves de données enregistrées dans

[1617] P. Truche, *Juger, être jugé. Le magistrat face aux autres et à lui- même*, Fayard, 2001, p.149.
[1618] A. Girardet, « La réalité de l'indépendance judiciaire », mai 2007, p.1, https://www.courdecassation.fr/IMG/File/pdf_2007/10-05-2007/10-05-2007_girardet.pdf (consulté le 31/05/2020).
[1619] F. Vermeille cité *in* E. Edmond, « Les experts : auxiliaires ou substituts du juge ? », coll. Centre français de droit comparé, Revue internationale de droit comparé. Vol. 61 n°3, 2009, p.667 : « *Un rapport d'expertise technique bien construit et argumenté ne serait-il pas « de nature à renforcer l'impression que l'expert devient nolens volens le substitut du juge » ?* » ; Centre français de droit comparé, Colloque « Les experts : Auxiliaires ou substituts du juge », 5 dec. 2008 ; V. Loquin, « Les experts auxiliaires ou substituts du juge ? », *in* rapport de synthèse, Les experts : auxiliaires ou substituts du juge, Centre français de droit comparé, 2009, p.147 et s.

la *blockchain*, tant par des risques quant à l'ingérence de l'expert (paragraphe 1), que par la prédominance de la vérité cryptographique (paragraphe 2).

Paragraphe 1 : Les risques quant à l'ingérence de l'expert

812. Loin de l'approche neutralisée du Code de procédure civile, l'expertise ne prend pas la simple place tracée dans les ornières du droit, elle va bien plus loin : « *la réalité nuancée joue avec la règle* »[1620]. Le lien entre l'expert et le jugement en droit devient poreux[1621]. La vérité cryptographique pourrait donc servir la vérité juridictionnelle. L'adhésion systématique à l'avis de l'expert dans la construction du jugement (A), au risque d'un véritable « *règne* » des experts dans le traitement juridictionnel des preuves *blockchains* est une dérive possible qui ne peut être éludée (B).

A. Le risque d'adhésion systématique à l'avis de l'expert dans la construction du jugement

813. **Le rôle de l'expert confiné à ses missions.** L'expert n'est en principe invité à intervenir dans le processus judiciaire que dans la stricte mesure où il y a été convié, c'est un « *pourvoyeur d'analyse des techniques cryptographiques* ». Il ne peut guère s'octroyer le droit à une quelconque immixtion sur des questions de droit et d'aspects décisionnels[1622], ce qui lui accorde sa légitimité. Le juge démuni dans l'appréhension de pièces liées à la *blockchain* pourra toutefois se tourner vers l'expertise pour une analyse pertinente des faits dont il est saisi[1623]. Mais bien plus que de nourrir les réflexions du magistrat et le dossier judiciaire, l'expertise influence, voire intervient dans la construction du jugement.

[1620] L. Dumoulin, « L'expertise judiciaire dans la construction du jugement : de la ressource à la contrainte », *op.cit*., p.202.
[1621] Voir une démonstration de cette porosité en matière pénale : J.-R. Demarchi, *La preuve scientifique et le procès pénal*, Thèse ss. dir. C. Ambroise-Castérot, Nice, 2010, n°463 et s., p. 245 et s.
[1622] C. pr. civ., art. 238.
[1623] Voir en ce sens de façon générale dans les contentieux techniques : J. Moury, « Les limites de la quête en matière de preuve : expertise et *jurisdictio* », *op.cit*., p.665.

814. **« *L'art de la pioche* » dans les conclusions expertales.** Le jugement est normalement élaboré au bout d'un long « *processus cognitif complexe* »[1624] du juge s'appuyant sur des connaissances juridiques, un examen rationnel des faits, mais faisant aussi intervenir son bon sens. Il est louable de penser, de prime abord, que le juge sélectionne uniquement un certain nombre d'idées et d'éléments dans les conclusions de l'expert, ce qui a été nommé « *l'art de la pioche* »[1625]. Seuls certains passages considérés comme des ressources par le juge seraient utilisés pour soutenir son argumentation, tels que des chiffres, des analyses, des termes techniques.

815. **Réalités pratiques dans le contentieux technique.** Mais les textes qui encadrent les conditions de réalisation de l'expertise et la place de l'expert dans un rapport de subordination face au magistrat ne sont pas un reflet de la pratique dans les contentieux techniques. Si l'usage exact de la parole expertale dans le jugement ne peut pas être à ce stade réellement analysé en l'absence d'affaire jugée en France, des tendances sont à esquisser en matière de contentieux liés à la *blockchain*. En théorie, la parole expertale peut être contournée, délaissée, instrumentalisée mais elle peut aussi être suivie à l'identique. L'expert pourrait certainement participer « *(…) à la construction du syllogisme judiciaire en nourrissant sa mineure, voire même partiellement sa majeure. Il est d'une certaine façon coauteur partiel et caché de la décision judiciaire que seule le juge signe* »[1626]. Dans ce cas, le juge sera amené à décider uniquement des conséquences juridiques provoquées par les résultats scientifiques de l'expert. Ces conséquences juridiques pourraient toutefois être altérées. L'expert prendra donc une place considérable dans l'élaboration du jugement et cela affecterait la *juridicitio*[1627]. Par exemple, le juge reprenant verbatim les analyses du rapport de l'expert sur la fiabilité ou non d'une preuve *blockchain* pourrait biaiser ses orientations en droit. L'expert pourrait en effet être influencé dans sa position par rapport à telle ou telle nature de *blockchain* ou de protocole, voire un fournisseur de technologie en particulier.

816. **Pénétration des experts dans la construction du jugement**. Ces partenaires des juges se sont installés progressivement dans l'espace judiciaire, pénétrant le cœur de ce qui constitue

[1624] L. Dumoulin, « L'expertise judiciaire dans la construction du jugement : de la ressource à la contrainte », *op.cit*., p.211.
[1625] *Ibid*., p.207.
[1626] V. Loquin, « Les experts auxiliaires ou substituts du juge ? », *op.cit.*, p.153.
[1627] Voir les alertes sur ces risques : J. Moury, « Les limites de la quête en matière de preuve : expertise et *jurisdictio* », *op.cit*., p.665-676.

l'essence de l'activité de justice : le jugement[1628]. Naguère, une circulaire du premier président de la Cour d'appel de Paris du 2 février 1967 alertait déjà sur « *le recours trop facile à l'expertise* »[1629]. Elle relevait que « *le juge (...) ne doit ni céder aveuglément à la demande qui lui en est faite, ni entériner les conclusions d'un rapport sans un examen approfondi, sinon (il) manquerait à sa mission de juger* » rappelant aussi que « *le juge ne doit consentir aucune délégation de pouvoir à l'expert* ». La doctrine s'est aussi emparée de ce sujet, avertissant sur le suivi presque aveugle des conclusions expertales par le juge civil, parce qu'il détient un savoir technique faisant défaut au magistrat[1630]. L'expertise fonctionnerait comme une sorte de « *ressource-contrainte* »[1631] susceptible « *d'être instrumentalisée par les acteurs judiciaire mais aussi de les contraindre et de peser sur la construction du jugement* »[1632].

817. **Influence des sciences exactes dans la construction du jugement.** C'est cette légitimité scientifique de l'expert en sciences dures, cette forme de caution scientifique qui donne une « *réalité objectivée et attestée* » aux juges[1633]. Se développe alors un nouveau genre de « *procès technique dans le procès judiciaire* »[1634]. La capacité de l'expertise à accorder des certitudes définit le niveau de participation du technicien dans l'élaboration du jugement[1635]. La nature de la discipline joue ainsi sur l'influence de l'expertise dans la construction du jugement[1636]. Si une discipline est une science dite « *exacte* », comme les mathématiques issues des preuves *blockchains*, les résultats expertaux auront fréquemment un caractère péremptoire, avec des énoncés affirmatifs considérés comme vrais et de ce fait, ils pourront contraindre le jugement. Cette participation de plus en plus importante des disciplines techniques, comme le secteur des nouvelles technologies, et nécessairement de la *blockchain*, dans la construction du

[1628] L. Dumoulin, « L'expertise judiciaire dans la construction du jugement : de la ressource à la contrainte », *op.cit*.,p.200.
[1629] Circulaire CA de Paris du 2 février 1967 : JCP 1967, III, 125.
[1630] L. Cadiet et E. Jeuland, Cadiet et E. Jeuland, *Droit judiciaire privé*, 5e éd., Litec, 2006, n°390 ; F. Ferrand, « Preuve », *op.cit.*, n°450 ; J. Moury, « Les limites de la quête en matière de preuve : expertise et *jurisdictio* », *op.cit*., p.670, n°8.
[1631] L. Dumoulin, « L'expertise judiciaire dans la construction du jugement : de la ressource à la contrainte », *op.cit*., p.199.
[1632] *Ibid*.
[1633] *Ibid*., p.214.
[1634] D. Tricot, « Qualification et indépendance de l'expert », *in* Les experts : auxiliaires ou susbtituts du juge, coll. Centre français de droit comparé, 2009, p.53 et s.
[1635] L. Dumoulin, « L'expertise judiciaire dans la construction du jugement : de la ressource à la contrainte », *op.cit*., p.200.
[1636] *Ibid*., p.218.

jugement nous amène à reconsidérer la place du magistrat dans le jugement. Elle fait varier le rôle du magistrat du « *maître de la décision* »[1637] en un simple « *organisateur* »[1638].

818. **Risques de transformation de la vérité cryptographique en vérité juridictionnelle.** Le risque d'user excessivement de la parole expertale est qu'elle devienne une ressource unique, une structure jusqu'à déterminer le jugement, transposant les vérités cryptographiques en vérité juridictionnelle. Cette vérité cryptographique pourrait alors avoir une fonction normative, devenant ainsi acteur actif de la décision judiciaire[1639]. Le juge serait ainsi dépossédé dans la construction du jugement. Ce risque de dépossession pourrait également être perçu comme une forme de « *déresponsabilisation* » du juge[1640].

B. Le risque d'un « *règne* » des experts dans le traitement juridictionnel des preuves *blockchains*

819. **Évolution de l'idée d'un « *règne* » des experts[1641].** L'idée ancienne du règne des experts était une obsession perçue comme baroque, mais elle prend une tournure on ne peut plus sensée à notre ère de la *blockchain* où l'« *emballement technicisant* »[1642] impliquerait l'intervention de façon systématisée d'experts et ce de manière excessive[1643]. D'un simple éclairage sur les faits litigieux en raison de ses compétences, nous pourrions en venir à un recours « *routinisé* » au savoir-faire expertal[1644].

820. **Nature de l'expertise influant sur le « *règne* » des experts.** Le règne des experts pourra être plus ou moins marqué en fonction de la nature de l'expertise. Il est possible de distinguer trois types d'expertises faisant varier la place de l'expert : l'expertise obligatoire,

---

[1637] *Ibid*., p.200.
[1638] *Ibid*.
[1639] O. Leclerc, *Le juge et l'expert. Contribution à l'étude des rapports entre le droit et la science*, LGDJ, coll. Bibliothèque droit privé, 2005, n°196.
[1640] J. Boirot, « Expertise juridique et expertise scientifique : L'interactivité juges/experts, source d'indépendance », *in* K. Favro, M. Lobé Lobas, J.- P. Markus (ss. dir.), *L'expert dans tous ses états. À la recherche d'une déontologie de l'expert*, *op.cit.*, p.127.
[1641] L'expression de « *règne des experts* » est reprise du Professeur Ellul historien du droit, sociologue et théologien : J. Ellul, « Le bluff technologique », Hachette Littératures, 2004, p.353, 355.
[1642] C. Protais, « Le réajustement du rapport juge/expert : entre consensus et domination », Revue internationale interdisciplinaire, 2008, p.181-200, n°21.
[1643] Voir le risque de gouvernement des experts déjà dénoncé par la doctrine : L. Dumoulin, « L'expertise judiciaire dans la construction du jugement : de la ressource à la contrainte », *op.cit*., p.203.
[1644] J. Boirot, « Expertise juridique et expertise scientifique : L'interactivité juges/experts, source d'indépendance », *op.cit.*, p.127.

l'expertise obligée et l'expertise nécessaire[1645]. Si l'expertise est obligatoire, c'est-à-dire requise et régie par des textes, ces mesures répondront davantage à un formalisme juridique qu'à un impératif pratique dans l'éclairage du juge. Elle n'aurait donc pas en principe un intérêt majeur pour la recherche de la vérité, et le risque d'un règne des experts serait moindre. Ce risque est d'autant plus écarté qu'aucune expertise requise par la loi n'est recensée pour l'instant à notre connaissance dans le domaine de la *blockchain*. Si l'expertise est obligée conformément à la nature de l'infraction ou des circonstances de la commission de celle-ci, comme les cas de violences sexuelles en matière pénale, son caractère est contraignant puisqu'elle exprime la « *caution morale* » qui précède et accompagne la prise de décision du juge. Dans cette hypothèse, l'adhésion contrainte aux conclusions des experts pourrait encourir un risque de règne des experts. Les infractions pénales appliquées aux actifs numériques et à la *blockchain* se multipliant[1646], cette hypothèse ne peut être écartée. Enfin, si l'expertise est nécessaire, c'est-à-dire que l'intervention est justifiée par la nature complexe du dossier, la contrainte cognitive sera la plus forte car l'expertise est alors empiriquement impérative. Cette hypothèse est complètement représentative des cas que l'on pourrait couramment retrouver avec la complexité des dossiers *blockchains*. De cela, le risque de la parole expertale hégémonique interpelle, nous ne saurons ainsi occulter une pareille évolution de règne des experts de notre analyse.

821. **Risque du « *règne* » des experts : une hégémonie des sciences mathématiques-informatiques.** Si le juge n'a plus pleinement son pouvoir d'appréciation[1647], la crainte du règne des experts est pleine et entière. La parole du technocrate qui tend à faire prévaloir les aspects techniques, au détriment de l'élément humain, serait différente de celle du juge qui considère les particularismes sociaux et culturels. Le juge doit ainsi conserver son double pouvoir d'appréciation, dans la mise en œuvre des procédés techniques de la *blockchain* comme sur l'objet, les preuves *blockchains* elles-mêmes.

822. Avec le recours à la parole scientifique, la justice contemporaine pourra prétendre au vrai, elle ne sera toutefois plus guidée par le droit mais par les sciences mathématiques et informatiques. Cette dépendance du juge par rapport au pouvoir cognitif de l'expert[1648] pourra

[1645] *Ibid.*, p.129.
[1646] Voir *supra* n°586 et s.
[1647] R. Houin, « Le progrès de la science et le droit de la preuve », *op.cit.*, p.74.
[1648] J. Boirot, « Expertise juridique et expertise scientifique : L'interactivité juges/experts, source d'indépendance », *op.cit.*, p.128 et s.

entraîner dans sa perception la plus extrême une dictature des sciences mathématiques-informatique et plus largement, des sciences fondamentales[1649].

823. Ce phénomène a été entraperçu par Bruno Oppetit en 1976 qui redoutait un « *effacement du généraliste derrière le spécialiste ou l'homme de l'art (qui) n'est qu'un aspect du phénomène plus général du passage de la culture à la technique* »[1650]. Ce désir de vérité cryptographique absolu - certainement trop ambitieux - guidé par les promoteurs de la *blockchain* traduisant une « *technophilie* »[1651] exacerbée pourrait amener à mélanger un objectif scientifique à une attente extra-scientifique qu'est la justice. Cela dit, un siècle qui se dit lié à l'évolution des technologies, ne se doit-il pas finalement de juger techniquement ses litiges liés à la technologie. Le sociologue et psychologue Jean-Gabriel Tarde exprimait d'ailleurs à son époque en 1890 que « *les ordalies, puis la torture, puis le jury, bientôt l'expertise tels ont été ou seront les talismans successifs imaginés pour la découverte du vrai en justice* »[1652].

Paragraphe 2 : Les risques quant à la prédominance de la vérité cryptographique

824. La logique profane de la vérité cryptographique introduite « *au plus profond du judiciaire* » interroge. La distinction entre vérité scientifique et vérité cryptographique devient alors poreuse (A). Toutefois, la vérité cryptographique comme toute autre vérité scientifique reste évolutive, le postulat selon lequel elle est inébranlable doit être nuancé car cette vérité cryptographique se révèle aussi relative (B).

A. La distinction poreuse entre vérité juridictionnelle et vérité cryptographique

825. **Rapports entre vérité cryptographique et vérité juridictionnelle.** La frénésie technologique autour de la technologie *blockchain* est de nature à servir la vérité cryptographique, forme de vérité scientifique opposée de prime abord à la vérité juridictionnelle. Il existe donc un décalage de principe entre cette preuve technique parfaite, qui

[1649] Voir sur cette notion de dictature des sciences : J. Moury, « Les limites de la quête en matière de preuve : expertise et *jurisdictio* », *op.cit.*, p.668.
[1650] B. Oppeti cité *in* Colloque des Instituts d'études judiciaires (X^{ème}), Les rôles respectifs des juges et du technicien dans l'administration de la preuve en droit privé, Puf, 1976, p.54.
[1651] L. Cadiet, J. Normand et S. Amrani-Mekki, *Théorie générale du procès*, *op. cit.*, n°36.
[1652] J.-G. Tarde, *La philosophie pénale*, Paris Cujas, coll. Bibliothèque internationale de criminologie, 4^{e} ed., 1972 (1ère ed. 1890), p.436.

ne coïncide pas avec la preuve juridique conduisant à la vérité juridictionnelle, celle qui soutient le juste. En exprimant le réel, c'est l'expert qui contribue à façonner une vérité particulière qui n'est pas la vérité juridictionnelle mais la vérité cryptographique. Il « *compose* » en effet le « *discours de vérité cryptographique* » qui s'imposera au juge[1653]. Non confinées l'une de l'autre dans le cadre d'un litige, la vérité cryptographique et la vérité juridictionnelle se retrouvent dans un rapport direct d'interrelation. La justice sollicite une source de vérité extérieure à la vérité juridictionnelle pour établir le vrai. Nous devons donc traiter en détail ce qui les distingue et ce qui les rassemble.

826. **Éloignement de la vérité cryptographique et vérité juridictionnelle.** La vérité cryptographique est une vérité objective, une « *vraie vérité* » à laquelle on pourrait prêter une vérité incontestable qui saurait justement accorder une caution judiciaire. Contrairement à la vérité juridictionnelle, vérité de l'homme qui peut parfois être arbitraire et subjective, qui représente ce que le juge veut considérer et faire accepter comme vrai[1654].

827. La vérité cryptographique ne serait pas variable car elle est exacte et réduit les approximations que connaît la vérité juridictionnelle. Elle est toutefois évolutive, contrairement à la vérité juridictionnelle statique qui, au moment où les juges statuent, indique l'état des connaissances vraisemblables et peu contestables lorsque l'on s'interroge sur leur réalité. La traduction de cette vérité statique se retrouve pleinement dans l'adage *res judicata pro veritate habetur* signifiant que la chose jugée est tenue pour vérité.

828. La vérité juridictionnelle ne sera pas autonome et considère bien d'autres réalités que la seule réalité scientifique et cryptographique ; elle arbitre parmi un ensemble de réalités culturelles et sociales. Si nous prenons le cas de la vérité biologique, par exemple, la filiation n'est pas seulement un code génétique. La biologie fait les origines, mais elle n'établira pas la filiation[1655]. À ce même titre, la *blockchain* pourra apporter un horodatage certain pour la preuve d'une antériorité sur une œuvre de l'esprit mais cela ne signifie pas pour autant que cette œuvre sera originale. Cette appréciation de l'originalité dépassera donc la seule vérité cryptographique de l'horodatage *blockchain*.

[1653] Voir en ce sens le « discours de vérité » dans le fait de gouverner : M. Foucault, « La gouvernementalité », *in* Dits et écrits, 1954-1988, t.3, n°239, Gallimard, coll. Bibliothèque des sciences humaines, 1994, p.635-657.
[1654] M. Mekki, « Vérité et preuve. Rapport français », *op.cit.*, p.827, n°2.
[1655] P. Malaurie, *Droit de la famille*, LGDJ, 6e ed., janv. 2018, n°958.

829. **Rapprochement de la vérité cryptographique et vérité juridictionnelle.** Contrairement à l'expression de Paul Vidonne formulée sur un « *no bridge* » entre vérité juridictionnelle et vérité scientifique, qui selon lui est dû au fait que la science a pour but de démontrer la vérité relative au monde réel alors que le droit a lui pour objet de faire fonctionner le monde[1656], nous pensons qu'il y a un pont entre la vérité juridictionnelle et la vérité cryptographique établissant des liens de connexion.

830. Classiquement, l'ampleur des recours à l'expertise est une traduction manifeste de la participation de la vérité scientifique, cryptographique, à la vérité juridictionnelle[1657]. La vérité scientifique est complémentaire et fonde parfois la vérité juridictionnelle : lorsqu'il s'agit d'établir l'existence objective de faits conditionnant la mise en œuvre de la règle de droit, notamment[1658].

831. La vérité cryptographique se rapproche de la vérité juridictionnelle dans la mesure où dans les domaines techniques, le fait techniquement constaté est très proche du fait juridiquement recherché. Les attentes de vérité juridictionnelle sont finalement très proches de celle fournies par la vérité cryptographique.

832. La vérité cryptographique, comme la vérité juridictionnelle, ne sont pas modifiables. Non transformable, la vérité cryptographique n'est donc pas une vérité fragile (contrairement à d'autres vérités comme celle parfois puisée sur internet). La vérité juridictionnelle n'est pas non plus modifiable : une fois la décision rendue, le juge ne peut revenir dessus. Il est d'ailleurs obligé de la rendre, à peine de déni de justice[1659]. Elle est toutefois susceptible de recours.

B. La vérité cryptographique relative

833. **Vérité cryptographique et relativisme.** La vérité cryptographique, présentée comme absolue, juste et réelle apparaît comme un truisme inébranlable. Derrière cette vérité absolue presque dogmatique, le relativisme qui pourrait aussi la caractériser se dessine de proche en

[1656] Expression de P. Vidonne cité in M. Garcias, M. Chouzier, « La preuve informatique – Quelles nouveautés techniques pour quelles évolutions juridiques », Lexbase Hebdo édition affaires n°280, janv. 2012, p.3.
[1657] M. Mekki, « Vérité et preuve. Rapport français », *op.cit.*, p.816.
[1658] O. Leclerc, *Le juge et l'expert – Contribution à l'étude des rapports entre le droit et la science*, LGDJ, 2005, n°110.
[1659] C. civ., art. 4.

proche. La vérité cryptographique est en effet « *partagée entre le désir d'absolu et les contraintes du relatif* »[1660].

834. **L'erreur dans la vérité cryptographique.** L'erreur mathématique - dans la prise de contact avec un concept, l'application d'un concept appris, la réalisation d'un calcul, la représentation d'une situation - fait partie de tout procédé et ne peut être évitée puisque « *ni le savoir technique, ni l'objectivité, ni la connaissance scientifique ne prémunissent contre les erreurs* »[1661]. L'erreur et la confrontation participent à la vérité scientifique[1662] et à la vérité cryptographique *de facto*. La vérité cryptographique en tant que preuve cryptographique connaît alors une certaine relativité, ses propres limites. La vérité cryptographique annoncée comme une vérité dogmatique, incontestable et intangible, formulée par le code, nouvelle institution ou autorité qui ferait foi, n'est pourtant pas épargnée d'erreurs dans le code et d'autres erreurs mathématiques générant des dysfonctionnements du réseau[1663].

835. **Le doute dans la vérité cryptographique.** La technologie *blockchain* dans la preuve réduit le doute car la preuve est informatiquement exacte. Les incertitudes épistémologiques dans la technologie *blockchain* existent cependant dans l'aléa de l'étude des sciences de la cryptographie distribuée, leurs méthodes et leurs découvertes.

836. Le doute pourra résider dans le protocole ou les algorithmes employés par une *blockchain*. Certaines architectures de protocole peuvent être sujettes à polémique car peu fiables ou peu stables, avec des algorithmes non vérifiés. L'illustration symptomatique est l'algorithme de consensus distribué, la véritable pierre angulaire d'une *blockchain* qui permet aux agents validateurs de faire entrer une transaction dans le registre. Rachid Guerraoui, Professeur et ancien titulaire de la chaire Informatique et sciences numériques au Collège de France reconnu pour ses travaux relatifs aux calculs distribués, fait part de ses doutes et critiques sur la performance de l'algorithme de consensus utilisé par bitcoin[1664]. Les concepts

[1660] V. Lassere-Kiesow, « La vérité en droit civil », D. 2010, p.907.
[1661] Cour de cassation, rapport annuel, La preuve, *op.cit.*, p.85.
[1662] G. Bachelard, *Le nouvel esprit scientifique*, PUF, 1971, p.177 ; K. Popper, *Le réalisme et la science*, Hermann, 1990, p.8-11.
[1663] Voir l'affaire dite « *The DAO* » *supra* n°108.
[1664] Cours du collège de de France en partenariat avec l'Inria - Chaire Informatique et sciences numériques « Si *Blockchain* est la solution, quel est le problème », par R. Guerraoui « Demystifier Bitcoin. Voyage au cœur de l'algorithme répartie », le 1 mars 2019, https://www.college-de-france.fr/site/rachid-guerraoui/course-2019-03-01-10h00.htm (consulté le 31/05/2020).

d'algorithmie répartie sont à la fois compliqués[1665] et empreints de doutes. Selon Rachid Guerraoui, l'élection de « *leader* » est un problème fondamentalement complexe dans la mise en place d'un cahier d'opérations permettant de mettre en ordre les transactions. Une fois la difficulté de l'élection du leader levée, les transactions peuvent être mises en ordre dans une machine dupliquée décrite par Leslie Lamport, chercheur en informatique, en 1978[1666].

837. Les résultats d'algorithme réparti de Michael J. Fisher, Nancy A. Lynch, et Michael S. Paterson en 1985 mettent en évidence qu'aucun algorithme asynchrone ne peut résoudre le consensus[1667]. Mais si les chercheurs opèrent des hypothèses sur le temps et se permettent des résultats probabilistes, il est possible de contourner cette impossibilité de principe. Depuis, nombre de travaux en algorithmique répartie se sont focalisés sur la manière de contourner l'impossibilité du consensus[1668]. Le prix pour permettre ce consensus est ainsi le temps de latence et la consommation d'une grande énergie que l'on retrouve - non sans critique selon Rachid Guerraoui - dans bitcoin.

838. Ces doutes scientifiques ont nécessairement un impact sur la fiabilité de la preuve fournie en fonction de l'algorithme distribué utilisé par la *blockchain* en cause. Si l'algorithme a été prouvé mathématiquement ou s'il ne l'a pas été, la fiabilité sera variable. Selon Ricardo Perez Marco, chercheur au CNRS, l'algorithme de la preuve de travail utilisé dans Bitcoin et Ethereum a été prouvé mathématiquement, contrairement à celui de la preuve d'enjeu à l'étude[1669].

839. **Appréhension du doute dans la vérité cryptographique par le juge.** Le juge ne pourra finalement jamais exclure totalement le doute sur la vérité cryptographique puisque « *toute preuve implique l'existence d'un doute. Là où tout est clair et sans ambiguïté, là où aucune question ne se pose, on ne saurait user de la preuve, de même qu'une personne en bonne santé n'a que faire des remèdes* »[1670]. Cela impliquera une certaine vigilance du juge, mais qui

[1665] D. Conan, « Initiation à l'algorithmique répartie », Cours de Telecom Sud Paris, CSC4509, avr. 2019, p.15-16, https://www-inf.telecom-sudparis.eu/COURS/AlgoRep/Web/poly_initar_etudiants.pdf (consulté le 31/05/2020).
[1666] L. Lamport, « Time, clocks, and the ordering of events in a distributed system », Communications of the ACM, vol. 21, issue 7, 1978, p.558-565.
[1667] M. Fisher, N. Lynch, M. Paterson, « Impossibility of consensus with one faulty process », Journal of the ACM, vol. 32, n°2, 1985, p.374-382.
[1668] R. Guerarоui, *L'algorithmique répartie : à la recherche de l'universalité perdue*. *Leçon inaugurale prononcée au Collège de France le jeudi 25 octobre 2018*, OpenEdition Books, 4 dec. 2019, n°107.
[1669] R. Perez Marco, « Ricardo Perez-Marco : "95 % des monnaies créées aujourd'hui vont disparaître" », *op.cit.*
[1670] H. Lévy-Bruhl, *La preuve judiciaire. Étude de sociologie juridique*, *op.cit.*, n°15.

ne sera pas différente de celle portée à d'autres vérités. Le célèbre Doyen Carbonnier avançait que « *le jugement est un doute qui décide ; le procès, l'institution d'une mise en doute* »[1671]. L'ancien premier président de la Cour de cassation Bertrand Louvel assenait quant à lui lors d'un discours au cours du Colloque « *La vérité… sans doute. Vérité scientifique, vérité judiciaire* » que « *c'est cet exercice raisonné du doute qui, sans nous paralyser, imprime en chacun une prudence et fonde, je crois, cette éthique commune que le juge et l'expert, tous deux soucieux de vérité, ont en partage. Les procédures, celles du procès comme d'un protocole de recherche, s'y offrent comme des garanties ; le doute comme une méthode ; toutes indispensables à la pertinence et la justesse du résultat. Alors pardonnez-moi, mais « la vérité sans le doute » n'existe pas…* »[1672].

840. **Doutes exclus par le droit.** Dans certains cas les doutes sont exclus par le droit, notamment en matière pénale en vertu du principe *dubio pro reo*, adage selon lequel un accusé ne peut être condamné dans l'affaire pénale si le tribunal reste douteux quant à sa culpabilité. La Cour de cassation prohibe également les motifs dubitatifs[1673]. Dans d'autres cas, le doute est contrôlé[1674]. Il est ainsi contrôlé rigoureusement par la Cour de cassation lorsque les juges du fond n'ont pas usé des mesures d'instruction ou encore ordonné un complément d'expertise ou interrogé l'expert[1675]. Ces exclusions du doute par le droit pourront être particulièrement ardues à appréhender dans le contexte de la vérité cryptographique, si cette dernière fait l'objet de doutes particuliers.

841. Ainsi, au même titre que la vérité scientifique, la vérité cryptographique ne fait pas exception aux incertitudes. La vérité cryptographique est relative, avec une part d'incertitude qui subsiste en tout examen, soit en raison des limites des données de la connaissance, soit en fonction des conditions de son intervention. Des incertitudes et inconnues pèsent donc sur le discours scientifique. Parfois les questions soumises à l'expert ne sont pas stabilisées scientifiquement, ou sujettes à polémiques et l'expert peut d'ailleurs l'exposer[1676]. Dans ce cas,

---

[1671] J. Carbonnier, *Sociologie juridique*, PUF, coll. Thémis, 1978, p.194.
[1672] Cour de cassation, Colloque « La vérité… sans doute. Vérité scientifique, vérité judiciaire » (commémorant le trentenaire de la Compagnie des experts agréés par la Cour de cassation), Discours de Monsieur B. Louvel, premier président de la Cour de cassation, le 2 oct. 2015.
[1673] X. Lagarde, *Réflexion critique sur le droit de la preuve*, *op.cit.*, p.216 et s., n°137 et s. Voir les critiques : J.-F. Césaro, *Le doute en droit privé*, préf. B. Teyssié, Éd. Panthéon-Assas, LGDJ, 2003, p.210 et s., n°157 et s.
[1674] M. Mekki, « Réflexions sur le risque de la preuve en droit des contrats (1ère partie), *op.cit.*, p.681 et s.
[1675] Cass. 1ère civ., 30 janv. 2007, n°06-11028 : Procédures 2007, comm. n°79, obs. R. Perrot ; JCP G 2007, I, 200, n°17, obs. E. Jeuland.
[1676] J. Moury, « Les limites de la quête en matière de preuve : expertise et *jurisdictio* », *op.cit.*, p.670, n°16.

le juge aura une certaine latitude et devra statuer parfois entre ce qui lui parait « *possiblement vrai* » et « *certainement faux* »[1677]. Pour les plaideurs, l'incertitude générée par la vérité cryptographique les soumettra aux aléas des procédures et aux risques que leur preuve cryptographique ne soit pas retenue. En apprenant à mieux connaître les sciences (informatiques), « *nous devons (aussi) vivre avec l'incertitude* », selon le philosophe Edgard Morin[1678]. Sciences dures et incertitudes semblent donc indissociables[1679].

842. **Vérité cryptographique empreinte d'évolution.** « *La permanence de l'image idéale de la preuve scientifique constitue une croyance partagée* »[1680] ou une « *idéologie sociale* »[1681]. Henri Atlan, médecin biologiste et philosophe a admis que la vérité scientifique est « *elle aussi, un ornement du réel* »[1682]. Une vérité scientifique ne serait jamais absolue, jamais acquise mais finalement transitoire[1683]. Par ailleurs, la vérité cryptographique ne serait pas nécessairement toujours stable et pourra faire l'objet d'évolutions grâce aux diverses méthodes heuristiques usitées de la recherche ou aux développeurs très actifs sur cette technologie, soutenus par les pouvoirs publics. Le rapport Mis/De La Raudière annonce à ce titre dans sa proposition n°17 l'appui à la réalisation des projets de recherche et développement afin de renforcer les capacités de chiffrement des protocoles fondés sur la technologie des *blockchains*[1684]. La vérité cryptographique est donc tout compte fait une vérité provisoire. Elle est susceptible d'être réévaluée en fonction de la durée de vie des algorithmes, notamment. Le risque pesant sur la vérité cryptographique est donc son érosion par l'effet du temps et des évolutions des techniques

[1677] A. Comte-Sponville, *Justice et vérité, in* Expert du juge, expert de partie, vérité scientifique et vérité judiciaire, XVII[ème] Congrès national des experts judiciaires, p.90.
[1678] Intervention au sujet de la crise épidémiologique du Covid19 de 2020 https://lejournal.cnrs.fr/articles/edgar-morin-nous-devons-vivre-avec-lincertitude?utm_term=Autofeed&utm_medium=Social&utm_source=Twitter#Echobox=1586179455 (consulté le 31/05/2020).
[1679] Cour de cassation, Colloque « La vérité... sans doute. Vérité scientifique, vérité judiciaire » (commémorant le trentenaire de la Compagnie des experts agréés par la Cour de cassation), Discours de Monsieur B. Louvel, premier président de la Cour de cassation, le 2 oct. 2015.
[1680] E. Truilhé-Marengo, « Les rapports du droit et de la science », *in* K. Favro, M. Lobé Lobas, J.- P. Markus (ss. dir.), L'expert dans tous ses états. *À la recherche d'une déontologie de l'expert, op.cit.*, p.119.
[1681] E. Truilhé-Marengo, « Des preuves dans les pratiques scientifiques et dans les pratiques juridiques. Prolégomènes à une conversation », *in Preuve scientifique, preuve juridique*, Bruxelles, Larcier, 2011, p.33 s.
[1682] H. Altan, *A tort et à raison. Intercritique de la science et du mythe*, Points, Seuil, 1986, p.28.
[1683] Voir les développements selon lesquels la vérité scientifique n'est pas absolue : M. Allais, « Autorité de la science ou autorité en matière de science ? L'immense danger d'une domination oppressive des pseudo-vérités établies », *in L'autorité*, ss. dir. J. Foyer, G. Lebreton et C. Puigelier, Puf, coll. Cahiers des sciences morales et politiques, 2008, p. 117 et s. ; K. Popper, *La connaissance objective*, trad. J.-J. Rosat, Flammarion, coll. Champs essais, 1998, p. 115 et s.
[1684] Assemblée Nationale, Rapport d'information n°1501, *op.cit.*, p.98.

cryptographiques. Le progrès des connaissances scientifiques entraîne une forme d'obsolescence de la vérité cryptographique.

Section 2 : Les propositions de renforcement de l'indépendance du juge en matière de preuve des données enregistrées dans la *blockchain*

843. Alors que la question de l'indépendance se posait entre les juges et le pouvoir exécutif et législatif avant la révolution française et avec une résurgence au XIX[ème] siècle[1685], elle interroge aujourd'hui de manière lancinante au sujet des auxiliaires en matière de nouvelles technologies. L'indépendance, comme d'autres critères comportementaux, relève de la déontologie, de l'éthique, et de la morale[1686]. Si l'indépendance du juge constitue une possibilité de « *prendre des décisions à l'abri de toute instruction ou pression* »[1687], elle serait bien plus : une liberté pour le juge de « *(…) conduire et d'exposer son analyse pour aboutir à une décision qu'il aura prise en respectant un corpus de règles et de valeurs qui fondent son office* »[1688]. L'indépendance du pouvoir judiciaire en tant que corps, et des magistrats le composant, est matérialisé par deux éléments : un élément objectif, c'est-à-dire que l'indépendance constitue une caractéristique dont le système judiciaire ne saurait faire l'économie, et un élément subjectif en vertu duquel toute personne a le droit de voir ses droits et ses libertés établis par un juge indépendant[1689]. Ces deux éléments se justifient par la nécessité pour les juges de remplir leur mission de gardiens des droits et des libertés.

844. Pour renforcer son indépendance, le juge doit alors exercer ses pleins pouvoirs dans son office et veiller à l'innocuité des auxiliaires dans le cadre des données enregistrées dans la *blockchain*. Pour cela, nous formulerons des propositions d'approfondissement des obligations déontologiques (paragraphe 1), qui, outre le cadre normatif formel, devront faire évoluer les pratiques professionnelles avec des outils concrets d'indépendance des magistrats (paragraphe 2).

[1685] A. Girardet, *La réalité de l'indépendance judiciaire*, *op.cit.*, p.2.
[1686] C. Lienhard, « Les principes généraux du comportement du "bon expert" », *in* K. Favro, M. Lobé Lobas, J.-P. Markus (ss. dir.), *L'expert dans tous ses états. À la recherche d'une déontologie de l'expert*, *op.cit.*, p.78.
[1687] Cons. const. n°2007-551 DC, 1[er] mars 2007.
[1688] A. Girardet, *La réalité de l'indépendance judiciaire*, *op.cit.*, p.1.
[1689] Commission de Venise, Étude n°494/2008, Rapport sur l'indépendance du système judiciaire partie I : l'indépendance des juges, Adopté par la Commission de Venise lors de sa 82[ème] session plénière, 12-13 mars 2010, p.3, n°6.

Paragraphe 1 : Une proposition d'approfondissement des obligations déontologiques

845. Les magistrats ont entre leur main l'honneur, la sûreté et les intérêts des citoyens[1690]. En pleine crise de confiance publique des citoyens en nos institutions et en la justice, le renforcement de l'indépendance entre le juge et ses auxiliaires est une nécessité. Jacques Mézard, membre de la mission d'information sur le redressement de la justice avançait que « *le statut des magistrats mériterait à lui seul un débat spécifique. Il est nécessaire de faire évoluer (…) et de renforcer leur indépendance, qui va de pair avec une certaine neutralité – nul besoin d'y insister* »[1691], dans le rapport d'information issu de cette mission dont est extrait ce propos. Les textes normatifs imposent des obligations suffisantes d'indépendance et d'impartialité des juges sans lesquelles leurs jugements perdraient la confiance des justiciables (A). Il convient également de développer le renforcement textuel des obligations déontologiques de l'expert, corrélées à celles du juge (B).

A. Le socle textuel suffisamment exigeant quant aux obligations déontologiques du juge

846. Le « *socle naturel de la justice* »[1692] est basé sur la déontologie professionnelle très exigeante et de plus en plus précise du magistrat en lien avec les attentes des citoyens à des fins de bonne justice. Les textes qui entourent le magistrat de garanties pour « *pallier la nécessaire imperfection de l'homme* »[1693] sont naturellement applicables aux futurs contentieux mettant en cause des preuves *blockchains*.

847. **Dimension universelle de l'obligation d'indépendance.** Tout d'abord, l'article 10 de la Déclaration universelle des droits de l'homme du 10 décembre 1948 offre une dimension universelle à l'obligation d'indépendance en précisant que « *toute personne a droit, en pleine égalité, à ce que sa cause soit entendue équitablement et publiquement par un tribunal*

[1690] A. Legoux, « Vérité médicale, vérité juridique », Gaz. pal. n°277, oct. 2014, p.19.
[1691] Rapport d'information n°495 au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale, par la mission d'information sur le redressement de la justice, de M. P. Bas, E. Benbassa, J. Bigot, F.-N. Buffet, C. Cukierman, J. Mézard et F. Zocchetto, déposé le 4 avril 2017, p.330.
[1692] Discours de B. Louvel (premier président de la Cour de cassation), L'indépendance du juge dans son contexte judiciaire et social, sept. 2018.
[1693] Colloque « La déontologie des magistrats de l'ordre judiciaire : la déclaration d'intérêt », Allocution d'ouverture de J.-M. Marin, 30 juin 2017.

indépendant et impartial, qui décidera, soit de ses droits et obligations, soit du bien-fondé de toute accusation en matière pénale dirigée contre elle ». C'est après la Seconde Guerre mondiale que ce principe a été établi et est mis en œuvre par une autonomisation progressive de l'institution judiciaire.

848. **Dimension européenne de l'obligation d'indépendance.** À l'échelle européenne, le droit à un tribunal indépendant et impartial est aussi une composante du droit au procès équitable visé à l'article 6 paragraphe 1 de la Convention européenne des droits de l'homme de 1950. La charte des droits fondamentaux de l'Union européenne du 18 décembre 2000 ajoute au deuxième alinéa de son article 47 que « *toute personne a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable par un tribunal indépendant et impartial, établi préalablement par la loi* (…) »[1694]. Enfin, la délibération du Conseil Consultatif des Juges Européens du 26 et 27 mars 2007, consacrée aux Conseils supérieurs de la magistrature des différents États appartenant au Conseil de l'Europe à Rome, mentionne que « *l'indépendance est une garantie d'impartialité. Pour être impartial, il faut que le juge ne soit soumis à personne d'autre, pouvoir public ou privé, si ce n'est la loi* ».

849. **Les acteurs garants de l'indépendance.** N'oublions pas que pour garantir ce « *socle* », l'article 64 de la constitution impose que le Président de la République, assisté par le Conseil supérieur de la magistrature, soient garants de l'indépendance de l'autorité judiciaire. En somme, le Président, l'un des deux titulaires actifs du pouvoir exécutif, sera le garant principal de l'indépendance des juges. Alors que le Conseil supérieur de la magistrature est le co-garant, assistant le Président dans cette mission. Ce conseil dispose aussi d'une instance disciplinaire, laquelle est saisie seulement par le ministre de la justice ou par les premiers présidents de Cour d'appel. Cette instance est présidée par le Premier Président de la Cour de Cassation. Dans sa mission de co-garant, le Conseil supérieur de la magistrature a élaboré en 2010 un Recueil des obligations déontologiques des magistrats de l'ordre judiciaire (actualisé en 2019), qui rend concrètes une série d'exigences comme l'intégrité, la légalité, mais aussi la dignité, l'écoute de l'autre, la discrétion, la réserve. Par son rôle progressivement renforcé, le Conseil supérieur de la magistrature apporte ainsi des garanties statutaires d'indépendance.

[1694] Charte des droits fondamentaux de l'Union européenne (2000/C 364/01), JOEU C 364/1 du 18 déc. *2000.*

850. **La récusation des juges.** Par ailleurs, des mécanismes de sanctions sont visés par le Code de procédure civile qui prévoit les causes de récusation des juges[1695]. La loi organise assez largement les cas de récusation et la procédure y afférente. Ils touchent essentiellement au conflit d'intérêts individuels ou familiaux. Les justiciables ont alors la possibilité de récuser le ou les juges dont l'impartialité leur paraît discutable. C'est le Haut conseil de la justice - indépendant dans sa composition et autonome dans son fonctionnement - qui connaît de la discipline des magistrats. Il n'a pas cependant de double degré de juridiction[1696].

851. **Consolidation de l'indépendance des juges par un dispositif déontologique préventif.** En France - estimant qu'il fallait encore davantage consolider l'indépendance de la justice considérée comme une garantie essentielle pour le justiciable - le Gouvernement a adopté en procédure accélérée la loi organique n°2016-1090 du 8 août 2016 relative aux garanties statutaires, aux obligations déontologiques et au recrutement des magistrats ainsi qu'au Conseil supérieur de la magistrature. Cette loi établit un cadre qui prévoit un dispositif déontologique préventif. Elle vise notamment à accroître les droits et obligations des magistrats par le renfort de leur transparence en prévenant les conflits d'intérêts, définis comme *« toute situation d'interférence entre un intérêt public et des intérêts publics ou privés qui est de nature à influencer ou à paraître influencer l'exercice indépendant, impartial et objectif d'une fonction »*, instaurant une obligation de les prévenir ou d'y mettre fin, et établissant des déclarations d'intérêts et entretiens déontologiques. Le nombre de décisions au fond et de sanctions liées à la déontologie du juge rapporté au nombre de juges reste toutefois assez faible[1697].

852. **Approfondissement déontologique croisé entre les magistrats et les experts.** Dans ce contexte, la base textuelle complète et précise de la déontologie des juges suscite davantage la réflexion au sujet d'un approfondissement déontologique croisé entre les magistrats et les experts. Elle imposerait une indépendance globalisée de la justice, par le biais d'obligations incombant aux différents acteurs intervenants dans l'appréciation des preuves cryptographiques.

[1695] C. proc. civ., art. 341, et C. de l'organisation judiciaire, art. L. 111-6.
[1696] Discours de B. Louvel (premier président de la Cour de cassation), L'indépendance du juge dans son contexte judiciaire et social, sept. 2018, p.2.
[1697] En matière disciplinaire en 2017, 7 décisions ou avis ont été rendus, 2 en 2018 et 5 en 2019 (au 13 décembre 2019). De 2007 à 2019, 69 sanctions au total ont été adressées à des magistrats en fonctions (http://www.conseil-superieur-magistrature.fr/actualites/activite-disciplinaire-du-conseil-superieur-de-la-magistrature (consulté le 31/05/2020).

853. Il pourrait être opportun d'établir une disposition spécifique qui obligerait le magistrat à une indépendance vis-à-vis de l'expert. L'élargissement de ce champ de la responsabilité disciplinaire pour le juge en l'absence d'indépendance vis-à-vis de l'expert serait enclin à introduire une responsabilité du juge dans les contentieux techniques. La problématique centrale de cette responsabilité disciplinaire réside dans la preuve de la violation de cette obligation d'indépendance. La preuve du jugement qui manquerait d'indépendance par rapport à un avis rendu par un expert peut sembler difficile à apporter. Le jugement et l'avis expertal sont souvent inextricables et ne permettent pas de savoir ce qui relève d'une simple considération ou d'une totale influence. Démêler le subtil assemblage de l'avis d'un expert à la décision du juge pourrait se révéler efficace dans l'hypothèse de la seule reprise verbatim des conclusions de l'expert. Il serait un indicateur flagrant de la violation de l'obligation d'indépendance.

854. Enfin, cette réflexion devra nécessairement impliquer des mesures concrètes qui s'inscriront dans un cadre d'une dimension internationale[1698] ; en d'autres termes, des mesures impliquant des obligations déontologiques des magistrats uniformisées à l'échelle internationale.

B. Le renforcement textuel interdépendant et nécessaire quant aux obligations déontologiques de l'expert

855. **Le renforcement déontologique de l'expert, une condition de l'indépendance des juges**. Le renforcement normatif ténu de la déontologie des juges ne peut occulter celui des experts, qui constitue une condition de l'indépendance des juges[1699]. Ce renfort doit être notable et manifeste en ce que l'indépendance des experts est en effet toujours plus débattue[1700]. Certains professeurs ont pu dénoncer une dépendance technique grandissante du juge à l'expert[1701], par-dessus tout lorsque « […] *l'opacité technique du litige l'a obligé à s'en remettre*

[1698] Discours de B. Louvel (premier président de la Cour de cassation), L'indépendance du juge dans son contexte judiciaire et social, sept. 2018, p.3.
[1699] J.-P. Markus, « L'expert pris en défaut. Responsabilité vis- à- vis du décideur ou des parties », *in* K. Favro, M. Lobé Lobas, J.- P. Markus (ss. dir.), *L'expert dans tous ses états. À la recherche d'une déontologie de l'expert*, *op.cit.*, p.432.
[1700] Direction Générale de la Santé, M.-D. Furet, Rapport sur l'indépendance et la valorisation de l'expertise venant à l'appui des décisions en santé publique, juin 2008, p.20.
[1701] J.- P. Marguénaud, « Le droit à l'expertise équitable », D. 2000, p.111-115.

en partie à un tiers »[1702]. Cette indépendance peut être aussi entachée en ce qui concerne le rattachement d'un expert à un milieu professionnel, lié directement ou indirectement aux intérêts économiques de ce milieu pour le financement de ses recherches[1703]. Ce cas se retrouve assez facilement dans les industries pharmaceutiques ou agro-alimentaires mais aussi dans le secteur des nouvelles technologies. Il pourrait donc l'être aussi dans le milieu de la *blockchain* qui voit une forme de dépendance technologique de plus en plus développée avec certains prestataires fournissant des solutions techniques. Parfois, c'est la dépendance économique de l'expert à l'expertise judiciaire qui l'incite à complaire aux tribunaux[1704], à l'instar de publications sur des sujets scientifiques très pointus dans le but d'obtenir plus de missions[1705]. Plus généralement, le risque de déviance de l'expert est présent lorsque ce dernier est conduit à faire un usage stratégique de ses ressources intellectuelles, modulant l'emploi d'un outil pour en tirer avantage, pour satisfaire son commanditaire ou même honorer ses pairs[1706]. L'absence d'indépendance de l'expert peut le conduire en ce sens à émettre un avis partial[1707]. L'avis d'un expert non indépendant sera ainsi biaisé ou au pire erroné.

856. **Les textes généraux sur l'indépendance des experts.** Certains textes d'exigence générale imposent l'indépendance de l'expert, comme la Charte nationale de l'expertise publiée le 2 mars 2010 qui introduit en préambule que *« la qualité d'une expertise s'apprécie essentiellement au regard de la compétence et de l'indépendance de ceux qui la conduisent, de la traçabilité des sources utilisées, de la transparence des méthodes mises en œuvre et de la clarté des conclusions* ». La portée de cette charte est toutefois réduite puisque les chartes ne sont pas obligatoires et n'ont pas de force contraignante, elles relèvent du droit mou.

857. Par ailleurs, les articles 237 du Code de procédure civile et R. 621- 3 du Code de justice administrative indiquent que l'expert doit accomplir sa mission avec conscience, objectivité et impartialité. Le défaut d'indépendance empêche l'expert d'exercer sa mission selon les exigences mentionnées mais l'indépendance n'est pas incluse de façon explicite dans ce texte.

[1702] J. Moury, « Les limites de la quête en matière de preuve : expertise et *jurisdictio* », *op.cit*., p.670, n°9.
[1703] *Ibid*.,p.670, n°9.
[1704] C. Byk, « Justice et expertise scientifique : un dialogue organisé dont il faut renouveler les fondements », RRJ 2013, p.29.
[1705] B. Ludes, « La situation de conflit d'intérêts intra-personnelle », Experts, déc. 2012, p.15, n°105.
[1706] J. Boirot, « Expertise juridique et expertise scientifique : L'interactivité juges/experts, source d'indépendance, *in* K. Favro, M. Lobé Lobas, J.- P. Markus (ss. dir.), *L'expert dans tous ses états. À la recherche d'une déontologie de l'expert, op.cit.*, p.136.
[1707] J.-P. Markus, « L'expert pris en défaut. Responsabilité vis-à-vis du décideur ou des parties », *op.cit.*, p.432.

858. Ce sont essentiellement les conditions à satisfaire pour être inscrit sur la liste des experts visées par le décret n°2004-1463 du 23 décembre 2004 relatif aux experts judiciaires qui mentionnent cette obligation d'indépendance[1708]. Selon les articles 2, 6°, 3, et 3° de ce décret, pour l'inscription d'une personne physique ou morale sur une liste d'experts, elle doit n'exercer aucune activité incompatible avec l'indépendance nécessaire à l'exercice de missions judiciaires d'expertise. Cette condition donne lieu à un contentieux fourni dans diverses fonctions. Il est exceptionnel que l'exercice d'une fonction soit jugé incompatible avec l'exigence d'indépendance[1709]. Par ailleurs, si l'inscription sur les listes est rejetée sur le fondement du manque d'indépendance de la personne physique ou morale, il convient de préciser en quoi celui-ci consiste[1710]. Le refus d'une inscription par des conclusions d'une enquête de moralité doit tout de même être motivé et préciser en quoi les conclusions de cette enquête sont défavorables[1711].

859. **Les textes spéciaux sur l'indépendance des experts.** D'autres textes spéciaux imposent cette indépendance, comme la loi n°2013-316 du 16 avril 2013 relative à l'indépendance de l'expertise en matière de santé et d'environnement et à la protection des lanceurs d'alerte, l'article L. 271-6 du Code de la construction relatif à celui chargé d'effectuer un diagnostic immobilier, ou encore l'article L. 326- 6 du Code de la route concernant la profession d'expert. Alors que les besoins d'indépendance s'accroissent, cette obligation *manque à l'appel en matière de* nouvelles technologies.

860. L'existence d'un ensemble complet de normes relatives à l'indépendance des experts doit être largement approfondi de façon individuelle et de façon croisée avec les magistrats pour un alignement des obligations. Si pour la docteure Jennifer Boirot, le rapport expert/juge serait déjà en lui-même une source d'indépendance, grâce à l'intervention réglementée de l'expert qui obligerait autant qu'elle garantirait son indépendance, cette idée ne semble pas convaincante et doit être largement mise en perspective dans l'environnement des preuves *blockchains*[1712].

[1708] Décret n°2004-1463, 23 déc. 2004 relatif aux experts judiciaires.
[1709] Incompatibilité admise au sujet des fonctions de juges consulaires d'un Tribunal de commerce du ressort de la même Cour d'appel, bien qu'il formât une demande dans la branche agricole (ne relevant pas du contentieux commercial) : Cass. 2ème civ., 2 sept. 2014, n°14- 60.154, Bull. civ. II, n°175.
[1710] Cass. 2ème civ.,, 19 sept. 2013, n°13-60.100.
[1711] Cass. 2ème civ.,, 22 sept. 2014, n°14-60.168 : Bull. civ. II, n°194 ; Cass. 2ème civ., 9 juill. 2015, n°15-60.142 ; Cass. 2ème civ., 9 juill. 2015, n°15-60.106.
[1712] J. Boirot, « Expertise juridique et expertise scientifique : L'interactivité juges/ experts, source d'indépendance, *in* K. Favro, M. Lobé Lobas, J.- P. Markus (ss. dir.), *L'expert dans tous ses états. À la recherche d'une déontologie de l'expert, op.cit.*, p.123-139.

861. **La proposition d'un règlement général de déontologie de l'expert.** Dans le but d'offrir plus de clarté et de lisibilité des sources normatives, des principes généraux du bon expert ou un règlement général de déontologie faisant figurer l'indépendance renforceraient l'ensemble des textes applicables à l'expert[1713]. Pour l'heure, l'incomplétude de ce principe fait peser sur les justiciables un risque de subir les affres de leur dépendance. L'indépendance devra donc être absolue, applicable en toute circonstance, et non pas envisagée limitativement. Ce serait une indépendance *erga omnes* tant intellectuelle, que matérielle, économique, et sociale.

862. Jean-Raymond Lemaire et Jean-Paul Markus ont quant à eux proposé un Code de déontologie de l'expert judiciaire européen[1714] donnant une vision plus européenne à l'obligation d'indépendance.

863. Par ailleurs, Jean-Maurice Beaufrere, président du Tribunal de Grande Instance de Fort de France a avancé que les obligations d'indépendance exigées du juge sont largement transposables à l'expert[1715]. Cette suggestion nous apparaît inopportune car elle ne semble pas satisfaire notre ambition de séparation stricte entre les deux professions.

864. **Une déclaration d'indépendance requise.** Perçue comme un trait « *congénital* » de l'expertise[1716], l'indépendance doit nécessairement être renforcée et systématisée par une déclaration formelle de l'expert. Outre la prestation de serment et le mandat par le juge, la mission de l'expert serait accompagnée d'une déclaration d'intérêts et d'indépendance systématique et générale lui permettant d'être tangible[1717]. Plus encore, ces déclarations comprendraient des éléments d'information que l'expert estime devoir porter à la connaissance de toutes les parties engagées dans le dispositif expertal.

865. **Des sanctions disciplinaires renforcées.** La sanction de l'absence d'indépendance d'un expert judiciaire est sa récusation[1718], laquelle dispose d'un régime bien bordé par les articles

[1713] Pour des principes généraux voir : C. Lienhard, « Les principes généraux du comportement du "bon expert" », *op.cit.*, p.78.
[1714] J.- R. Lemaire, J.-P. Markus, « L'européanisation de l'expertise », *in* K. Favro, M. Lobé Lobas, J.- P. Markus (ss. dir.), *L'expert dans tous ses états.* À *la recherche d'une déontologie de l'expert*, *op.cit*., p.247.
[1715] J.-M. Beaufrere, « Faut-il demander à l'expert une "déclaration d'indépendance" », 2007, https://www.courdecassation.fr/IMG/File/pdf_2007/conf_de_consensus/bibliographie/consensus_beaufrere_declaration_independance.pdf (consulté le 31/05/2020)
[1716] H. Motulsky, « Notions générales », *in L'expertise dans les principaux systèmes juridiques d'Europe*, Travaux de recherche de l'Institut de droit comparé de Paris, XXXII, Paris, éd. De l'épargne, 1969, p.18.
[1717] Voir en ce sens la proposition de déclaration d'intérêt : allocution de j.-c. Marin, cour de cassation, colloque « l'expertise : entre neutralité et partis-pris », 16 mars 2018.
[1718] J.-P. Markus, « L'expert pris en défaut. Responsabilité vis-à-vis du décideur ou des parties », *op.cit.*, p.433-434.

234 du Code de procédure civile, R621-6 du Code de la justice administrative et par la jurisprudence[1719]. La suspension provisoire de l'inscription sur la liste des experts pourra également être décidée, si l'urgence le justifie, par le premier président de la Cour d'appel ou de la Cour de cassation, à la demande du procureur général, lorsque l'expert fait l'objet de poursuites pénales ou disciplinaires[1720]. Une sanction disciplinaire peut en outre s'ajouter, avec une radiation de la liste des experts[1721]. La radiation joue lorsque l'expert est coupable d'un grave manquement déontologique dans l'exercice de sa profession[1722], mais également pour des faits commis en dehors de toute mission expertale, comme certaines infractions pénales[1723]. Les contours jurisprudentiels de cette sanction disciplinaire sont à nos yeux largement insatisfaisants. Le manquement grave à l'indépendance mériterait davantage de précisions. Les incertitudes qui entourent cette sanction disciplinaire au motif de la dépendance entravent son efficacité. Nous songeons parallèlement qu'un assouplissement des conditions requises pour statuer sur la radiation soit à même de renforcer la vigilance quant à l'indépendance de l'expert. Après l'intervention de l'expert, il sera toujours possible de procéder à une demande de nullité de l'expertise si les causes de dépendance de l'expert n'ont pu être décelées qu'*a posteriori*[1724].

Paragraphe 2 : Une proposition d'approche différente dans la pratique professionnelle des juges

866. Accéder à l'effectivité de l'indépendance du juge nécessite de dépasser les seuls textes, et de travailler l'idée de position professionnelle (A) afin de la mettre en place pour les données enregistrées dans la *blockchain* (B).

[1719] CE, avis cont., 23 mars 2012, Centre hospitalier d'Alès-Cévennes, n°355151, publié au Lebon, à propos de la motivation réduite de la décision rendue sur demande de récusation, aux fins de protection de la vie privée de l'expert.
[1720] Décret n°2004-1463 du 23 déc. 2004, art. 31.
[1721] CE, 22 mars 2010, Francis A., req. n°327251.
[1722] Cass. 1ère civ., 3 juin 2010, n°09-14.896, Bull. civ. I, n°126 : médecin, expert, qui délivrait des certificats de complaisance.
[1723] J. Pradel, « La responsabilité pénale de l'expert judiciaire », RSC, 1986.
[1724] N. Contis, J. Gayrard, « Invoquer la nullité d'un rapport d'expertise judiciaire », JCP n°5, févr. 2016, p.250-251.

A. L'idée de position professionnelle pour l'indépendance du juge

867. **L'importance de la position professionnelle.** Une étude de la Commission de Venise de mars 2010 confirme que dans de nombreux pays, les meilleures règles institutionnelles ne peuvent rien sans la bonne volonté des magistrats en charge de les mettre en œuvre[1725]. La lettre des textes relatifs à l'indépendance du juge résiste en effet à leur mise en contexte. Un écart persiste entre les textes encadrant et garantissant l'indépendance des juges, et le réalisme issu de l'exercice de leurs fonctions[1726]. Outre les règles, d'autres facteurs comme la personnalité et le professionnalisme entrent en considération dans l'approche de l'indépendance. Le droit ne suffit pas en déontologie, il doit aussi mêler les aspects comportementaux pour totalement enrayer la dépendance vis-à-vis des experts et tendre à la morale et l'acceptabilité attendues par les justiciables.

B. La mise en œuvre d'une position professionnelle pour les données enregistrées dans la *blockchain*

868. **Source de la position professionnelle.** Le juge doit être porteur d'une position par rapport au litige mettant en cause soit des éléments de preuves *blockchains*, soit un litige lié à cette technologie. Autrement dit, cette position serait une position professionnelle inhérente à la confrontation de son expertise forgée grâce à d'autres affaires. Elle mettrait aussi à contribution le savoir-faire et le savoir-être enseignés, cultivés, et approfondis lors de la carrière du magistrat[1727].

869. **Mise en pratique de la position professionnelle.** Il conviendra alors que les juges, lorsque des données sont enregistrées dans la *blockchain*, s'attachent à rendre transparentes les interventions et les motivations qui fondent leurs décisions. L'expertise devra rester un outil pour la formulation et la justification d'une solution[1728], mais certainement pas être la source

[1725] Commission de Venise, Étude n°494/2008, Rapport sur l'indépendance du système judiciaire partie I : l'indépendance des juges, Adopté par la Commission de Venise lors de sa 82ème session plénière, 12-13 mars 2010, p.4, n°10.
[1726] A. Girardet, « La réalité de l'indépendance judiciaire », *op.cit*, p.1-6.
[1727] Conseil Supérieur de la Magistrature, « Déontologie des magistrats. L'indépendance », juin 2010, http://www.conseil-superieur-magistrature.fr/publications/recueil-des-obligations-deontologiques/lindependance (consulté le 31/05/2020).
[1728] L. Dumoulin, « L'expertise judiciaire dans la construction du jugement : de la ressource à la contrainte », *op.cit*., p.211.

exclusive dans la construction d'un jugement. En effet, l'homologation aveugle du rapport d'expertise et les reprises intégrales verbatim des conclusions dans le rapport de l'expert, retranscrites dans les attendus des jugements, seront à bannir. Le risque serait que des faits non retenus ou non jugés pertinents par l'expert soient écartés et oubliés du juge. Pour éviter cette « *ratification* » pure et simple d'une solution, les juges sont invités à évaluer, interroger, discuter les raisonnements du rapport d'expertise. Pour permettre aux juges de s'émanciper de l'avis expertal, il pourra leur être imposé de motiver leur décision par un faisceau d'indices autre que le rapport de l'expert, prouvant par exemple qu'une preuve *blockchain* est fiable. Ces mesures viseront à lutter contre le phénomène de « *démission* » des juges[1729], par lequel ces derniers abandonnent totalement leurs pouvoirs aux auxiliaires.

870. Dans un objectif de bonne justice face à un contentieux complexe, les juges devront également s'attacher à la perception par les parties de leur indépendance. Le but d'instaurer une confiance solide des justiciables en nos institutions judiciaires sur les contentieux techniques impliquant des preuves *blockchains* est au cœur de cette réflexion.

871. **Support de la position professionnelle.** L'ensemble de ces bonnes pratiques qui pourrait être formulé par la chancellerie dans une circulaire ou au sein d'une politique d'action publique plus générale de la chancellerie serait une garantie d'une meilleure administration du service public de la justice dans ce type de contentieux.

872. **Conclusion du chapitre 2.** En conclusion de ce deuxième chapitre, la mise en évidence du déséquilibre systémique entre les juges et les auxiliaires dans l'adhésion généralisée des conclusions du rapport d'expertise alarme et met en exergue des risques à venir possibles concernant le rapport d'expertise des preuves *blockchains* complexes. Même si la vérité cryptographique complète la vérité juridictionnelle, créant un pont entre elles, les caractéristiques d'absolue, de juste, et d'objective accordées à la vérité cryptographique ne sont pas inflexibles. Cette vérité cryptographique se révélerait aussi relative, évolutive et empreinte de doutes mathématiques. Des solutions dans le renforcement de l'indépendance du juge croisée avec celle de l'expert seraient pertinentes.

873. Alors que les textes encadrant l'indépendance du juge ne nécessitent pas d'être approfondis, de bonnes pratiques pourraient être formulées par la chancellerie (circulaire ou

[1729] *Ibid.*, p.203.

politique d'action publique) imposant expressément aux juges de motiver leurs décisions par un faisceau d'indices autre que le rapport d'expertise sur les preuves *blockchains*.

874. En outre, ce sont les textes relatifs à l'indépendance de l'expert - disparates et manquant de lisibilité - qui nécessiteraient d'emprunter la voie d'un règlement général de déontologie de l'expert accompagné d'une déclaration d'indépendance et d'intérêt. Pour être efficaces, ces propositions seraient accompagnées d'une mesure dissuasive au manque d'indépendance : le renforcement de la sanction disciplinaire de radiation. Ce renfort serait le résultat de précisions du critère du manquement déontologique grave à sa profession entrainant la radiation étendu à certains faits commis en dehors de toute mission expertale[1730]. Un assouplissement de ce critère serait par ailleurs à même d'inciter l'expert à renforcer sa vigilance quant à son indépendance.

875. **Conclusion du titre 2.** En résumé du deuxième titre, la collecte, la constatation, la compréhension et plus largement la démystification des preuves *blockchains*, sont autant d'aides apportées - ou qui pourraient l'être - au juge par les auxiliaires, jusqu'à la supplantation même dans ses fonctions. Tantôt, l'huissier, par son constat des preuves *blockchains*, est déjà mobilisé par les acteurs économiques et ne sera pas indispensable mais constituera une aide utile à l'amorce de la démocratisation de ces nouvelles preuves, tantôt, l'intervention prochaine des experts dans les phases du procès se révèlera essentielle mais longue et coûteuse.

876. Pour autant, ces derniers interviennent à notre sens de façon démesurée dans la reconnaissance des preuves de données enregistrées dans la *blockchain*. La précaution sera de mise afin que le juge conserve toute son indépendance au regard de ces interventions.

877. Des propositions sont trouvées dans le renforcement de l'indépendance du juge, corrélée à celle de l'expert, par de bonnes pratiques de la chancellerie lui imposant de motiver expressément sa décision par un faisceau d'indices sur les preuves *blockchains*, autre que le rapport d'expertise.

878. Quant à l'indépendance seule de l'expert, les textes mériteraient plus d'intelligibilité par la mise en place d'un règlement général de déontologie de l'expert accompagné d'une déclaration d'indépendance et d'intérêt. En parallèle de cette voie à emprunter, viendrait en renfort la sanction précisée de radiation de l'expert.

[1730] J. Pradel, « La responsabilité pénale de l'expert judiciaire », RSC, 1986.

CONCLUSION DE LA PARTIE 2

879. Pour conclure cette deuxième partie, l'appréhension et ainsi la réception juridictionnelle de la vérité cryptographique est manifestement insuffisante. Elle voit s'affronter deux courants qui s'opposent : une intervention juridictionnelle avec prudence et une intervention extra-juridictionnelle trop importante. Ainsi, cette appréhension de la vérité cryptographique issue des preuves de données enregistrées dans la *blockchain* par le juge français est à la fois timide, et par procuration. Cette timidité du juge et substitution aux auxiliaires de justice traduit son inconfort général dans la difficile appropriation du code, des algorithmes, de la cryptographie immanents de ces nouvelles preuves techniques.

880. Les résultats d'une approche prophylactique seraient de nature à remédier à ce constat tout d'abord dans le renforcement de l'intervention juridictionnelle et dans l'endiguement de celle extra-juridictionnelle.

881. **Mesures pour le renfort de l'intervention juridictionnelle.** Tout d'abord, pour la recherche en matière pénale des preuves liées à la *blockchain*, seraient mis en place des moyens d'investigation renforcés élargissant leur champ matériel technique - compatibles avec de nombreux crypto-actifs -, et le champ des services à destination desquels ils sont mis à disposition : agents et officiers de police judiciaire, TRACFIN, et cyberdouanes. Le CMII serait désigné comme l'acteur pivot pour établir ces moyens à l'échelle internationale.

882. Ensuite, pour les mesures générales du renforcement de l'office des juges, des moyens visant à prévenir et outiller les juges seraient de nature à accorder une meilleure appréhension des preuves *blockchains* et asseoir leur légitimité. Il s'agirait d'un côté, de renforcer les formations des juges par un socle de connaissances et compétences et de l'autre côté, d'établir une infrastructure adéquate : un tribunal numérique pilote pour le contentieux civil hautement spécialisé sur des technologies avancées.

883. **Mesures pour l'endiguement de l'intervention extra-juridictionnelle.** Des mesures permettant de procéder à la canalisation des auxiliaires seront nécessaires pour encadrer leur intervention dans les preuves *blockchains*. Les auxiliaires doivent en effet se cantonner à leur

rôle d'aide en apportant leur concours au juge dans la reconnaissance de ces preuves mais pas les reconnaître d'eux-mêmes.

884. Dans ce contexte, pour assurer l'indépendance du juge, de bonnes pratiques seraient formulées par la chancellerie imposant au juge de motiver expressément sa décision par un faisceau d'indices sur les preuves *blockchains*, autre que le rapport d'expertise. Pour l'indépendance seule de l'expert, son régime mériterait plus d'intelligibilité par la mise en place d'un règlement général de déontologie de l'expert, d'une déclaration d'indépendance et d'intérêt et d'un renfort de la sanction de radiation.

885. L'ensemble de ces mesures participera à une meilleure appréhension de la vérité cryptographique issue des preuves *blockchains*. Bien que la vérité cryptographique apporte un complément à la vérité juridictionnelle, le truisme de l'absolue, de la juste, et de l'objective vérité cryptographique n'est pas inébranlable. Elle invite donc à nuancer cette idée manichéenne que l'on se fait d'elle : elle serait aussi relative, évolutive et empreinte de doutes mathématiques.

886. À cette étape du développement des preuves *blockchains,* démontrer par la preuve cryptographique sera moins le fait de dire une vérité cryptographique pour le plaideur, qu'un effort à déployer pour convaincre le juge[1731]. Mais cette vérité cryptographique remet en perspective la confiance que l'on accorde aux mathématiques et à la cryptographie : l'intime conviction du juge sera amenée à se fondre dans cette certitude matérielle.

[1731] Voir en ce sens de façon général : X. Lagarde, « Vérité et légitimité dans le droit de la preuve », Droits, 1993, p.31 et s., n°23 ; P. Théry, « Les finalités du droit de la preuve en droit privé », *op.cit.*, p. 41 et s., n°23 ; M. Mekki, « Vérité et preuve. Rapport français », *op.cit.*, p.827, n°23.

CONCLUSION DE LA THESE

887. **État des lieux du droit de la preuve à l'aune de la *blockchain*.** En conclusion de la présente étude, les preuves *blockchains*, nouvelles preuves cryptographiques distribuées, apparaissent comme des blandices du paysage probatoire[1732]. Reprenant des procédés traditionnels dans une architecture informatique originale, les signatures *blockchains*, horodatages *blockchains*, et empreintes *blockchains* émergent progressivement. De ces procédés résultent un ensemble de données dans un registre distribué (soit transactionnelles, soit complémentairement ajoutées) formant la grande catégorie des données enregistrées. Ces preuves peu orthodoxes apportent un souffle d'air nouveau qui pourrait être en proie à bouleverser le droit français et international de la preuve. Ces preuves *blockchains* ne constituent pas un simple ersatz de preuve numérique en plus évolué. Elles ne supplantent pas non plus les modes de preuve existants, elles les complètent par leurs propriétés en les enrichissant. Plus encore, elles font naître un nouveau modèle probatoire décentralisé, rationalisé et particulièrement sécurisé.

888. Nous avons pu démontrer tout au long de cette étude que les preuves de données enregistrées dans la *blockchain* et le droit de la preuve ne sont pas inconciliables. Ces preuves peuvent être objet de droits et le droit pourra se construire avec elles sur des certitudes scientifiques (les sciences informatiques) ; les règles dont elles font l'objet seront sujettes à interprétation par les juridictions ; elles forment enfin un outil opérationnel au service du droit. En revanche, si elles peuvent être suffisamment appréhendées par le droit, elles le sont encore difficilement par nos juridictions traditionnelles.

889. **Projections juridiques pour les preuves *blockchains*.** Par leur correspondance au droit commun, ces preuves peuvent être suffisamment appréhendées permettant leur qualification en vertu des règles du Code civil, du règlement eIDAS, et de la loi type de la CNUDCI sur les

[1732] Voir l'apport de la réforme du droit des contrats en droit de la preuve : E. Vergès, « Droit de la preuve : une réforme en trompe-l'œil », *op.cit.*, p.837-840 ; G. Lardeux, « Commentaire du titre IV bis nouveau du livre III du code civil intitulé "De la preuve des obligations" ou l'art de ne pas réformer », D. n°15, avr. 2016, p.850-856.

documents transférables électroniques. La proposition d'un avis adopté par le Parlement européen est toutefois formulée pour clarifier l'assimilation de la signature et de l'horodatage *blockchain* à la signature et l'horodatage électronique simple conçu par le règlement eIDAS. Il s'agirait aussi dans cet avis de soutenir la fiabilité de l'horodatage pour permettre aux États membres de consacrer une présomption de fiabilité de l'horodatage blockchain. Cette proposition se traduit en ces termes :

Avis sur l'application du règlement électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur à la technologie des registres distribués

Le Parlement européen,

– vu le règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (règlement (UE) 910/2014),

– vu la résolution du 3 octobre 2018 sur les technologies des registres distribués et les chaînes de blocs : renforcer la confiance par la désintermédiation,

– vu la résolution du 26 mai 2016 sur les monnaies virtuelles,

– vu la résolution du 28 avril 2017 sur la technologie financière : influence de la technologie sur l'avenir du secteur financier,

– vu les initiatives de la Commission concernant l'étude des TRD, notamment le projet « Blockchain4EU : Blockchain for Industrial Transformations », l'observatoire et forum européen des chaînes de blocs, le prix « blockchains for Social Good » et l'étude sur la faisabilité d'une infrastructure européenne des chaînes de blocs et les possibilités qu'elle offre,

Considérant ce qui suit :

A. considérant que la technologie des registres distribués est une technologie à usage général susceptible d'améliorer le rapport coût-efficacité des opérations en réduisant l'intervention de certains intermédiaires et les coûts d'intermédiation, ainsi que d'accroître la transparence des opérations, de remodeler les chaînes de valeur et d'améliorer l'efficacité organisationnelle grâce à une décentralisation fiable ;

B. considérant que les procédés d'horodatage et de signature par la technologie des registres distribués contribuent à améliorer la rapidité, le coût et la sécurité des institutions, acteurs économiques, usagers et consommateurs dans les principaux secteurs de l'économie et les services publics qui usent de ces procédés ;

C. considérant que les procédés d'horodatage et de signature par la technologie des registres distribués nécessitent un cadre qui assure une sécurité juridique, propice à l'innovation, favorable et incitatif, et respecte le principe de neutralité technologique au sein des États membres ;

D. considérant qu'aux procédés d'horodatage et de signature par la technologie des registres distribués s'appliquent le règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (règlement eIDAS) qui vise déjà à établir un cadre d'interopérabilité pour les différents systèmes mis en place au sein des États membres afin de promouvoir le développement d'un marché de la confiance numérique ;

Est d'avis dans ce contexte :

- *D'accorder à la signature par la technologie des registres distribués la valeur de la signature électronique visée à l'article 3.10 et les effets de l'article du 25 règlement eIDAS ;*
- *D'accorder à l'horodatage par la technologie des registres distribués la valeur de l'horodatage visé à l'article 3.33 et les effets de l'article 41 du règlement eIDAS ;*
- *De soutenir le renforcement de l'horodatage par la technologie des registres distribués concernant la fiabilité de la date et heure des blocs de transactions et d'intégrité de ces données, laissant aux États membres la marge de manœuvre pour aménager et préciser les modalités d'une présomption.*

890. Des régimes spéciaux novateurs concernant les domaines circonscrits des minibons et des titres financiers non cotés sont consacrés et constituent une véritable première étape symbolique dans la reconnaissance des preuves *blockchains*. Ils ne sont toutefois que partiels ; un régime général des preuves *blockchains* mérite que l'on s'y attèle. C'est un canevas de règles qui est proposé. Elles se traduisent par la formulation d'une loi type de la CNUDCI relative à la *blockchain* de la façon suivante :

Article 1. Champ d'application

1. *La présente Loi s'applique aux registres distribués.*
2. *La présente Loi ne se substitue à aucune règle de droit visant à protéger le consommateur.*

Article 2. Valeur juridique des données enregistrées dans un registre distribué

1. *La signature par la technologie de registres distribués est considérée comme une signature électronique.*
2. *L'horodatage par la technologie de registres distribués est considéré comme un horodatage électronique.*
3. *Le registre de la technologie de registres distribués est considéré comme un registre électronique.*

Article 3. Non-discrimination des données enregistrées dans un registre distribué

Une signature, un horodatage ou toute autre donnée inscrite et enregistrée dans un registre distribué ne peut se voir refuser sa validé et ses effets au seul motif que le registre est électronique et distribué.

Article 4. Satisfaction de l'exigence de fiabilité et sécurité du registre distribué

Peu importe la nature du registre distribué mis en œuvre, lorsque la loi soumet la possibilité d'utiliser un registre distribué pour inscrire des données, il doit être fait usage d'un registre distribué dont la fiabilité et la sécurité sont suffisantes.

Article 4. Éthique dans la technologie de registres distribués

Les acteurs et fournisseurs de services liés à la technologie de registres distribués s'engagent au respect des droits fondamentaux et des lois visant à lutter contre le blanchiment ou le financement du terrorisme dans la conception et la mise en œuvre des registres distribués.

Article 5. Égalité des traitements dans la technologie de registres distribués

Aucune disposition de la présente loi n'est appliquée de manière à exclure, restreindre ou priver d'effets juridiques l'usage d'un registre distribué quelle que soit la nature du registre distribué employé dès l'instant où il satisfait aux exigences mentionnées ci-avant et aux exigences de la loi applicable.

891. Cette ossature de principes internationaux doit être transposée en droit interne par un cadre dual de *hard law* et de *soft law*, dans le but de permettre une certaine souplesse de mise en œuvre d'un régime des preuves *blockchains* en France. Les particularités d'une *Lex blockchain* à la française serait exprimées de cette façon :

Titre 1 : Certification de données inscrites dans un registre distribué

***Article 1** : Toutes données inscrites dans un registre distribué vaut certification de ces données.*

***Article 2** : Est présumée fiable, jusqu'à preuve du contraire, la certification de données dans un registre distribué de blockchain publique, à l'exclusion du nouveau registre qui a fait l'objet d'une bifurcation.*

***Article 3** : Est présumé identifié, jusqu'à preuve du contraire, l'inscriveur de données dans un registre distribué de blockchain privée ou publique permissionnée une fois le seuil fixé par décret en Conseil d'État atteint.*

***Article 4** : Si les données sont inscrites par leur empreinte dans un registre distribué, cette empreinte pourra bénéficier de la qualification de copie au sens de l'article 1379 du Code civil.*

***Article 5** : L'empreinte serait dite fiable au sens de l'article 1379 du Code civil dès l'instant où l'intégrité de l'ensemble des données serait vérifiée par un nouveau calcul de l'empreinte desdites données. L'intégrité des données ancrées serait acquise en l'absence de modifications des données ancrées à l'origine.*

***Article 6** : L'empreinte fiable a la même force probante que les données qu'elle représente.*

Titre 2 : Authentification de l'inscriveur des données dans un registre distribué

Article 7 *: L'inscriveur de données dans un registre distribué est authentifié.*

Article 8 *: La clé privée de l'inscriveur permet de réaliser une signature électronique au sens de l'article 3.10 du règlement (UE) n°910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.*

Article 9 *: Toute transaction signée par clé privée dans un registre distribué est présumée avoir été effectuée par le titulaire de ladite clé privée jusqu'à preuve du contraire.*

Article 10 *: Toute donnée inscrite dans un registre distribué par l'inscriveur manifeste son assentiment à certifier des données.*

Titre 3 : Datation des données enregistrées dans un registre distribué

Article 11 *: La date de validation des blocs de transactions du registre distribué est la seule opposable.*

Article 12 *: La date mentionnée à l'article 11 est présumée fiable et ses données intègres.*

Article 13 *: La date mentionnée à l'article 11 vaut date de l'existence desdites données datées dans le registre distribué.*

Article 14 *: La date d'existence des données dans le registre distribué de blockchain publique est présumée irréfragable.*

Titre 4 : Recours

Article 13 *: Le recours de dénégation de l'écrit s'applique à une partie qui dénie la certification dans le registre distribué dans les mêmes conditions que celles fixées à l'article 287 du Code de procédure civile.*

***Article 14** : Le recours de dénégation de signature s'applique à une partie qui dénie signature par la technologie des registres distribués dans les mêmes conditions que celles fixées à l'article 287 du Code de procédure civile.*

***Article 15** : Il appartient au juge de procéder à la vérification d'écriture et de signature des articles 13 et 14, conformément à l'article 288 du Code de procédure civile.*

***Article 15** : Le délit d'usurpation d'identité tel que visé à l'article 226-4-1 du Code pénal s'applique à toute personne qui emploie la clé publique et privée d'un tiers sans son autorisation et dans les mêmes conditions que l'article précité.*

892. Dans le même temps, des mesures de *soft law*, comme un label optionnel délivré par l'ANSSI, seront à même d'attester la conformité d'un produit ou service lié à la *blockchain* par rapport à un référentiel. Des guides de bonnes pratiques également publiés par l'ANSSI, comme par les développeurs et leurs propres référentiels (référentiel ERC pour Ethereum) seront enclins à accompagner les projets relatifs à la *blockchain* incluant ces preuves. L'ensemble de ces propositions pourra ainsi participer au cadre requis au soutien de la traduction de la vérité cryptographique issue des preuves *blockchains*.

893. La vérité cryptographique projetée par ces preuves *blockchains* distribuées correspondrait à la probabilité qu'un fait du monde réel ou natif des registres distribués soit vrai. Elle apparaît pour l'heure comme une vérité autonome qui se dissout toutefois dans la vérité juridictionnelle, laquelle est à la recherche d'autres réalités culturelles et sociétales. Si la vérité cryptographique sert la vérité juridictionnelle - essentiellement pénale -, elle conquiert progressivement le droit. Les fondements de leur relation restent cependant à bâtir, charge à la vérité juridique de l'accueillir et de lui laisser la place escomptée.

894. Cette vérité cryptographique est parallèlement difficilement appréhendée par les juridictions. Une adhésion lente et prudente des juridictions quant à ces preuves numériques distribuées résulte de cette appréhension complexe. Les propositions d'un renfort de l'intervention juridictionnelle jumelé à une canalisation des rôles des huissiers et des experts de justice dans la reconnaissance de ces preuves *blockchains* sont soutenues.

895. D'une part, est proposé le renfort de l'office du juge face aux preuves *blockchains* par des moyens visant à former les juges sur cette technologie et établir un tribunal numérique pilote pour le contentieux civil hautement spécialisé sur des technologies avancées.

Des moyens d'investigation renforcés seront, en outre, une aide à la recherche de preuves *blockchains* en matière pénale à destination des agents et officiers de police judiciaire, de TRACFIN et des cyberdouanes.

D'autre part, des propositions de canalisation des auxiliaires de justice, afin qu'ils se cantonnent à leur rôle d'aide apportant leur concours au juge dans la reconnaissance de ces preuves, sont suggérées comme suit sous la forme :

De bonnes pratiques formulées par la chancellerie (circulaire ou politique d'action publique) imposant expressément au juge de motiver sa décision par un faisceau d'indices sur les preuves *blockchains*, autre que le rapport d'expertise ; et

D'un règlement général de déontologie de l'expert, d'une déclaration d'indépendance et d'intérêt et d'un renfort de la sanction radiation de l'expert.

896. Cependant, cette recherche de vérité à tout prix avec cette nouvelle forme de vérité scientifique - asymptotique d'une vérité idéale - n'est-elle pas finalement vaine ? Elle est somme toute relative et limitée par l'évolution des connaissances scientifiques. Albert Camus rendait évidente cette idée esquissant les contours de la vérité comme « … *mystérieuse, fuyante toujours à conquérir* »[1733]. Mais la recherche de vérité nous rapproche quand même en fin de compte de l'universel ; des rapports universels gouvernant les sujets de droit dont la connaissance les rend meilleurs[1734].

897. **Perspectives de l'étude.** Proudhon, l'inspirateur des crypto-anarchistes, ne nie pas la nécessité du droit : dans son acceptation proudhonienne, l'anarchisme contient en effet un principe d'ordre[1735]. D'ailleurs, si l'anti-légalisme est selon lui une conséquence de l'antiétatisme, à partir de la critique de la loi, il élargit le champ des sources formelles du droit.

[1733] A. Camus, *Discours de Suède*, coll. Folio, Gallimard, 1997, p.20.
[1734] A. Legoux, « vérité médicale, vérité juridique », *op.cit.*, p.18.
[1735] Proudhou suggère une conception sociale du droit : c'est le droit étatique incarné par la loi qu'il rejette (A.-S. Chambost, proudhon et la norme, pensée juridique d'un anarchiste, thèse, Lyon 3, Pur, 2004, 295 p.).

898. Effleurant finalement l'histoire de la pensée juridique, les idées crypto-anarchistes et les preuves *blockchains* se conjuguent avec syncrétisme. Partiellement anomiques en France, les preuves *blockchains* doivent être garanties par les évolutions normatives mentionnées permettant à ces nouvelles preuves cryptographiques de bénéficier d'une force probante suffisante, les rendant pleinement efficaces. Elles doivent aussi être accompagnées d'une hardiesse des juridictions propre à nous surprendre. Ces perspectives devront se placer dans le sillon d'une politique favorable de la chancellerie, de l'OCDE, d'Interpol et des autres autorités et organisations impliquées sur ce sujet.

ANNEXES

Annexe n°1 : Amendement n°CF2 au projet de loi Sapin II n°3623

Annexe n°2 : Legge 11 febbraio 2019 n°12 (Italie)

Annexe n°3 : Proposition de loi n°237 du 4 décembre 2017 (Monaco)

Annexe n°4 : Projet de loi n°995 relative à la technologie *blockchain* du 20 mai 2019 (Monaco)

Annexe n°5 : Amendements n°434, 773 et 1309 au projet de loi PACTE n°1088

Annexe n°6 : Compte rendu n°18 des débats parlementaires de la commission spéciale chargée d'examiner le projet de loi PACTE du 13 septembre 2018 – séance de 15h

Annexe n°7 : Amendement n°1317 et au projet de loi PACTE n°1088

Annexe n°8 : Public Act 101-0514 - *Blockchain* Technology Act (Illinois, États-Unis)

Annexe n°9 : Circulaire n°2018/F/0090/FC1 de la Direction des affaires criminelles et des grâces du Ministère de la Justice, Dépêche relative au recensement des procédures d'escroqueries aux faux investissements dans les cryptoactifs du 18 octobre 2018

Annexe n°10 : Question écrite n°22103 de Daniel Fasquelle publiée au JO le 30 juillet 2019 et réponse du Ministère de la Justice publiée au JO le 10 décembre 2019

Annexe n°11 : Traduction anglaise du Cabinet Dennemeyer de la décision : Hangzhou Internet Court, Province of Zhejiang People's Republic of China, Case No. 055078 (2018) Zhe 0192 No. 81 Huatai Yimei/Daotong, June 27, 2018

Annexe n°12 : H. 868 (Act no. 157) relating to miscellaneous economic development (Vermont, États-Unis)

ANNEXE N°1

APRÈS ART. 27 **N° CF2**

ASSEMBLÉE NATIONALE

13 mai 2016

RELATIF À LA TRANSPARENCE, À LA LUTTE CONTRE LA CORRUPTION ET À LA MODERNISATION DE LA VIE ÉCONOMIQUE - (N° 3623)

Non soutenu

AMENDEMENT

N º CF2

présenté par
Mme de La Raudière

ARTICLE ADDITIONNEL

APRÈS L'ARTICLE 27, insérer l'article suivant:

Après le deuxième alinéa de l'article L. 330-1 du code monétaire et financier, il est inséré un alinéa ainsi rédigé :

« Les opérations effectuées au sein d'un système organisé selon un registre décentralisé permanent et infalsifiable de chaine de blocs de transactions constituent des actes authentiques au sens du deuxième alinéa de l'article 1317 du code civil. L'Autorité des marchés financiers habilite le système répondant aux conditions de sécurité et de transparence définies dans un décret pris en conseil d'État. »

EXPOSÉ SOMMAIRE

L'objet de cet amendement est considérer que les opérations de règlement livraison d'instruments financiers ou de devises dénouées dans un système de règlement au sens au sens de la directive 98/26/ CE du Parlement européen et du Conseil du 19 mai 1998 concernant le caractère définitif du règlement dans les systèmes de paiement et de règlement des opérations sur titres, et dont le fonctionnement utilise la technologie dite de la « blockchain » constituent des actes authentiques électroniques de la même manière que les actes passés devant notaires.

Ainsi, les transactions dénouées dans ces systèmes auront toutes les caractéristiques de l'acte authentique :

- Date certaine : l'acte authentique fait foi d'une date et celle-ci est incontestable. Elle peut donc servir de preuve ;

- Le contenu est garanti par le registre décentralisé : il garantit la validité du fond et de la forme de l'acte ;

- L'acte a force probante : l'acte authentique est un élément de preuve incontestable, il fait l'objet du plus haut niveau de preuve recevable en cas de litige ;

- L'acte a force exécutoire : la force exécutoire est de plein droit. De plus, elle est valable non seulement sur le territoire français mais également au sein de l'espace judiciaire européen. Cela signifie que l'acte a force exécutoire de plein droit, même ailleurs qu'en France.

Cet amendement vise à permettre à la France de prendre une avance juridique en ce qui concerne la reconnaissance des effets juridiques de l'utilisation de la « blockchain » dans les opérations sur instruments financiers et devises. A l'heure où un projet de fusion géante entre bourses notamment en Europe avec le projet de rapprochement de LSE et Deutsche Börse, risque de marginaliser la Place de Paris, celle-ci se doit d'innover en mettant en avant ses atouts, au risque sinon de disparaitre. Or, les activités de post-marchés financiers comme celles liées à la conservation des instruments financiers et à la circulation de ces instruments constituent encore l'un des domaines d'excellence de la Place de Paris qui représente environ 25 % de ces activités en Europe. Il est donc nécessaire de permettre à la Place de Paris de reconnaitre les effets juridiques de la technologie de la « blockchain » dans les opérations de règlement-livraison.

L'utilisation de cette technologie va considérablement réduire le besoin de fonds propres des établissements membres du système boursier de la Place de Paris, offrant un avantage compétitif indéniable par rapport aux autres places financières. En effet, l'instantanéité des opérations de règlement-livraison va réduire la partie du risque de contrepartie lié à la durée entre l'opération et son dénouement, et de fait, le besoin de fonds propres nécessaires pour garantir la bonne fin de ces opérations.

Plus largement, le recours à la technologie de la « blockchain » constitue un enjeu de souveraineté pour la France. Sa reconnaissance, d'abord limitée aux opérations de dénouement d'instruments financiers et de devises faisant suite aux transactions effectuées sur un marché réglementé, un système multilatéral de négociation ou de gré à gré, permettra à la France et à l'Europe de garder la maitrise de la circulation des titres et des devises.

Les conditions techniques de sécurité et de transparence du registre décentralisé seront fixées par un décret pris en Conseil d'État.

L'utilisation de la « blockchain » par un système de règlement livraison devra toutefois faire l'objet d'une habilitation par l'AMF qui vérifiera que l'exploitant du système dispose bien des ressources techniques, humaines, et financière lui permettant de gérer en toute sécurité et transparence les opérations transitant par son système de règlement livraison.

ANNEXE N°2

LEGGE 11 febbraio 2019, n. 12

Conversione in legge, con modificazioni, del decreto-legge 14 dicembre 2018, n. 135, recante disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione. (19G00017)

Vigente al: 19-5-2020

La Camera dei deputati ed il Senato della Repubblica hanno approvato;

IL PRESIDENTE DELLA REPUBBLICA

Promulga

la seguente legge:

Art. 1

1. Il decreto-legge 14 dicembre 2018, n. 135, recante disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione, e' convertito in legge con le modificazioni riportate in allegato alla presente legge.

2. Il decreto-legge 29 dicembre 2018, n. 143, e' abrogato. Restano validi gli atti e i provvedimenti adottati e sono fatti salvi gli effetti prodottisi ed i rapporti giuridici sorti sulla base del medesimo decreto-legge 29 dicembre 2018, n. 143.

3. Il decreto-legge 11 gennaio 2019, n. 2, e' abrogato. Restano validi gli atti e i provvedimenti adottati e sono fatti salvi gli effetti prodottisi ed i rapporti giuridici sorti sulla base del medesimo decreto-legge 11 gennaio 2019, n. 2.

4. La presente legge entra in vigore il giorno successivo a quello della sua pubblicazione nella Gazzetta Ufficiale.

La presente legge, munita del sigillo dello Stato, sara' inserita nella Raccolta ufficiale degli atti normativi della Repubblica italiana. E' fatto obbligo a chiunque spetti di osservarla e di farla osservare come legge dello Stato.

Data a Roma, addi' 11 febbraio 2019

MATTARELLA

Conte, Presidente del Consiglio dei ministri

Visto, il Guardasigilli: Bonafede

Allegato

MODIFICAZIONI APPORTATE IN SEDE
DI CONVERSIONE AL DECRETO-LEGGE
14 DICEMBRE 2018, N. 135

All'articolo 1, dopo il comma 8 sono aggiunti i seguenti:

«8-bis. All'articolo 1 della legge 30 dicembre 2018, n. 145, sono apportate le seguenti modificazioni:

a) al comma 34 sono aggiunte, in fine, le seguenti parole: "e di quelli di cui all'articolo 6 del decreto del Presidente della Repubblica 29 settembre 1973, n. 601";

b) il comma 52 e' sostituito dai seguenti:

"52. La disposizione di cui al comma 51 si applica a decorrere dal periodo d'imposta di prima applicazione del regime agevolativo di cui al comma 52-bis.

52-bis. Con successivi provvedimenti legislativi sono individuate misure di favore, compatibili con il diritto dell'Unione europea, nei confronti dei soggetti che svolgono con modalita' non commerciali attivita' che realizzano finalita' sociali nel rispetto dei principi di solidarieta' e sussidiarieta'. E' assicurato il necessario coordinamento con le disposizioni del codice del Terzo settore, di cui al decreto legislativo 3 luglio 2017, n. 117".

8-ter. Ai maggiori oneri di cui al comma 8-bis, pari a 118,4 milioni di euro per l'anno 2019 e a 157,9 milioni di euro a decorrere dall'anno 2020, si provvede: quanto a 98,4 milioni di euro per l'anno 2019, a 131 milioni di euro per l'anno 2020 e a 77,9 milioni di euro a decorrere dall'anno 2021, mediante corrispondente riduzione del Fondo per interventi strutturali di politica economica, di cui all'articolo 10, comma 5, del decreto-legge 29 novembre 2004, n. 282, convertito, con modificazioni, dalla legge 27 dicembre 2004, n. 307; quanto a 20 milioni di euro per l'anno 2019 e a 16,9 milioni di euro per l'anno 2020, mediante corrispondente riduzione del Fondo di cui all'articolo 1, comma 748, della legge 30 dicembre 2018, n. 145; quanto a 10 milioni di euro per l'anno 2020 e a 80 milioni di euro a decorrere dall'anno 2021, mediante corrispondente riduzione del Fondo di cui all'articolo 1, comma 200, della legge 23 dicembre 2014, n. 190».

Dopo l'articolo 1 e' inserito il seguente:

«Art. 1-bis (Semplificazione e riordino delle disposizioni relative a istituti agevolativi). - 1. Al decreto-legge 23 ottobre 2018, n. 119, convertito, con modificazioni, dalla legge 17 dicembre 2018, n. 136, sono apportate le seguenti modificazioni:

a) all'articolo 3, comma 23, le parole da: "non possono" fino a: "improcedibile" sono sostituite dalle seguenti: "possono essere definiti secondo le disposizioni del presente articolo versando le somme di cui al comma 1 in unica soluzione entro il 31 luglio 2019, ovvero, in deroga al comma 2, lettera b), nel numero massimo di dieci rate consecutive, ciascuna di pari importo, scadenti la prima il 31 luglio 2019, la seconda il 30 novembre 2019 e le restanti il 28 febbraio, il 31 maggio, il 31 luglio e il 30 novembre degli anni 2020 e 2021";

b) all'articolo 5, comma 1, lettera d), dopo le parole: "restanti rate" sono inserite le seguenti: "il 28 febbraio, il 31 maggio".

2. All'articolo 1 della legge 30 dicembre 2018, n. 145, il comma 193 e' sostituito dal seguente:

"193. Nei casi previsti dal secondo periodo del comma 192, l'agente della riscossione avverte il debitore che i debiti delle persone fisiche inseriti nella dichiarazione presentata ai sensi del comma 189, ove definibili ai sensi dell'articolo 3 del decreto-legge 23 ottobre 2018, n. 119, convertito, con modificazioni, dalla legge 17 dicembre 2018, n. 136, sono automaticamente inclusi nella definizione disciplinata dallo stesso articolo 3 e indica l'ammontare

complessivo delle somme dovute a tal fine, ripartito in diciassette rate, e la scadenza di ciascuna di esse. La prima di tali rate, di ammontare pari al 30 per cento delle predette somme, scade il 30 novembre 2019; il restante 70 per cento e' ripartito nelle rate successive, ciascuna di pari importo, scadenti il 28 febbraio, il 31 maggio, il 31 luglio e il 30 novembre di ciascun anno a decorrere dal 2020. Nei medesimi casi previsti dal secondo periodo del comma 192, limitatamente ai debiti di cui all'articolo 3, comma 23, del citato decreto-legge n. 119 del 2018, l'ammontare complessivo delle somme dovute e' ripartito in nove rate, di cui la prima, di ammontare pari al 30 per cento, scadente il 30 novembre 2019 e le restanti, ciascuna di pari importo, scadenti il 28 febbraio, il 31 maggio, il 31 luglio e il 30 novembre degli anni 2020 e 2021. Si applicano, a decorrere dal 1° dicembre 2019, gli interessi al tasso del 2 per cento annuo".

3. All'articolo 1, comma 57, lettera d-bis), della legge 23 dicembre 2014, n. 190, sono aggiunte, in fine, le seguenti parole: ", ad esclusione dei soggetti che iniziano una nuova attivita' dopo aver svolto il periodo di pratica obbligatoria ai fini dell'esercizio di arti o professioni"».

All'articolo 2, comma 1, dopo le parole: «dalla legge 21 giugno 2017, n. 96,» sono inserite le seguenti: «come integrato ai sensi dell'articolo 12 del decreto-legge 16 ottobre 2017, n. 148, convertito, con modificazioni, dalla legge 4 dicembre 2017, n. 172,».

All'articolo 3, dopo il comma 1 sono aggiunti i seguenti:

«1-bis. All'articolo 1 della legge 23 dicembre 1956, n. 1526, i commi sesto e settimo sono abrogati.

1-ter. All'articolo 1-bis del decreto-legge 24 giugno 2014, n. 91, convertito, con modificazioni, dalla legge 11 agosto 2014, n. 116, il comma 7 e' abrogato.

1-quater. All'articolo 60 della legge 12 dicembre 2016, n. 238, sono apportate le seguenti modificazioni:

a) al comma 1, le parole: "I produttori, gli importatori e i grossisti" sono sostituite dalle seguenti: "I produttori e gli importatori";

b) il comma 2 e' abrogato.

1-quinquies. All'articolo 2330, primo comma, del codice civile, le parole: "entro venti giorni" sono sostituite dalle seguenti: "entro dieci giorni". La disposizione di cui al presente comma ha effetto a decorrere dalla data di entrata in vigore della legge di conversione del presente decreto.

1-sexies. All'articolo 25 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, sono apportate le seguenti modificazioni:

a) il comma 14 e' abrogato;

b) al comma 15, dopo le parole: "entro sei mesi dalla chiusura di ciascun esercizio," sono inserite le seguenti: "fatta salva l'ipotesi del maggior termine nei limiti e alle condizioni previsti dal secondo comma dell'articolo 2364 del codice civile, nel qual caso l'adempimento e' effettuato entro sette mesi,";

c) dopo il comma 17 e' aggiunto il seguente:

"17-bis. La start-up innovativa e l'incubatore certificato inseriscono le informazioni di cui ai commi 12 e 13 nella piattaforma informatica startup.registroimprese.it in sede di iscrizione nella sezione speciale di cui al comma 8, aggiornandole o confermandole almeno una volta all'anno in corrispondenza dell'adempimento di cui al comma 15, anche ai fini di cui al comma 10".

1-septies. All'articolo 4 del decreto-legge 24 gennaio 2015, n. 3, convertito, con modificazioni, dalla legge 24 marzo 2015, n. 33,

sono apportate le seguenti modificazioni:

a) al comma 6, dopo le parole: "entro sei mesi dalla chiusura di ciascun esercizio," sono inserite le seguenti: "fatta salva l'ipotesi del maggior termine nei limiti e alle condizioni previsti dal secondo comma dell'articolo 2364 del codice civile, nel qual caso l'adempimento e' effettuato entro sette mesi,";

b) dopo il comma 6 e' inserito il seguente:

"6-bis. La PMI innovativa inserisce le informazioni di cui al comma 4 nella piattaforma informatica startup.registroimprese.it in sede di iscrizione nella sezione speciale di cui al comma 2, aggiornandole o confermandole almeno una volta all'anno in corrispondenza dell'adempimento di cui al comma 6, anche ai fini di cui al comma 2".

1-octies. All'articolo 2, comma 2, della legge 22 febbraio 2006, n. 84, la lettera a) e' sostituita dalla seguente:

"a) frequenza di corsi di qualificazione tecnico-professionale della durata di 250 ore complessive da svolgersi nell'arco di un anno".

1-novies. All'articolo 12 del regolamento di cui al decreto del Presidente della Repubblica 9 febbraio 2001, n. 187, il secondo periodo del comma 1 e' soppresso e i commi 3 e 5 sono abrogati.

1-decies. Il comma 6 dell'articolo 1-bis del decreto-legge 24 giugno 2014, n. 91, convertito, con modificazioni, dalla legge 11 agosto 2014, n. 116, nonche' i decreti del Ministro delle politiche agricole alimentari e forestali 17 dicembre 2013, pubblicato nella Gazzetta Ufficiale n. 36 del 13 febbraio 2014, e n. 10 dell'8 gennaio 2015, recante "Disposizioni relative alla dematerializzazione del registro di carico e scarico degli sfarinati e delle paste alimentari", sono abrogati.

1-undecies. I dati della denuncia aziendale di cui all'articolo 5, comma 1, lettere a), c) e d), del decreto legislativo 11 agosto 1993, n. 375, possono essere acquisiti d'ufficio dall'INPS, dal fascicolo aziendale di cui all'articolo 9 del regolamento di cui al decreto del Presidente della Repubblica 1° dicembre 1999, n. 503, istituito nell'ambito dell'anagrafe delle aziende agricole, gestito dal Sistema informativo agricolo nazionale (SIAN). Le imprese agricole indicano nella denuncia aziendale i dati di cui al presente comma nel caso in cui non abbiano costituito o aggiornato il fascicolo aziendale.

1-duodecies. All'articolo 2, comma 5-undecies, del decreto-legge 29 dicembre 2010, n. 225, convertito, con modificazioni, dalla legge 26 febbraio 2011, n. 10, dopo le parole: "con rappresentanza diretta nel CNEL" sono inserite le seguenti: "e quelle stipulanti il contratto collettivo nazionale di lavoro di riferimento nel settore".

1-terdecies. All'articolo 7 del decreto legislativo 9 ottobre 2002, n. 231, dopo il comma 4 e' inserito il seguente:

"4-bis. Nelle transazioni commerciali in cui il creditore sia una PMI, come definita ai sensi del decreto del Ministro delle attivita' produttive 18 aprile 2005, pubblicato nella Gazzetta Ufficiale n. 238 del 12 ottobre 2005, si presume che sia gravemente iniqua la clausola che prevede termini di pagamento superiori a sessanta giorni. Il presente comma non si applica quando tutte le parti del contratto sono PMI".

1-quaterdecies. All'articolo 6, comma 2, della legge 11 gennaio 2018, n. 8, le parole: "quattro mesi" sono sostituite dalle seguenti: "sei mesi"».

Dopo l'articolo 3 sono inseriti i seguenti:

«Art. 3-bis (Disposizioni in materia di etichettatura). - 1.

All'articolo 4 della legge 3 febbraio 2011, n. 4, sono apportate le seguenti modificazioni:

a) i commi 1 e 2 sono abrogati;

b) il comma 3 e' sostituito dai seguenti:

"3. Con decreto del Ministro delle politiche agricole alimentari, forestali e del turismo, di concerto con il Ministro dello sviluppo economico e il Ministro della salute, previa intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, sentite le organizzazioni maggiormente rappresentative a livello nazionale nei settori della produzione e della trasformazione agroalimentare e acquisiti i pareri delle competenti Commissioni parlamentari, previo espletamento della procedura di notifica di cui all'articolo 45 del regolamento (UE) n. 1169/2011 del Parlamento europeo e del Consiglio, del 25 ottobre 2011, sono definiti, per le finalita' di cui alle lettere b), c) e d) del paragrafo 1 dell'articolo 39 del medesimo regolamento, i casi in cui l'indicazione del luogo di provenienza e' obbligatoria. Sono fatte salve le prescrizioni previste dalla normativa europea relative agli obblighi di tracciabilita' e di etichettatura dei prodotti contenenti organismi geneticamente modificati o da essi costituiti.

3-bis. Con il decreto di cui al comma 3 sono individuate le categorie specifiche di alimenti per le quali e' stabilito l'obbligo dell'indicazione del luogo di provenienza. Ai sensi dell'articolo 39, paragrafo 2, del regolamento (UE) n. 1169/2011, il Ministero delle politiche agricole alimentari, forestali e del turismo, in collaborazione con l'Istituto di servizi per il mercato agricolo alimentare (ISMEA), assicura la realizzazione di appositi studi diretti a individuare la presenza di un nesso comprovato tra talune qualita' degli alimenti e la relativa provenienza nonche' a valutare in quale misura sia percepita come significativa l'indicazione relativa al luogo di provenienza e quando la sua omissione sia riconosciuta ingannevole. I risultati delle consultazioni effettuate e degli studi eseguiti sono resi pubblici e trasmessi alla Commissione europea congiuntamente alla notifica del decreto di cui al comma 3. All'attuazione delle disposizioni di cui al presente comma si provvede con le risorse umane, finanziarie e strumentali disponibili a legislazione vigente, senza nuovi o maggiori oneri per la finanza pubblica.

3-ter. L'indicazione del luogo di provenienza e' sempre obbligatoria, ai sensi dell'articolo 26, paragrafo 2, lettera a), del regolamento (UE) n. 1169/2011, quando sussistano le condizioni di cui all'articolo 1 del regolamento di esecuzione (UE) 2018/775 della Commissione, del 28 maggio 2018. La difformita' fra il Paese di origine o il luogo di provenienza reale dell'alimento e quello evocato dall'apposizione di informazioni di cui al predetto articolo 1 del regolamento (UE) 2018/775, anche qualora risultino ottemperate le disposizioni dell'articolo 26, paragrafo 3, del regolamento (UE) n. 1169/2011, si configura quale violazione di cui all'articolo 7 del medesimo regolamento (UE) n. 1169/2011, in materia di pratiche leali d'informazione";

c) i commi 4 e 4-bis sono abrogati;

d) ai commi 6 e 12, le parole: "dei decreti" sono sostituite dalle seguenti: "del decreto";

e) il comma 10 e' sostituito dal seguente:

"10. Per le violazioni delle disposizioni relative all'indicazione obbligatoria dell'origine e della provenienza previste dal presente articolo e dai decreti attuativi, si applicano le sanzioni previste dal decreto legislativo 15 dicembre 2017, n.

231";

f) al comma 11, le parole: "del primo dei decreti" sono sostituite dalle seguenti: "del decreto".

2. Le disposizioni del presente articolo entrano in vigore tre mesi dopo la data della notifica di cui al paragrafo 1 dell'articolo 45 del regolamento (UE) n. 1169/2011 del Parlamento europeo e del Consiglio, del 25 ottobre 2011, di cui e' data comunicazione con pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.

Art. 3-ter (Semplificazioni per le zone economiche speciali - ZES e per le zone logistiche semplificate - ZLS) - 1. All'articolo 5, comma 1, del decreto-legge 20 giugno 2017, n. 91, convertito, con modificazioni, dalla legge 3 agosto 2017, n. 123, la lettera a) e' sostituita dalle seguenti:

"a) l'attivita' economica nelle ZES e' libera, nel rispetto delle norme nazionali ed europee sull'esercizio dell'attivita' d'impresa. Al fine di semplificare ed accelerare l'insediamento, la realizzazione e lo svolgimento dell'attivita' economica nelle ZES sono disciplinati i seguenti criteri derogatori alla normativa vigente, procedure semplificate e regimi procedimentali speciali applicabili. Per la celere definizione dei procedimenti amministrativi, sono ridotti di un terzo i termini di cui: agli articoli 2 e 19 della legge 7 agosto 1990, n. 241; al decreto legislativo 3 aprile 2006, n. 152, in materia di valutazione d'impatto ambientale (VIA), valutazione ambientale strategica (VAS) e autorizzazione integrata ambientale (AIA); al regolamento di cui al decreto del Presidente della Repubblica 13 marzo 2013, n. 59, in materia di autorizzazione unica ambientale (AUA); al codice di cui al decreto legislativo 22 gennaio 2004, n. 42, e al regolamento di cui al decreto del Presidente della Repubblica 13 febbraio 2017, n. 31, in materia di autorizzazione paesaggistica; al testo unico di cui al decreto del Presidente della Repubblica 6 giugno 2001, n. 380, in materia edilizia; alla legge 28 gennaio 1994, n. 84, in materia di concessioni demaniali portuali;

a-bis) eventuali autorizzazioni, licenze, permessi, concessioni o nulla osta comunque denominati la cui adozione richiede l'acquisizione di pareri, intese, concerti o altri atti di assenso comunque denominati di competenza di piu' amministrazioni sono adottati ai sensi dell'articolo 14-bis della legge n. 241 del 1990; i termini ivi previsti sono ridotti della meta';

a-ter) il Comitato di indirizzo della ZES, entro trenta giorni dalla data di entrata in vigore della presente disposizione, assicura il raccordo tra gli sportelli unici istituiti ai sensi della normativa vigente e lo sportello unico di cui alla legge 28 gennaio 1994, n. 84, che opera quale responsabile unico del procedimento ai sensi della legge n. 241 del 1990 per la fase di insediamento, di realizzazione e di svolgimento dell'attivita' economica nella ZES. Lo sportello unico e' disponibile in formato digitale, in almeno una lingua diversa dall'italiano, ed e' organizzato sulla base di moduli e formulari standardizzati per la presentazione dell'istanza nei quali e', in particolare, indicata la presenza di eventuali vincoli ambientali e urbanistico-paesaggistici nonche' di eventuali termini di conclusione del procedimento;

a-quater) presso la Presidenza del Consiglio dei ministri e' istituita la Cabina di regia ZES, presieduta dal Ministro per il Sud, Autorita' politica delegata per la coesione territoriale e composta dal Ministro per gli affari regionali e le autonomie, dal Ministro per la pubblica amministrazione, dal Ministro dell'economia e delle finanze, dal Ministro delle infrastrutture e dei trasporti, dal

Ministro dello sviluppo economico, dai Presidenti delle regioni e delle province autonome e dai presidenti dei Comitati di indirizzo delle ZES istituite, nonche' dagli altri Ministri competenti in base all'ordine del giorno. Alle riunioni della Cabina di regia possono essere invitati come osservatori i rappresentanti di enti pubblici locali e nazionali e dei portatori di interesse collettivi o diffusi. L'istruttoria tecnica delle riunioni della Cabina di regia, che si avvale a tal fine del Dipartimento per le politiche di coesione della Presidenza del Consiglio dei ministri, riguarda principalmente la verifica e il monitoraggio degli interventi nelle ZES, sulla base dei dati raccolti ai sensi del comma 6. Alla prima riunione della Cabina di regia e' altresi' approvata la delibera recante il regolamento di organizzazione dei lavori della stessa;

a-quinquies) entro centoventi giorni dalla data di entrata in vigore della presente disposizione, ogni regione interessata puo' presentare al Ministro per il Sud, Autorita' politica delegata per la coesione territoriale una proposta di protocollo o convenzione per l'individuazione di ulteriori procedure semplificate e regimi procedimentali speciali. La proposta individua dettagliatamente le procedure oggetto di semplificazioni, le norme di riferimento e le amministrazioni locali e statali competenti ed e' approvata dalla Cabina di regia di cui alla lettera a-quater). Sono parti dell'accordo o protocollo la regione proponente e le amministrazioni locali o statali competenti per ogni procedimento individuato;

a-sexies) nelle ZES possono essere istituite zone franche doganali intercluse ai sensi del regolamento (UE) n. 952/2013 del Parlamento europeo e del Consiglio, del 9 ottobre 2013, che istituisce il codice doganale dell'Unione, e dei relativi atti di delega e di esecuzione. La perimetrazione di dette zone franche doganali e' proposta da ciascun Comitato di indirizzo entro trenta giorni dalla data di entrata in vigore della presente disposizione, ed e' approvata con determinazione del direttore dell'Agenzia delle dogane e dei monopoli, da adottare entro sessanta giorni dalla proposta".

2. All'articolo 5 del decreto-legge 20 giugno 2017, n. 91, convertito, con modificazioni, dalla legge 3 agosto 2017, n. 123, dopo il comma 2 e' inserito il seguente:

"2-bis. Gli interventi relativi agli oneri di urbanizzazione primaria di cui all'articolo 16, comma 7, del testo unico di cui al decreto del Presidente della Repubblica 6 giugno 2001, n. 380, per le imprese beneficiarie delle agevolazioni che effettuano gli investimenti ammessi al credito d'imposta di cui al comma 2, sono realizzati entro il termine perentorio di novanta giorni dalla presentazione della relativa istanza da parte delle imprese ai gestori dei servizi di pubblica utilita'. In caso di ritardo si applica l'articolo 2-bis della legge 7 agosto 1990, n. 241".

3. Il comma 64 dell'articolo 1 della legge 27 dicembre 2017, n. 205, e' sostituito dal seguente:

"64. Le nuove imprese e quelle gia' esistenti che operano nella Zona logistica semplificata fruiscono delle procedure semplificate di cui all'articolo 5, comma 1, lettere a), a-bis), a-ter), a-quater), a-quinquies) e a-sexies), del decreto-legge 20 giugno 2017, n. 91, convertito, con modificazioni, dalla legge 3 agosto 2017, n. 123".

4. Dall'attuazione del presente articolo non devono derivare nuovi o maggiori oneri a carico della finanza pubblica e ad essa si provvede mediante le risorse umane, finanziarie e strumentali disponibili a legislazione vigente.

Art. 3-quater (Altre misure di deburocratizzazione per le

imprese). - 1. All'articolo 3 della legge 27 gennaio 1968, n. 35, il secondo periodo e' soppresso.

2. Per gli aiuti di Stato e gli aiuti de minimis contenuti nel Registro nazionale degli aiuti di Stato di cui all'articolo 52 della legge 24 dicembre 2012, n. 234, la registrazione degli aiuti individuali nel predetto sistema, con conseguente pubblicazione nella sezione trasparenza ivi prevista, operata dai soggetti che concedono o gestiscono gli aiuti medesimi ai sensi della relativa disciplina, tiene luogo degli obblighi di pubblicazione posti a carico delle imprese beneficiarie previsti dall'articolo 1, comma 125, secondo periodo, della legge 4 agosto 2017, n. 124, a condizione che venga dichiarata nella nota integrativa del bilancio l'esistenza di aiuti oggetto di obbligo di pubblicazione nell'ambito del Registro nazionale degli aiuti di Stato.

3. Al solo fine di garantire un'ulteriore riduzione degli oneri amministrativi per le imprese e nel contempo una piu' uniforme applicazione delle disposizioni in materia di societa' a responsabilita' limitata semplificata, l'atto di scioglimento e messa in liquidazione, di cui all'articolo 2484 del codice civile, delle societa' a responsabilita' limitata semplificata di cui all'articolo 2463-bis del codice civile e' redatto per atto pubblico ovvero per atto sottoscritto con le modalita' previste dagli articoli 24 e 25 del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82. L'atto privo delle formalita' richieste per l'atto pubblico e' redatto secondo un modello uniforme adottato con decreto del Ministero dello sviluppo economico, di concerto con il Ministero della giustizia, ed e' trasmesso al competente ufficio del registro delle imprese di cui all'articolo 8 della legge 29 dicembre 1993, n. 580.

4. Ai soli fini dell'applicazione della disciplina di cui all'articolo 1, comma 9, della legge 11 dicembre 2016, n. 232, il costo agevolabile dei magazzini automatizzati interconnessi ai sistemi gestionali di fabbrica, di cui all'allegato A annesso alla suddetta legge, si intende comprensivo anche del costo attribuibile alla scaffalatura asservita dagli impianti automatici di movimentazione, che costituisce, al contempo, parte del sistema costruttivo dell'intero fabbricato; resta ferma la rilevanza di detta scaffalatura ai fini della determinazione della rendita catastale, in quanto elemento costruttivo dell'intero fabbricato.

Art. 3-quinquies (Agibilita' per lavoratori autonomi dello spettacolo). - 1. Al decreto legislativo del Capo provvisorio dello Stato 16 luglio 1947, n. 708, ratificato, con modificazioni, dalla legge 29 novembre 1952, n. 2388, sono apportate le seguenti modificazioni:

a) l'articolo 6 e' sostituito dal seguente:

"Art. 6. - 1. Le imprese dell'esercizio teatrale, cinematografico e circense, i teatri tenda, gli enti, le associazioni, le imprese del pubblico esercizio, gli alberghi, le emittenti radiotelevisive e gli impianti sportivi non possono far agire nei locali di proprieta' o di cui abbiano un diritto personale di godimento i lavoratori autonomi dello spettacolo, ivi compresi quelli con rapporti di collaborazione, appartenenti alle categorie indicate ai numeri da 1) a 14) del primo comma dell'articolo 3, che non siano in possesso del certificato di agibilita'. Per le prestazioni svolte dai lavoratori di cui al numero 23-bis) del primo comma dell'articolo 3 il certificato di agibilita' e' richiesto dai lavoratori medesimi, salvo l'obbligo di custodia dello stesso che e' posto a carico del committente.

2. In caso di inosservanza delle disposizioni di cui al comma 1 le imprese sono soggette alla sanzione amministrativa di euro 129 per ogni giornata di lavoro prestata da ciascun lavoratore autonomo";

b) all'articolo 10, il terzo comma e' abrogato».

All'articolo 4, il comma 2 e' sostituito dal seguente:

«2. L'articolo 560 del codice di procedura civile e' sostituito dal seguente:

"Art. 560 (Modo della custodia). - Il debitore e il terzo nominato custode debbono rendere il conto a norma dell'articolo 593.

Il custode nominato ha il dovere di vigilare affinche' il debitore e il nucleo familiare conservino il bene pignorato con la diligenza del buon padre di famiglia e ne mantengano e tutelino l'integrita'.

Il debitore e i familiari che con lui convivono non perdono il possesso dell'immobile e delle sue pertinenze sino al decreto di trasferimento, salvo quanto previsto dal sesto comma.

Il debitore deve consentire, in accordo con il custode, che l'immobile sia visitato da potenziali acquirenti.

Le modalita' del diritto di visita sono contemplate e stabilite nell'ordinanza di cui all'articolo 569.

Il giudice ordina, sentiti il custode e il debitore, la liberazione dell'immobile pignorato per lui ed il suo nucleo familiare, qualora sia ostacolato il diritto di visita di potenziali acquirenti, quando l'immobile non sia adeguatamente tutelato e mantenuto in uno stato di buona conservazione, per colpa o dolo del debitore e dei membri del suo nucleo familiare, quando il debitore viola gli altri obblighi che la legge pone a suo carico, o quando l'immobile non e' abitato dal debitore e dal suo nucleo familiare.

Al debitore e' fatto divieto di dare in locazione l'immobile pignorato se non e' autorizzato dal giudice dell'esecuzione.

Fermo quanto previsto dal sesto comma, quando l'immobile pignorato e' abitato dal debitore e dai suoi familiari il giudice non puo' mai disporre il rilascio dell'immobile pignorato prima della pronuncia del decreto di trasferimento ai sensi dell'articolo 586"».

Dopo l'articolo 4 e' inserito il seguente:

«Art. 4-bis (Disposizioni in favore dei familiari delle vittime e dei superstiti del disastro di Rigopiano del 18 gennaio 2017). - 1. E' autorizzata la spesa di 10 milioni di euro per l'anno 2019 ai fini della corresponsione di speciali elargizioni in favore delle famiglie delle vittime del disastro di Rigopiano, avvenuto il 18 gennaio 2017, e in favore di coloro che a causa del disastro hanno riportato lesioni gravi e gravissime.

2. La Presidenza del Consiglio dei ministri, d'intesa con i sindaci dei comuni di residenza delle vittime e dei soggetti che hanno riportato lesioni gravi e gravissime, individua le famiglie beneficiarie delle elargizioni di cui al comma 1 e determina la somma spettante a ciascuna famiglia e a ciascun soggetto.

3. A ciascuna delle famiglie delle vittime e' attribuita una somma determinata tenuto conto anche dello stato di effettiva necessita'.

4. Ai soggetti che hanno riportato lesioni gravi e gravissime e' attribuita una somma determinata, nell'ambito del limite di spesa complessivo stabilito dal comma 1, in proporzione alla gravita' delle lesioni subite e tenuto conto dello stato di effettiva necessita'. All'attribuzione delle speciali elargizioni di cui al presente articolo si provvede, ai sensi del comma 7, nei limiti dell'autorizzazione di spesa di cui al comma 1.

5. Le elargizioni di cui al comma 1 spettanti alle famiglie delle

vittime sono assegnate e corrisposte secondo il seguente ordine:

a) al coniuge superstite, con esclusione del coniuge rispetto al quale sia stata pronunciata sentenza anche non definitiva di scioglimento o di cessazione degli effetti civili del matrimonio e del coniuge cui sia stata addebitata la separazione con sentenza passata in giudicato, e ai figli se a carico;

b) ai figli, in mancanza del coniuge superstite o nel caso di coniuge rispetto al quale sia stata pronunciata sentenza anche non definitiva di scioglimento o di cessazione degli effetti civili del matrimonio o di coniuge cui sia stata addebitata la separazione con sentenza passata in giudicato;

c) al convivente more uxorio;

d) ai genitori;

e) ai fratelli e alle sorelle, se conviventi e a carico;

f) ai conviventi a carico negli ultimi tre anni precedenti l'evento.

6. In presenza di figli a carico della vittima nati da rapporti di convivenza more uxorio, l'elargizione di cui al comma 3 e' assegnata al convivente more uxorio con lo stesso ordine di priorita' previsto per i beneficiari di cui alla lettera a) del comma 5.

7. Le elargizioni di cui al comma 1 sono corrisposte con decreti del Presidente del Consiglio dei ministri.

8. Le medesime elargizioni sono esenti da ogni imposta o tassa e sono assegnate in aggiunta ad ogni altra somma cui i soggetti beneficiari abbiano diritto a qualsiasi titolo ai sensi della normativa vigente.

9. Agli oneri derivanti dal presente articolo, pari a 10 milioni di euro per l'anno 2019, si provvede mediante utilizzo delle risorse iscritte per l'anno 2019 nel Fondo per il federalismo amministrativo di parte corrente, di cui alla legge 15 marzo 1997, n. 59, dello stato di previsione del Ministero dell'interno.

10. Il Ministro dell'economia e delle finanze e' autorizzato ad apportare, con propri decreti, le occorrenti variazioni di bilancio».

All'articolo 6, il comma 3 e' sostituito dai seguenti:

«3. A decorrere dalla data di entrata in vigore della legge di conversione del presente decreto e' istituito il Registro elettronico nazionale per la tracciabilita' dei rifiuti, gestito direttamente dal Ministero dell'ambiente e della tutela del territorio e del mare, cui sono tenuti ad iscriversi, entro il termine individuato con il decreto di cui al comma 3-bis, gli enti e le imprese che effettuano il trattamento dei rifiuti, i produttori di rifiuti pericolosi e gli enti e le imprese che raccolgono o trasportano rifiuti pericolosi a titolo professionale o che operano in qualita' di commercianti ed intermediari di rifiuti pericolosi, i Consorzi istituiti per il recupero e il riciclaggio di particolari tipologie di rifiuti, nonche', con riferimento ai rifiuti non pericolosi, i soggetti di cui all'articolo 189, comma 3, del decreto legislativo 3 aprile 2006, n. 152.

3-bis. Il Ministro dell'ambiente e della tutela del territorio e del mare, con proprio decreto adottato ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, di concerto con il Ministro dell'economia e delle finanze, sentiti il Ministro dello sviluppo economico, il Ministro per la pubblica amministrazione e il Ministro delle infrastrutture e dei trasporti, nonche' per gli aspetti di competenza il Ministro della difesa, definisce le modalita' di organizzazione e funzionamento del Registro elettronico nazionale, le modalita' di iscrizione dei soggetti obbligati e di coloro che intendano volontariamente aderirvi, nonche' gli

adempimenti cui i medesimi sono tenuti, secondo criteri di gradualita' per la progressiva partecipazione di tutti gli operatori.

3-ter. Dal 1° gennaio 2019 e fino al termine di piena operativita' del Registro elettronico nazionale come individuato con il decreto di cui al comma 3-bis, la tracciabilita' dei rifiuti e' garantita effettuando gli adempimenti di cui agli articoli 188, 189, 190 e 193 del decreto legislativo 3 aprile 2006, n. 152, nel testo previgente alle modifiche apportate dal decreto legislativo 3 dicembre 2010, n. 205, anche mediante le modalita' di cui all'articolo 194-bis del decreto legislativo n. 152 del 2006; si applicano altresi' le disposizioni di cui all'articolo 258 del decreto legislativo n. 152 del 2006, nel testo previgente alle modifiche apportate dal decreto legislativo n. 205 del 2010.

3-quater. L'iscrizione al Registro elettronico nazionale comporta il versamento di un diritto di segreteria e di un contributo annuale, al fine di assicurare l'integrale copertura dei costi di funzionamento del sistema. Con il medesimo decreto di cui al comma 3-bis, da aggiornare ogni tre anni, sono determinati gli importi dovuti a titolo di diritti di segreteria e di contributo nonche' le modalita' di versamento. Agli oneri derivanti dall'istituzione del Registro elettronico nazionale, pari a 1,61 milioni di euro per l'anno 2019, si provvede: quanto a 1,5 milioni di euro per l'anno 2019, mediante corrispondente riduzione dello stanziamento del fondo speciale di conto capitale iscritto, ai fini del bilancio triennale 2019-2021, nell'ambito del programma "Fondi di riserva e speciali" della missione "Fondi da ripartire" dello stato di previsione del Ministero dell'economia e delle finanze per l'anno 2019, allo scopo parzialmente utilizzando l'accantonamento relativo al Ministero dell'ambiente e della tutela del territorio e del mare; quanto a 0,11 milioni di euro per l'anno 2019, mediante corrispondente riduzione dello stanziamento del fondo speciale di parte corrente iscritto, ai fini del bilancio triennale 2019-2021, nell'ambito del programma "Fondi di riserva e speciali" della missione "Fondi da ripartire" dello stato di previsione del Ministero dell'economia e delle finanze per l'anno 2019, allo scopo parzialmente utilizzando l'accantonamento relativo al Ministero dell'ambiente e della tutela del territorio e del mare. A decorrere dall'anno 2020 agli oneri di funzionamento si provvede con i proventi derivanti dai diritti di segreteria e con il contributo annuale, che sono versati ad apposito capitolo dell'entrata del bilancio dello Stato per essere riassegnati, con decreto del Ministro dell'economia e delle finanze, ad apposito capitolo dello stato di previsione del Ministero dell'ambiente e della tutela del territorio e del mare.

3-quinquies. La violazione dell'obbligo di iscrizione, il mancato o parziale versamento del contributo e le violazioni degli obblighi stabiliti con il decreto di cui al comma 3-bis sono soggetti a sanzioni amministrative pecuniarie il cui importo e' determinato, per le singole condotte sanzionate, con il medesimo decreto. Gli importi delle sanzioni sono versati ad apposito capitolo dell'entrata del bilancio dello Stato per essere riassegnati, con decreto del Ministro dell'economia e delle finanze, ai pertinenti capitoli dello stato di previsione del Ministero dell'ambiente e della tutela del territorio e del mare, destinati agli interventi di bonifica dei siti di cui all'articolo 252, comma 5, del decreto legislativo 3 aprile 2006, n. 152, ove ricorrano le condizioni di cui all'articolo 253, comma 5, del medesimo decreto legislativo, secondo criteri e modalita' di ripartizione fissati con decreto del Ministro dell'ambiente e della tutela del territorio e del mare.

3-sexies. Il Ministro dell'economia e delle finanze e' autorizzato ad apportare, con propri decreti, le occorrenti variazioni di bilancio».

All'articolo 8:

dopo il comma 1 sono inseriti i seguenti:

«1-bis. Il mandato del Commissario straordinario per l'attuazione dell'Agenda digitale, nominato con decreto del Presidente del Consiglio dei ministri 25 ottobre 2018, ai sensi dell'articolo 63 del decreto legislativo 26 agosto 2016, n. 179, nonche' l'operativita' della relativa struttura di supporto, sono prorogati al 31 dicembre 2019.

1-ter. A decorrere dal 1° gennaio 2020, al fine di garantire l'attuazione degli obiettivi dell'Agenda digitale italiana, anche in coerenza con l'Agenda digitale europea, le funzioni, i compiti e i poteri conferiti al Commissario straordinario per l'attuazione dell'Agenda digitale dall'articolo 63 del decreto legislativo 26 agosto 2016, n. 179, sono attribuiti al Presidente del Consiglio dei ministri o al Ministro delegato che li esercita per il tramite delle strutture della Presidenza del Consiglio dei ministri dallo stesso individuate, di concerto con il Ministero dell'economia e delle finanze per le materie di sua competenza.

1-quater. Per l'esercizio delle funzioni di cui al comma 1-ter, il Presidente del Consiglio dei ministri, o il Ministro delegato, si avvale di un contingente di esperti messi a disposizioni delle strutture di cui al medesimo comma 1-ter, in possesso di specifica ed elevata competenza tecnologica e di gestione di processi complessi, nonche' di significativa esperienza in tali materie, ivi compreso lo sviluppo di programmi e piattaforme digitali con diffusione su larga scala, da nominare ai sensi dell'articolo 9 del decreto legislativo 30 luglio 1999, n. 303. Con apposito decreto del Presidente del Consiglio dei ministri, sono individuati il contingente di tali esperti e la relativa composizione, con le specifiche qualificazioni richieste ed i relativi compensi.

1-quinquies. Agli oneri derivanti dall'attuazione dei commi da 1-bis a 1-quater, pari a 6 milioni di euro annui a decorrere dall'anno 2020, si provvede:

a) quanto a 4 milioni di euro per l'anno 2020, mediante corrispondente riduzione dello stanziamento del fondo speciale di parte corrente iscritto, ai fini del bilancio triennale 2019-2021, nell'ambito del programma "Fondi di riserva e speciali" della missione "Fondi da ripartire" dello stato di previsione del Ministero dell'economia e delle finanze per l'anno 2019, allo scopo parzialmente utilizzando l'accantonamento relativo al Ministero dell'economia e delle finanze;

b) quanto a 2 milioni di euro per l'anno 2020 e a 6 milioni di euro a decorrere dall'anno 2021, mediante riduzione dell'autorizzazione di spesa di cui all'articolo 1, comma 200, della legge 23 dicembre 2014, n. 190, relativa al Fondo per esigenze indifferibili»;

al comma 2:

al primo periodo, le parole: «gia' assegnate all'Agenzia per l'Italia digitale» sono sostituite dalle seguenti: «gia' destinate dall'Agenzia per l'Italia digitale»;

dopo il primo periodo e' inserito il seguente: «Le predette risorse finanziarie sono versate, nell'anno 2019, all'entrata del bilancio dello Stato per essere riassegnate allo stato di previsione del Ministero dell'economia e delle finanze e destinate al bilancio autonomo della Presidenza del Consiglio dei ministri».

Dopo l'articolo 8 sono inseriti i seguenti:

«Art. 8-bis (Misure di semplificazione per l'innovazione). - 1. Al decreto legislativo 15 febbraio 2016, n. 33, sono apportate le seguenti modificazioni:

a) all'articolo 7, dopo il comma 2 sono aggiunti i seguenti:

"2-bis. Qualora siano utilizzate infrastrutture fisiche esistenti e tecnologie di scavo a basso impatto ambientale in presenza di sottoservizi, ai fini dell'autorizzazione archeologica di cui all'articolo 21 del codice di cui al decreto legislativo 22 gennaio 2004, n. 42, l'avvio dei lavori e' subordinato alla trasmissione, da parte dell'operatore di rete alla soprintendenza competente, di documentazione cartografica rilasciata dalle competenti autorita' locali che attesti la sovrapposizione dell'intero tracciato ai sottoservizi esistenti. La disposizione si applica anche alla realizzazione dei pozzetti accessori alle infrastrutture stesse, qualora essi siano realizzati al di sopra dei medesimi sottoservizi preesistenti. L'operatore di rete comunica, con un preavviso di almeno quindici giorni, l'inizio dei lavori alla soprintendenza competente. Qualora la posa in opera dei sottoservizi interessi spazi aperti nei centri storici, e' altresi' depositato presso la soprintendenza, ai fini della preventiva approvazione, apposito elaborato tecnico che dia conto anche della risistemazione degli spazi oggetto degli interventi.

2-ter. Qualora siano utilizzate tecnologie di scavo a basso impatto ambientale con minitrincea, come definita dall'articolo 8 del decreto del Ministro dello sviluppo economico 1° ottobre 2013, pubblicato nella Gazzetta Ufficiale n. 244 del 17 ottobre 2013, ai fini dell'autorizzazione archeologica di cui all'articolo 21 del decreto legislativo 22 gennaio 2004, n. 42, le attivita' di scavo sono precedute da indagini non invasive, concordate con la soprintendenza, in relazione alle caratteristiche delle aree interessate dai lavori. A seguito delle suddette indagini, dei cui esiti, valutati dalla soprintendenza, si tiene conto nella progettazione dell'intervento, in considerazione del limitato impatto sul sottosuolo, le tecnologie di scavo in minitrincea si considerano esentate dalla procedura di verifica preventiva dell'interesse archeologico di cui all'articolo 25, commi 8 e seguenti, del codice di cui al decreto legislativo 18 aprile 2016, n. 50. In ogni caso il soprintendente puo' prescrivere il controllo archeologico in corso d'opera per i lavori di scavo";

b) all'articolo 8, dopo il comma 4 e' inserito il seguente:

"4-bis. I lavori necessari alla realizzazione di infrastrutture interne ed esterne all'edificio predisposte per le reti di comunicazione elettronica a banda ultralarga, volte a portare la rete sino alla sede dell'abbonato, sono equiparati ai lavori di manutenzione straordinaria urgente di cui all'articolo 1135 del codice civile. Tale disposizione non si applica agli immobili tutelati ai sensi della parte seconda del decreto legislativo 22 gennaio 2004, n. 42";

c) all'articolo 12, comma 3, sono aggiunte, in fine, le seguenti parole: ", restando quindi escluso ogni altro tipo di onere finanziario, reale o contributo, comunque denominato, di qualsiasi natura e per qualsivoglia ragione o titolo richiesto".

2. All'articolo 88 del codice di cui al decreto legislativo 1° agosto 2003, n. 259, sono apportate le seguenti modificazioni:

a) al comma 1, dopo le parole: "conforme ai modelli predisposti dagli Enti locali e, ove non predisposti, al modello C di cui all'allegato n. 13, all'Ente locale ovvero alla figura soggettiva

pubblica proprietaria delle aree" sono aggiunte le seguenti: "un'istanza unica";

b) al comma 6, dopo le parole: "Il rilascio dell'autorizzazione comporta l'autorizzazione alla effettuazione degli scavi" sono inserite le seguenti: "e delle eventuali opere civili";

c) dopo il comma 7 e' inserito il seguente:

"7-bis. In riferimento ad interventi per l'installazione di reti di comunicazione elettronica a banda ultralarga, in deroga a quanto previsto dall'articolo 22, comma 1, del codice di cui al decreto legislativo 22 gennaio 2004, n. 42, l'autorizzazione prevista dall'articolo 21, comma 4, relativa agli interventi in materia di edilizia pubblica e privata, ivi compresi gli interventi sui beni di cui all'articolo 10, comma 4, lettera g), del medesimo decreto legislativo n. 42 del 2004, e' rilasciata entro il termine di novanta giorni dalla ricezione della richiesta da parte della soprintendenza a condizione che detta richiesta sia corredata di idonea e completa documentazione tecnica".

3. All'allegato B al regolamento di cui al decreto del Presidente della Repubblica 13 febbraio 2017, n. 31, il capoverso B.10 e' sostituito dal seguente:

"B.10. Installazione di cabine per impianti tecnologici a rete, fatta salva la fattispecie dell'installazione delle stesse all'interno di siti recintati gia' attrezzati con apparati di rete che, non superando l'altezza della recinzione del sito, non comporti un impatto paesaggistico ulteriore del sito nel suo complesso, da intendersi ricompresa e disciplinata dalla voce A.8 dell'allegato A, o colonnine modulari ovvero sostituzione delle medesime con altre diverse per tipologia, dimensioni e localizzazione".

4. All'articolo 26 del codice della strada, di cui al decreto legislativo 30 aprile 1992, n. 285, dopo il comma 3 e' inserito il seguente:

"3-bis. Nel caso di interventi finalizzati all'installazione di reti di comunicazione elettronica a banda ultralarga, il nulla osta di cui al comma 3 e' rilasciato nel termine di quindici giorni dalla ricezione della richiesta da parte del comune".

5. All'articolo 94, comma 2, del testo unico di cui al decreto del Presidente della Repubblica 6 giugno 2001, n. 380, dopo le parole: "entro sessanta giorni dalla richiesta" sono inserite le seguenti: ", ed entro quaranta giorni dalla stessa in riferimento ad interventi finalizzati all'installazione di reti di comunicazione elettronica a banda ultralarga,".

Art. 8-ter (Tecnologie basate su registri distribuiti e smart contract). - 1. Si definiscono "tecnologie basate su registri distribuiti" le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili.

2. Si definisce "smart contract" un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o piu' parti sulla base di effetti predefiniti dalle stesse. Gli smart contract soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale con linee guida da adottare entro novanta giorni dalla data di entrata in vigore della

legge di conversione del presente decreto.

3. La memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica di cui all'articolo 41 del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014.

4. Entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto, l'Agenzia per l'Italia digitale individua gli standard tecnici che le tecnologie basate su registri distribuiti debbono possedere ai fini della produzione degli effetti di cui al comma 3».

Dopo l'articolo 9 e' inserito il seguente:

«Art. 9-bis (Semplificazioni in materia di personale del Servizio sanitario nazionale e di fatturazione elettronica per gli operatori sanitari). - 1. All'articolo 1 della legge 30 dicembre 2018, n. 145, sono apportate le seguenti modificazioni:

a) al comma 365 e' aggiunto, in fine, il seguente periodo: "Le previsioni di cui ai commi 361, 363 e 364 si applicano alle procedure concorsuali per l'assunzione di personale medico, tecnico-professionale e infermieristico, bandite dalle aziende e dagli enti del Servizio sanitario nazionale a decorrere dal 1° gennaio 2020";

b) al comma 687, il secondo periodo e' sostituito dal seguente: "Per il triennio 2019-2021, la dirigenza amministrativa, professionale e tecnica del Servizio sanitario nazionale, in considerazione della mancata attuazione nei termini previsti della delega di cui all'articolo 11, comma 1, lettera b), della legge 7 agosto 2015, n. 124, e' compresa nell'area della contrattazione collettiva della sanita' nell'ambito dell'apposito accordo stipulato ai sensi dell'articolo 40, comma 2, del decreto legislativo 30 marzo 2001, n. 165".

2. Le disposizioni di cui all'articolo 10-bis del decreto-legge 23 ottobre 2018, n. 119, convertito, con modificazioni, dalla legge 17 dicembre 2018, n. 136, si applicano anche ai soggetti che non sono tenuti all'invio dei dati al Sistema tessera sanitaria, con riferimento alle fatture relative alle prestazioni sanitarie effettuate nei confronti delle persone fisiche.

3. Per le finalita' di cui al comma 582 dell'articolo 1 della legge 30 dicembre 2018, n. 145, nel caso in cui alla data del 15 febbraio 2019 non si sia perfezionato il recupero integrale delle risorse finanziarie connesse alle procedure di ripiano della spesa farmaceutica per gli anni dal 2013 al 2015 e per l'anno 2016, ai sensi dell'articolo 1, commi da 389 a 392, della legge 27 dicembre 2017, n. 205, nonche' per l'anno 2017 per la spesa per acquisti diretti, il direttore generale dell'Agenzia italiana del farmaco (AIFA) accerta che entro il 30 aprile 2019 sia stato versato dalle aziende farmaceutiche titolari di autorizzazione all'immissione in commercio (AIC) almeno l'importo di euro 2.378 milioni, a titolo di ripiano della spesa farmaceutica stessa. Al fine di semplificare le modalita' di versamento, le predette aziende si avvalgono del Fondo istituito presso il Ministero dell'economia e delle finanze dall'articolo 21, comma 23, del decreto-legge 24 giugno 2016, n. 113, convertito, con modificazioni, dalla legge 7 agosto 2016, n. 160, che e' ridenominato allo scopo "Fondo per payback 2013-2017".

4. L'accertamento di cui al comma 3 e' compiuto entro il 31 maggio 2019, anche sulla base dei dati forniti dal Ministero dell'economia e delle finanze nonche' dalle regioni interessate, ed e' effettuato computando gli importi gia' versati per i ripiani degli

anni 2013-2017 e quelli versati risultanti a seguito degli effetti, che restano fermi, delle transazioni stipulate ai sensi dell'articolo 1, comma 390, della legge 27 dicembre 2017, n. 205, e dell'articolo 22-quater del decreto-legge 23 ottobre 2018, n. 119, convertito, con modificazioni, dalla legge 17 dicembre 2018, n. 136. Dell'esito dell'accertamento e' data notizia nel sito istituzionale dell'AIFA.

5. L'accertamento positivo del conseguimento della somma complessivamente prevista dal comma 3 si intende satisfattivo di ogni obbligazione a carico di ciascuna azienda farmaceutica titolare di AIC tenuta al ripiano della spesa farmaceutica per gli anni dal 2013 al 2017 e ne consegue l'estinzione di diritto, per cessata materia del contendere, a spese compensate, delle liti pendenti dinanzi al giudice amministrativo, aventi ad oggetto le determinazioni dell'AIFA relative ai ripiani di cui al comma 3. L'AIFA e' tenuta a comunicare l'esito dell'accertamento di cui al comma 4 alle segreterie degli organi giurisdizionali presso i quali pendono i giudizi di cui al presente comma, inerenti all'attivita' di recupero del ripiano della spesa farmaceutica degli anni 2013-2017.

6. A seguito dell'accertamento positivo, con decreto del Ministro dell'economia e delle finanze, sentita l'AIFA, d'intesa con la Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano, e' ripartito tra le regioni e le province autonome l'importo giacente sul Fondo per payback 2013-2017».

Dopo l'articolo 10 e' inserito il seguente:

«Art. 10-bis (Misure urgenti in materia di autoservizi pubblici non di linea). - 1. Alla legge 15 gennaio 1992, n. 21, sono apportate le seguenti modificazioni:

a) all'articolo 3, comma 1, le parole: "presso la rimessa" sono sostituite dalle seguenti: "presso la sede o la rimessa" e sono aggiunte, in fine, le seguenti parole: "anche mediante l'utilizzo di strumenti tecnologici";

b) all'articolo 3, il comma 3 e' sostituito dal seguente:

"3. La sede operativa del vettore e almeno una rimessa devono essere situate nel territorio del comune che ha rilasciato l'autorizzazione. E' possibile per il vettore disporre di ulteriori rimesse nel territorio di altri comuni della medesima provincia o area metropolitana in cui ricade il territorio del comune che ha rilasciato l'autorizzazione, previa comunicazione ai comuni predetti, salvo diversa intesa raggiunta in sede di Conferenza unificata entro il 28 febbraio 2019. In deroga a quanto previsto dal presente comma, in ragione delle specificita' territoriali e delle carenze infrastrutturali, per le sole regioni Sicilia e Sardegna l'autorizzazione rilasciata in un comune della regione e' valida sull'intero territorio regionale, entro il quale devono essere situate la sede operativa e almeno una rimessa";

c) all'articolo 10, dopo il comma 2 e' inserito il seguente:

"2-bis. I titolari di licenza per l'esercizio del servizio di taxi o di autorizzazione per l'esercizio del servizio di noleggio con conducente di autovettura ovvero di natante, in caso di malattia, invalidita' o sospensione della patente, intervenute successivamente al rilascio della licenza o dell'autorizzazione, possono mantenere la titolarita' della licenza o dell'autorizzazione, a condizione che siano sostituiti alla guida dei veicoli o alla conduzione dei natanti, per l'intero periodo di durata della malattia, dell'invalidita' o della sospensione della patente, da persone in possesso dei requisiti professionali e morali previsti dalla normativa vigente";

d) all'articolo 10, il comma 3 e' sostituito dal seguente:

"3. Il rapporto di lavoro con un sostituto alla guida e' regolato con contratto di lavoro stipulato in base alle norme vigenti. Il rapporto con il sostituto alla guida puo' essere regolato anche in base ad un contratto di gestione";

e) all'articolo 11, il comma 4 e' sostituito dal seguente:

"4. Le prenotazioni di trasporto per il servizio di noleggio con conducente sono effettuate presso la rimessa o la sede, anche mediante l'utilizzo di strumenti tecnologici. L'inizio ed il termine di ogni singolo servizio di noleggio con conducente devono avvenire presso le rimesse di cui all'articolo 3, comma 3, con ritorno alle stesse. Il prelevamento e l'arrivo a destinazione dell'utente possono avvenire anche al di fuori della provincia o dell'area metropolitana in cui ricade il territorio del comune che ha rilasciato l'autorizzazione. Nel servizio di noleggio con conducente e' previsto l'obbligo di compilazione e tenuta da parte del conducente di un foglio di servizio in formato elettronico, le cui specifiche sono stabilite dal Ministero delle infrastrutture e dei trasporti con proprio decreto, adottato di concerto con il Ministero dell'interno. Il foglio di servizio in formato elettronico deve riportare: a) targa del veicolo; b) nome del conducente; c) data, luogo e chilometri di partenza e arrivo; d) orario di inizio servizio, destinazione e orario di fine servizio; e) dati del fruitore del servizio. Fino all'adozione del decreto di cui al presente comma, il foglio di servizio elettronico e' sostituito da una versione cartacea dello stesso, caratterizzata da numerazione progressiva delle singole pagine da compilare, avente i medesimi contenuti previsti per quello in formato elettronico, e da tenere in originale a bordo del veicolo per un periodo non inferiore a quindici giorni, per essere esibito agli organi di controllo, con copia conforme depositata in rimessa";

f) all'articolo 11, dopo il comma 4 sono inseriti i seguenti:

"4-bis. In deroga a quanto previsto dal comma 4, l'inizio di un nuovo servizio puo' avvenire senza il rientro in rimessa, quando sul foglio di servizio sono registrate, sin dalla partenza dalla rimessa o dal pontile d'attracco, piu' prenotazioni di servizio oltre la prima, con partenza o destinazione all'interno della provincia o dell'area metropolitana in cui ricade il territorio del comune che ha rilasciato l'autorizzazione. Per quanto riguarda le regioni Sicilia e Sardegna, partenze e destinazioni possono ricadere entro l'intero territorio regionale.

4-ter. Fermo restando quanto previsto dal comma 3, e' in ogni caso consentita la fermata su suolo pubblico durante l'attesa del cliente che ha effettuato la prenotazione del servizio e nel corso dell'effettiva prestazione del servizio stesso".

2. Il decreto del Ministero delle infrastrutture e dei trasporti, di concerto con il Ministero dell'interno, di cui all'articolo 11, comma 4, della legge 15 gennaio 1992, n. 21, come modificato dal comma 1, lettera e), del presente articolo, e' adottato entro il 30 giugno 2019.

3. Entro un anno dalla data di entrata in vigore del presente decreto, presso il Centro elaborazione dati del Ministero delle infrastrutture e dei trasporti e' istituito un registro informatico pubblico nazionale delle imprese titolari di licenza per il servizio taxi effettuato con autovettura, motocarrozzetta e natante e di quelle di autorizzazione per il servizio di noleggio con conducente effettuato con autovettura, motocarrozzetta e natante. Con decreto del Ministero delle infrastrutture e dei trasporti sono individuate le specifiche tecniche di attuazione e le modalita' con le quali le

predette imprese dovranno registrarsi. Agli oneri derivanti dalle previsioni del presente comma, connessi all'implementazione e all'adeguamento dei sistemi informatici del Centro elaborazione dati del Ministero delle infrastrutture e dei trasporti, pari ad euro un milione per l'annualita' 2019, si provvede mediante utilizzo dell'autorizzazione di spesa di cui all'articolo 1, comma 3, del decreto-legge 29 dicembre 2018, n. 143. Alla gestione dell'archivio il Ministero delle infrastrutture e dei trasporti provvede con le risorse umane, finanziarie e strumentali disponibili a legislazione vigente, senza nuovi o maggiori oneri per la finanza pubblica.

4. Le sanzioni di cui all'articolo 11-bis della legge 15 gennaio 1992, n. 21, per l'inosservanza degli articoli 3 e 11 della medesima legge, come modificati dal comma 1 del presente articolo, si applicano a decorrere dal novantesimo giorno successivo alla data di entrata in vigore del presente decreto. Parimenti rimangono sospese per la stessa durata le sanzioni previste dall'articolo 85, commi 4 e 4-bis, del codice della strada, di cui al decreto legislativo 30 aprile 1992, n. 285, limitatamente ai soggetti titolari di autorizzazione per l'esercizio del servizio di noleggio con conducente.

5. A decorrere dal 1° gennaio 2019, il comma 3 dell'articolo 2 del decreto-legge 25 marzo 2010, n. 40, convertito, con modificazioni, dalla legge 22 maggio 2010, n. 73, e' abrogato.

6. A decorrere dalla data di entrata in vigore del presente decreto e fino alla piena operativita' dell'archivio informatico pubblico nazionale delle imprese di cui al comma 3, non e' consentito il rilascio di nuove autorizzazioni per l'espletamento del servizio di noleggio con conducente con autovettura, motocarrozzetta e natante.

7. A decorrere dal 1° gennaio 2019, l'articolo 7-bis del decreto-legge 10 febbraio 2009, n. 5, convertito, con modificazioni, dalla legge 9 aprile 2009, n. 33, e' abrogato.

8. Con decreto del Presidente del Consiglio dei ministri, su proposta del Ministro delle infrastrutture e dei trasporti e del Ministro dello sviluppo economico, da adottare ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, e' disciplinata l'attivita' delle piattaforme tecnologiche di intermediazione che intermediano tra domanda e offerta di autoservizi pubblici non di linea.

9. Fino alla data di adozione delle deliberazioni della Conferenza unificata di cui al comma 1, lettera b), e comunque per un periodo non superiore a due anni dalla data di entrata in vigore del presente decreto, l'inizio di un singolo servizio, fermo l'obbligo di previa prenotazione, puo' avvenire da luogo diverso dalla rimessa, quando lo stesso e' svolto in esecuzione di un contratto in essere tra cliente e vettore, stipulato in forma scritta con data certa sino a quindici giorni antecedenti la data di entrata in vigore del presente decreto e regolarmente registrato. L'originale o copia conforme del contratto deve essere tenuto a bordo della vettura o presso la sede e deve essere esibito in caso di controlli».

All'articolo 11, dopo il comma 2 sono aggiunti i seguenti:

«2-bis. Al fine di semplificare le procedure per la copertura dei posti non riservati ai sensi dell'articolo 703, comma 1, lettera c), del codice dell'ordinamento militare, di cui al decreto legislativo 15 marzo 2010, n. 66, e' autorizzata l'assunzione degli allievi agenti della Polizia di Stato, nei limiti delle facolta' assunzionali non soggette alle riserve di posti di cui al citato articolo 703, comma 1, lettera c), e nel limite massimo di 1.851 posti, mediante

scorrimento della graduatoria della prova scritta di esame del concorso pubblico per l'assunzione di 893 allievi agenti della Polizia di Stato bandito con decreto del Capo della Polizia - Direttore generale della pubblica sicurezza del 18 maggio 2017, pubblicato nella Gazzetta Ufficiale - 4a Serie speciale - n. 40 del 26 maggio 2017. L'Amministrazione della pubblica sicurezza procede alle predette assunzioni:

a) a valere sulle facolta' assunzionali previste per l'anno 2019 in relazione alle cessazioni intervenute entro la data del 31 dicembre 2018 e nei limiti del relativo risparmio di spesa, determinato ai sensi dell'articolo 66, commi 9-bis e 10, del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133;

b) limitatamente ai soggetti risultati idonei alla relativa prova scritta d'esame e secondo l'ordine decrescente del voto in essa conseguito, ferme restando le riserve e le preferenze applicabili secondo la normativa vigente alla predetta procedura concorsuale, purche' in possesso, alla data del 1° gennaio 2019, dei requisiti di cui all'articolo 6 del decreto del Presidente della Repubblica 24 aprile 1982, n. 335, nel testo vigente alla data di entrata in vigore della legge 30 dicembre 2018, n. 145, fatte salve le disposizioni di cui all'articolo 2049 del citato codice dell'ordinamento militare;

c) previa verifica dei requisiti di cui alla lettera b), mediante convocazione degli interessati, individuati con decreto del Capo della Polizia - Direttore generale della pubblica sicurezza, in relazione al numero dei posti di cui al presente comma, secondo l'ordine determinato in applicazione delle disposizioni di cui alla citata lettera b);

d) previo avvio a piu' corsi di formazione di cui all'articolo 6-bis del citato decreto del Presidente della Repubblica n. 335 del 1982, ciascuno con propria decorrenza giuridica ed economica, secondo le disponibilita' organizzative e logistiche degli istituti di istruzione dell'Amministrazione della pubblica sicurezza.

2-ter. All'articolo 1 della legge 30 dicembre 2018, n. 145, sono apportate le seguenti modificazioni:

a) al comma 149, il secondo periodo e' soppresso;

b) al comma 151:

1) all'alinea, le parole: "pari a 7,5 milioni di euro per ciascuna delle annualita' del biennio 2019-2020 e a 20,5 milioni di euro" sono sostituite dalle seguenti: "pari a 7 milioni di euro per ciascuna delle annualita' del biennio 2019-2020 e a 18 milioni di euro";

2) alla lettera a), le parole: "quanto a 5 milioni di euro a decorrere dal 2019" sono sostituite dalle seguenti: "quanto a 4,5 milioni di euro per ciascuna delle annualita' del biennio 2019-2020 e a 2,5 milioni di euro a decorrere dal 2021".

2-quater. All'articolo 26 del decreto legislativo 21 maggio 2018, n. 53, sono apportate le seguenti modificazioni:

a) al comma 1, il secondo periodo e' sostituito dal seguente: "Le disposizioni del predetto decreto continuano ad applicarsi sino al 30 giugno 2019";

b) al comma 2, il primo periodo e' sostituito dal seguente: "Il decreto del Ministro dell'interno 16 dicembre 2010, pubblicato nella Gazzetta Ufficiale n. 302 del 28 dicembre 2010, cessa di avere efficacia a decorrere dal 1° luglio 2019".

2-quinquies. All'articolo 1, comma 441, secondo periodo, della legge 30 dicembre 2018, n. 145, le parole: "Previo avvio delle rispettive procedure negoziali e di concertazione," sono soppresse».

Dopo l'articolo 11 sono inseriti i seguenti:

«Art. 11-bis (Misure di semplificazione in materia contabile in favore degli enti locali). - 1. Nelle more della conclusione dei lavori del tavolo tecnico-politico per la redazione di linee guida finalizzate all'avvio di un percorso di revisione organica della disciplina in materia di ordinamento delle province e delle citta' metropolitane, al superamento dell'obbligo di gestione associata delle funzioni e alla semplificazione degli oneri amministrativi e contabili a carico dei comuni, soprattutto di piccole dimensioni, di cui all'articolo 1, comma 2-ter, del decreto-legge 25 luglio 2018, n. 91, convertito, con modificazioni, dalla legge 21 settembre 2018, n. 108, all'articolo 1, comma 1120, lettera a), della legge 27 dicembre 2017, n. 205, le parole: "30 giugno 2019" sono sostituite dalle seguenti: "31 dicembre 2019".

2. Fermo restando quanto previsto dai commi 557-quater e 562 dell'articolo 1 della legge 27 dicembre 2006, n. 296, per i comuni privi di posizioni dirigenziali, il limite previsto dall'articolo 23, comma 2, del decreto legislativo 25 maggio 2017, n. 75, non si applica al trattamento accessorio dei titolari di posizione organizzativa di cui agli articoli 13 e seguenti del contratto collettivo nazionale di lavoro (CCNL) relativo al personale del comparto funzioni locali - Triennio 2016-2018, limitatamente al differenziale tra gli importi delle retribuzioni di posizione e di risultato gia' attribuiti alla data di entrata in vigore del predetto CCNL e l'eventuale maggiore valore delle medesime retribuzioni successivamente stabilito dagli enti ai sensi dell'articolo 15, commi 2 e 3, del medesimo CCNL, attribuito a valere sui risparmi conseguenti all'utilizzo parziale delle risorse che possono essere destinate alle assunzioni di personale a tempo indeterminato che sono contestualmente ridotte del corrispondente valore finanziario.

3. E' costituito presso il Ministero dell'economia e delle finanze un tavolo tecnico-politico cui partecipano rappresentanti dell'Associazione nazionale dei comuni italiani (ANCI) e tecnici dei Dipartimenti del tesoro e della Ragioneria generale dello Stato del Ministero dell'economia e delle finanze, nonche' del Dipartimento per gli affari interni e territoriali del Ministero dell'interno, da individuare entro dieci giorni dalla data di entrata in vigore della legge di conversione del presente decreto, con il compito di formulare proposte per la ristrutturazione, senza nuovi o maggiori oneri per la finanza pubblica, del debito gravante sugli enti locali in considerazione della durata delle posizioni debitorie e dell'andamento dei tassi correntemente praticati nel mercato del credito rivolto agli enti locali. Ai partecipanti al tavolo di cui al presente comma non spettano gettoni di presenza o emolumenti a qualsiasi titolo dovuti, ne' rimborsi spese.

4. Al primo periodo del comma 866 dell'articolo 1 della legge 27 dicembre 2017, n. 205, le parole: "Per gli anni dal 2018 al 2020" sono soppresse.

5. All'articolo 4 del decreto-legge 24 giugno 2016, n. 113, convertito, con modificazioni, dalla legge 7 agosto 2016, n. 160, il comma 2 e' sostituito dal seguente:

"2. I comuni di cui al comma 1 comunicano al Ministero dell'interno, entro il termine perentorio di quindici giorni successivi alla data di entrata in vigore della legge di conversione del presente decreto per l'anno 2016, entro il 31 marzo per ciascuno degli anni dal 2017 al 2018, ed entro il 20 dicembre 2019 per l'anno 2019, la sussistenza della fattispecie di cui comma 1, ivi incluse le richieste non soddisfatte negli anni precedenti, con modalita'

telematiche individuate dal Ministero dell'interno. Le richieste sono soddisfatte per l'intero importo. La ripartizione del Fondo avviene con decreto del Presidente del Consiglio dei ministri, su proposta del Ministro dell'interno, di concerto con il Ministro dell'economia e finanze, sentita la Conferenza Stato-citta' ed autonomie locali, da adottare entro novanta giorni dal termine di invio delle richieste. Nel caso in cui l'ammontare delle richieste superi l'ammontare annuo complessivamente assegnato, le risorse sono attribuite proporzionalmente".

6. I comuni, le province e le citta' metropolitane possono ripartire l'eventuale disavanzo, conseguente all'operazione di stralcio dei crediti fino a 1.000 euro affidati agli agenti della riscossione prevista dall'articolo 4 del decreto-legge 23 ottobre 2018, n. 119, convertito, con modificazioni, dalla legge 17 dicembre 2018, n. 136, in un numero massimo di cinque annualita' in quote costanti. L'importo del disavanzo ripianabile in cinque anni non puo' essere superiore alla sommatoria dei residui attivi cancellati per effetto dell'operazione di stralcio al netto dell'accantonamento al fondo crediti di dubbia esigibilita' nel risultato di amministrazione.

7. Al comma 855 dell'articolo 1 della legge 30 dicembre 2018, n. 145, le parole: "entro il termine del 15 dicembre 2019" sono sostituite dalle seguenti: "entro il termine del 30 dicembre 2019".

8. Dopo il comma 895 dell'articolo 1 della legge 30 dicembre 2018, n. 145, sono inseriti i seguenti:

"895-bis. A titolo di ristoro del gettito non piu' acquisibile dai comuni a seguito dell'introduzione della TASI di cui al comma 639 dell'articolo 1 della legge 27 dicembre 2013, n. 147, e' attribuito ai comuni interessati un contributo complessivo di 110 milioni di euro per l'anno 2019, da ripartire con decreto del Ministero dell'interno di concerto con il Ministero dell'economia e delle finanze, previa intesa in sede di Conferenza Stato-citta' ed autonomie locali, da emanare entro il 30 aprile 2019, in proporzione al peso del contributo di ciascun ente di cui alla tabella B allegata al decreto del Presidente del Consiglio dei ministri 10 marzo 2017, pubblicato nel supplemento ordinario alla Gazzetta Ufficiale n. 123 del 29 maggio 2017.

895-ter. All'onere di cui al comma 895-bis, pari a 110 milioni di euro per l'anno 2019, si provvede:

a) quanto a 90 milioni di euro, mediante corrispondente riduzione del Fondo di cui all'articolo 1, comma 255;

b) quanto a 10 milioni di euro, mediante corrispondente riduzione del Fondo per interventi strutturali di politica economica, di cui all'articolo 10, comma 5, del decreto-legge 29 novembre 2004, n. 282, convertito, con modificazioni, dalla legge 27 dicembre 2004, n. 307;

c) quanto a 10 milioni di euro, mediante corrispondente riduzione del fondo derivante dal riaccertamento dei residui passivi ai sensi dell'articolo 49, comma 2, lettera a), del decreto-legge 24 aprile 2014, n. 66, convertito, con modificazioni, dalla legge 23 giugno 2014, n. 89, iscritto nello stato di previsione del Ministero dell'economia e delle finanze".

9. Nelle more dell'intesa di cui al punto 5 dell'accordo sottoscritto il 30 gennaio 2018 tra il Presidente del Consiglio dei ministri, il Ministro dell'economia e delle finanze e il Presidente della regione Friuli Venezia Giulia, il fondo di cui all'articolo 1, comma 748, della legge 30 dicembre 2018, n. 145, e' integrato di 71,8 milioni di euro per l'anno 2019 e di 86,1 milioni di euro a decorrere

dall'anno 2020, mediante corrispondente utilizzo delle maggiori entrate derivanti dai commi da 11 a 15.

10. All'articolo 1 della legge 30 dicembre 2018, n. 145, sono apportate le seguenti modificazioni:

a) al comma 126, le parole: "31 gennaio 2019" sono sostituite dalle seguenti: "15 marzo 2019", le parole: "20 febbraio 2019" sono sostituite dalle seguenti: "31 marzo 2019" e le parole: "10 marzo 2019" sono sostituite dalle seguenti: "15 aprile 2019";

b) ai commi 824 e 842, le parole: "dai commi 98 e 126" sono sostituite dalle seguenti: "dal comma 98";

c) al comma 875, le parole: "31 gennaio 2019" sono sostituite dalle seguenti: "15 marzo 2019".

11. Se un soggetto passivo facilita, tramite l'uso di un'interfaccia elettronica quale un mercato virtuale, una piattaforma, un portale o mezzi analoghi, le vendite a distanza di telefoni cellulari, console da gioco, tablet PC e laptop, importati da territori terzi o Paesi terzi, di valore intrinseco non superiore a euro 150, si considera che lo stesso soggetto passivo abbia ricevuto e ceduto detti beni.

12. Se un soggetto passivo facilita, tramite l'uso di un'interfaccia elettronica quale un mercato virtuale, una piattaforma, un portale o mezzi analoghi, le cessioni di telefoni cellulari, console da gioco, tablet PC e laptop, effettuate nell'Unione europea da un soggetto passivo non stabilito nell'Unione europea a una persona che non e' un soggetto passivo, si considera che lo stesso soggetto passivo che facilita la cessione abbia ricevuto e ceduto detti beni.

13. Ai fini dell'applicazione dei commi 11 e 12, si presume che la persona che vende i beni tramite l'interfaccia elettronica sia un soggetto passivo e la persona che acquista tali beni non sia un soggetto passivo.

14. Il soggetto passivo che facilita le vendite a distanza ai sensi dei commi 11 e 12 e' tenuto a conservare la documentazione relativa a tali vendite. Tale documentazione deve essere dettagliata in modo sufficiente da consentire alle amministrazioni fiscali degli Stati membri dell'Unione europea in cui tali cessioni sono imponibili di verificare che l'IVA sia stata contabilizzata in modo corretto, deve, su richiesta, essere messa a disposizione per via elettronica degli Stati membri interessati e deve essere conservata per un periodo di dieci anni a partire dal 31 dicembre dell'anno in cui l'operazione e' stata effettuata.

15. Il soggetto passivo che facilita le vendite a distanza ai sensi dei commi 11 e 12 e' tenuto a designare un intermediario che agisce in suo nome e per suo conto, se stabilito in un Paese con il quale l'Italia non ha concluso un accordo di assistenza reciproca.

16. Il comma 895 dell'articolo 1 della legge 30 dicembre 2018, n. 145, e' abrogato.

17. Al fine di potenziare ulteriormente gli interventi in materia di sicurezza urbana per la realizzazione degli obiettivi di cui all'articolo 5, comma 2, lettera a), del decreto-legge 20 febbraio 2017, n. 14, convertito, con modificazioni, dalla legge 18 aprile 2017, n. 48, con riferimento all'installazione, da parte dei comuni, di sistemi di videosorveglianza, l'autorizzazione di spesa di cui all'articolo 5, comma 2-ter, del citato decreto-legge n. 14 del 2017 e' incrementata di 20 milioni di euro per l'anno 2019.

18. All'onere di cui al comma 17 si provvede mediante utilizzo delle risorse iscritte, per l'anno 2019, nel fondo per il federalismo amministrativo di parte corrente, di cui alla legge 15 marzo 1997, n.

59, dello stato di previsione del Ministero dell'interno. Il Ministro dell'economia e delle finanze e' autorizzato ad apportare, con propri decreti, le occorrenti variazioni di bilancio.

19. Con decreto del Ministro dell'interno, di concerto con il Ministro dell'economia e delle finanze, da adottare entro il 31 marzo di ciascun anno di riferimento, sono definite le modalita' di presentazione delle richieste da parte dei comuni interessati nonche' i criteri di ripartizione delle ulteriori risorse di cui al comma 1 dell'articolo 35-quinquies del decreto-legge 4 ottobre 2018, n. 113, convertito, con modificazioni, dalla legge 1° dicembre 2018, n. 132, relativamente agli anni 2020, 2021 e 2022.

Art. 11-ter (Piano per la transizione energetica sostenibile delle aree idonee). - 1. Entro diciotto mesi dalla data di entrata in vigore della legge di conversione del presente decreto, con decreto del Ministro dello sviluppo economico, di concerto con il Ministro dell'ambiente e della tutela del territorio e del mare, e' approvato il Piano per la transizione energetica sostenibile delle aree idonee (PiTESAI), al fine di individuare un quadro definito di riferimento delle aree ove e' consentito lo svolgimento delle attivita' di prospezione, ricerca e coltivazione di idrocarburi sul territorio nazionale, volto a valorizzare la sostenibilita' ambientale, sociale ed economica delle stesse.

2. Il PiTESAI deve tener conto di tutte le caratteristiche del territorio, sociali, industriali, urbanistiche e morfologiche, con particolare riferimento all'assetto idrogeologico ed alle vigenti pianificazioni e, per quanto riguarda le aree marine, deve principalmente considerare i possibili effetti sull'ecosistema, nonche' tenere conto dell'analisi delle rotte marittime, della pescosita' delle aree e della possibile interferenza sulle coste. Nel PiTESAI devono altresi' essere indicati tempi e modi di dismissione e rimessa in pristino dei luoghi da parte delle relative installazioni che abbiano cessato la loro attivita'.

3. Il PiTESAI e' adottato previa valutazione ambientale strategica e, limitatamente alle aree su terraferma, d'intesa con la Conferenza unificata. Qualora per le aree su terraferma l'intesa non sia raggiunta entro sessanta giorni dalla prima seduta, la Conferenza unificata e' convocata in seconda seduta su richiesta del Ministro dello sviluppo economico entro trenta giorni, ai sensi dell'articolo 8, comma 4, del decreto legislativo 28 agosto 1997, n. 281. In caso di mancato raggiungimento dell'intesa entro il termine di centoventi giorni dalla seconda seduta, ovvero in caso di espresso e motivato dissenso della Conferenza unificata, il PiTESAI e' adottato con riferimento alle sole aree marine.

4. Nelle more dell'adozione del PiTESAI, ai fini della salvaguardia e del miglioramento della sostenibilita' ambientale e sociale, i procedimenti amministrativi, ivi inclusi quelli di valutazione di impatto ambientale, relativi al conferimento di nuovi permessi di prospezione o di ricerca di idrocarburi liquidi e gassosi sono sospesi, fatti salvi i seguenti procedimenti in corso o avviati successivamente alla data di entrata in vigore della legge di conversione del presente decreto, relativi a istanze di:

a) proroga di vigenza delle concessioni di coltivazione di idrocarburi in essere;

b) rinuncia a titoli minerari vigenti o alle relative proroghe;

c) sospensione temporale della produzione per le concessioni in essere;

d) riduzione dell'area, variazione dei programmi lavori e delle quote di titolarita'.

5. La sospensione di cui al comma 4 non si applica ai procedimenti relativi al conferimento di concessioni di coltivazione di idrocarburi liquidi e gassosi pendenti alla data di entrata in vigore della legge di conversione del presente decreto. Nelle more dell'adozione del PiTESAI, non e' consentita la presentazione di nuove istanze di conferimento di concessioni di coltivazione, fatto salvo quanto previsto dal comma 4, lettera a).

6. A decorrere dalla data di entrata in vigore della legge di conversione del presente decreto e fino all'adozione del PiTESAI, i permessi di prospezione o di ricerca di idrocarburi liquidi e gassosi in essere, sia per aree in terraferma che in mare, sono sospesi, con conseguente interruzione di tutte le attivita' di prospezione e ricerca in corso di esecuzione, fermo restando l'obbligo di messa in sicurezza dei siti interessati dalle stesse attivita'.

7. La sospensione di cui al comma 6 sospende anche il decorso temporale dei permessi di prospezione e di ricerca, ai fini del computo della loro durata; correlativamente, per lo stesso periodo di sospensione, non e' dovuto il pagamento del relativo canone. Ai relativi oneri, valutati in 134.000 euro in ragione d'anno, si provvede, ai sensi del comma 12, mediante utilizzo delle maggiori entrate di cui al comma 9 che restano acquisite all'erario.

8. Alla data di adozione del PiTESAI, nelle aree in cui le attivita' di prospezione e di ricerca e di coltivazione risultino compatibili con le previsioni del Piano stesso, i titoli minerari sospesi ai sensi del comma 6 riprendono efficacia. Nelle aree non compatibili, il Ministero dello sviluppo economico rigetta le istanze relative ai procedimenti sospesi ai sensi del comma 4 e revoca, anche limitatamente ad aree parziali, i permessi di prospezione e di ricerca in essere. In caso di revoca, il titolare del permesso di prospezione o di ricerca e' comunque obbligato al completo ripristino dei siti interessati. Nelle aree non compatibili, il Ministero dello sviluppo economico rigetta anche le istanze relative ai procedimenti di rilascio delle concessioni per la coltivazione di idrocarburi il cui provvedimento di conferimento non sia stato rilasciato entro la data di adozione del PiTESAI. In caso di mancata adozione del PiTESAI entro ventiquattro mesi dalla data di entrata in vigore della legge di conversione del presente decreto, i procedimenti sospesi ai sensi del comma 4 proseguono nell'istruttoria ed i permessi di prospezione e di ricerca sospesi ai sensi del comma 6 riprendono efficacia. Alla data di adozione del PiTESAI, nelle aree in cui le attivita' di coltivazione risultino incompatibili con le previsioni del Piano stesso, le concessioni di coltivazione, anche in regime di proroga, vigenti alla data di entrata in vigore della legge di conversione del presente decreto, mantengono la loro efficacia sino alla scadenza e non sono ammesse nuove istanze di proroga.

9. A decorrere dal 1° giugno 2019, i canoni annui di cui all'articolo 18, comma 1, del decreto legislativo 25 novembre 1996, n. 625, per le concessioni di coltivazione e stoccaggio nella terraferma, nel mare territoriale e nella piattaforma continentale italiana sono rideterminati come segue:

a) concessione di coltivazione: 1.481,25 euro per chilometro quadrato;

b) concessione di coltivazione in proroga: 2.221,75 euro per chilometro quadrato;

c) concessione di stoccaggio insistente sulla relativa concessione di coltivazione: 14,81 euro per chilometro quadrato;

d) concessione di stoccaggio in assenza di relativa concessione di coltivazione: 59,25 euro per chilometro quadrato.

10. Al venir meno della sospensione di cui al comma 6, i canoni annui di cui all'articolo 18, comma 1, del decreto legislativo 25 novembre 1996, n. 625, per i permessi di prospezione e ricerca sono rideterminati come segue:

a) permesso di prospezione: 92,50 euro per chilometro quadrato;

b) permesso di ricerca: 185,25 euro per chilometro quadrato;

c) permesso di ricerca in prima proroga: 370,25 euro per chilometro quadrato;

d) permesso di ricerca in seconda proroga: 740,50 euro per chilometro quadrato.

11. E' autorizzata la spesa di 1 milione di euro per ciascuno degli anni 2019 e 2020, da iscrivere su apposito capitolo dello stato di previsione del Ministero dello sviluppo economico per far fronte agli oneri connessi alla predisposizione del PiTESAI.

12. Per far fronte agli altri oneri derivanti dal presente articolo, e' istituito nello stato di previsione del Ministero dello sviluppo economico un fondo con dotazione di 15 milioni di euro a decorrere dall'anno 2020. Le maggiorazioni dei canoni di superficie derivanti dalle disposizioni di cui ai commi 9 e 10 sono versate ad apposito capitolo dell'entrata del bilancio dello Stato per essere riassegnate, con decreto del Ministro dell'economia e delle finanze, al fondo di cui al periodo precedente, per gli importi eccedenti 1,134 milioni di euro per l'anno 2019, 16,134 milioni di euro per l'anno 2020 e 15,134 milioni di euro a decorrere dall'anno 2021. Con decreto del Ministro dell'economia e delle finanze, di concerto con il Ministro dello sviluppo economico, sono stabilite le modalita' di versamento delle maggiorazioni dei canoni. Nel caso in cui le risorse disponibili sul fondo per un esercizio finanziario non risultino sufficienti per far fronte agli oneri di cui al presente articolo, con decreto del Ministro dello sviluppo economico, di concerto con il Ministro dell'economia e delle finanze, sono corrispondentemente rimodulati i canoni annui di cui all'articolo 18, comma 1, del decreto legislativo 25 novembre 1996, n. 625, al fine di assicurare un maggior gettito corrispondente ai maggiori oneri.

13. Alle attivita' di prospezione, ricerca e coltivazione di idrocarburi svolte nell'ambito di titoli minerari rilasciati a seguito di istanze presentate dopo la data di entrata in vigore della legge di conversione del presente decreto non si applica l'articolo 38, comma 1, del decreto-legge 12 settembre 2014, n. 133, convertito, con modificazioni, dalla legge 11 novembre 2014, n. 164. Resta fermo il carattere di pubblica utilita' delle attivita' di stoccaggio di gas naturale in sotterraneo.

Art. 11-quater (Disposizioni in materia di concessioni di grandi derivazioni idroelettriche). - 1. Al fine di definire una disciplina efficiente e coerente con le disposizioni dell'ordinamento dell'Unione europea in tema di assegnazione delle concessioni di grandi derivazioni idroelettriche, di cui all'articolo 6, comma 2, del testo unico di cui al regio decreto 11 dicembre 1933, n. 1775:

a) all'articolo 12 del decreto legislativo 16 marzo 1999, n. 79, i commi 1 e 1-bis sono sostituiti dai seguenti:

"1. Alla scadenza delle concessioni di grandi derivazioni idroelettriche e nei casi di decadenza o rinuncia, le opere di cui all'articolo 25, primo comma, del testo unico di cui al regio decreto 11 dicembre 1933, n. 1775, passano, senza compenso, in proprieta' delle regioni, in stato di regolare funzionamento. In caso di esecuzione da parte del concessionario, a proprie spese e nel periodo di validita' della concessione, di investimenti sui beni di cui al primo periodo, purche' previsti dall'atto di concessione o comunque

autorizzati dal concedente, alla riassegnazione della concessione secondo le procedure di cui ai commi seguenti, e' riconosciuto al concessionario uscente, per la parte di bene non ammortizzato, un indennizzo pari al valore non ammortizzato, fermo restando quanto previsto dall'articolo 26 del testo unico di cui al regio decreto n. 1775 del 1933. Per i beni diversi da quelli previsti dai periodi precedenti si applica la disciplina stabilita dall'articolo 25, commi secondo e seguenti, del testo unico di cui al regio decreto n. 1775 del 1933, con corresponsione del prezzo da quantificare al netto dei beni ammortizzati, sulla base del comma 1-ter del presente articolo, intendendosi sostituiti gli organi statali ivi indicati con i corrispondenti organi della regione.

1-bis. Le regioni, ove non ritengano sussistere un prevalente interesse pubblico ad un diverso uso delle acque, incompatibile con il mantenimento dell'uso a fine idroelettrico, possono assegnare le concessioni di grandi derivazioni idroelettriche, previa verifica dei requisiti di capacita' tecnica, finanziaria e organizzativa di cui al comma 1-ter, lettera d): a) ad operatori economici individuati attraverso l'espletamento di gare con procedure ad evidenza pubblica; b) a societa' a capitale misto pubblico privato nelle quali il socio privato e' scelto attraverso l'espletamento di gare con procedure ad evidenza pubblica; c) mediante forme di partenariato ai sensi degli articoli 179 e seguenti del codice di cui al decreto legislativo 18 aprile 2016, n. 50. L'affidamento a societa' partecipate deve comunque avvenire nel rispetto delle disposizioni del testo unico di cui al decreto legislativo 19 agosto 2016, n. 175.

1-ter. Nel rispetto dell'ordinamento dell'Unione europea e degli accordi internazionali, nonche' dei principi fondamentali dell'ordinamento statale e delle disposizioni di cui al presente articolo, le regioni disciplinano con legge, entro un anno dalla data di entrata in vigore della presente disposizione e comunque non oltre il 31 marzo 2020, le modalita' e le procedure di assegnazione delle concessioni di grandi derivazioni d'acqua a scopo idroelettrico, stabilendo in particolare:

a) le modalita' per lo svolgimento delle procedure di assegnazione di cui al comma 1-bis;

b) i termini di avvio delle procedure di cui al comma 1-bis;

c) i criteri di ammissione e di assegnazione;

d) la previsione che l'eventuale indennizzo e' posto a carico del concessionario subentrante;

e) i requisiti di capacita' finanziaria, organizzativa e tecnica adeguata all'oggetto della concessione richiesti ai partecipanti e i criteri di valutazione delle proposte progettuali, prevedendo quali requisiti minimi:

1) ai fini della dimostrazione di adeguata capacita' organizzativa e tecnica, l'attestazione di avvenuta gestione, per un periodo di almeno cinque anni, di impianti idroelettrici aventi una potenza nominale media pari ad almeno 3 MW;

2) ai fini della dimostrazione di adeguata capacita' finanziaria, la referenza di due istituti di credito o societa' di servizi iscritti nell'elenco generale degli intermediari finanziari che attestino che il partecipante ha la possibilita' di accedere al credito per un importo almeno pari a quello del progetto proposto nella procedura di assegnazione, ivi comprese le somme da corrispondere per i beni di cui alla lettera n);

f) i termini di durata delle nuove concessioni, comprese tra venti anni e quaranta anni; il termine massimo puo' essere incrementato fino ad un massimo di dieci anni, in relazione alla

complessita' della proposta progettuale presentata e all'importo dell'investimento;

g) gli obblighi o le limitazioni gestionali, subordinatamente ai quali sono ammissibili i progetti di sfruttamento e utilizzo delle opere e delle acque, compresa la possibilita' di utilizzare l'acqua invasata per scopi idroelettrici per fronteggiare situazioni di crisi idrica o per la laminazione delle piene;

h) i miglioramenti minimi in termini energetici, di potenza di generazione e di producibilita' da raggiungere nel complesso delle opere di derivazione, adduzione, regolazione e condotta dell'acqua e degli impianti di generazione, trasformazione e connessione elettrica con riferimento agli obiettivi strategici nazionali in materia di sicurezza energetica e fonti energetiche rinnovabili, compresa la possibilita' di dotare le infrastrutture di accumulo idrico per favorire l'integrazione delle stesse energie rinnovabili nel mercato dell'energia e nel rispetto di quanto previsto dal codice di trasmissione, dispacciamento, sviluppo e sicurezza della rete elettrica di cui all'articolo 1, comma 4, del decreto del Presidente del Consiglio dei ministri 11 maggio 2004, pubblicato nella Gazzetta Ufficiale n. 115 del 18 maggio 2004, e dai suoi aggiornamenti;

i) i livelli minimi in termini di miglioramento e risanamento ambientale del bacino idrografico di pertinenza, in coerenza con gli strumenti di pianificazione a scala di distretto idrografico in attuazione della direttiva 2000/60/CE del Parlamento europeo e del Consiglio, del 23 ottobre 2000, determinando obbligatoriamente una quota degli introiti derivanti dall'assegnazione, da destinare al finanziamento delle misure dei piani di gestione distrettuali o dei piani di tutela finalizzate alla tutela e al ripristino ambientale dei corpi idrici interessati dalla derivazione;

l) le misure di compensazione ambientale e territoriale, anche a carattere finanziario, da destinare ai territori dei comuni interessati dalla presenza delle opere e della derivazione compresi tra i punti di presa e di restituzione delle acque garantendo l'equilibrio economico finanziario del progetto di concessione;

m) le modalita' di valutazione, da parte dell'amministrazione competente, dei progetti presentati in esito alle procedure di assegnazione, che avviene nell'ambito di un procedimento unico ai fini della selezione delle proposte progettuali presentate, che tiene luogo della verifica o valutazione di impatto ambientale, della valutazione di incidenza nei confronti dei siti di importanza comunitaria interessati e dell'autorizzazione paesaggistica, nonche' di ogni altro atto di assenso, concessione, permesso, licenza o autorizzazione, comunque denominato, previsto dalla normativa statale, regionale o locale; a tal fine, alla valutazione delle proposte progettuali partecipano, ove necessario, il Ministero dell'ambiente e della tutela del territorio e del mare, il Ministero dello sviluppo economico, il Ministero per i beni e le attivita' culturali e gli enti gestori delle aree naturali protette di cui alla legge 6 dicembre 1991, n. 394; per gli aspetti connessi alla sicurezza degli invasi di cui al decreto-legge 8 agosto 1994, n. 507, convertito, con modificazioni, dalla legge 21 ottobre 1994, n. 584, e all'articolo 6, comma 4-bis, della legge 1° agosto 2002, n. 166, al procedimento valutativo partecipa il Ministero delle infrastrutture e dei trasporti;

n) l'utilizzo dei beni di cui all'articolo 25, secondo comma, del testo unico di cui al regio decreto n. 1775 del 1933, nel rispetto del codice civile, secondo i seguenti criteri:

1) per i beni mobili di cui si prevede l'utilizzo nel

progetto di concessione, l'assegnatario corrisponde agli aventi diritto, all'atto del subentro, un prezzo, in termini di valore residuo, determinato sulla base dei dati reperibili dagli atti contabili o mediante perizia asseverata; in caso di mancata previsione di utilizzo nel progetto di concessione, per tali beni si procede alla rimozione e allo smaltimento secondo le norme vigenti a cura ed onere del proponente;

2) per i beni immobili dei quali il progetto proposto prevede l'utilizzo, l'assegnatario corrisponde agli aventi diritto, all'atto del subentro, un prezzo il cui valore e' determinato sulla base dei dati reperibili dagli atti contabili o mediante perizia asseverata sulla base di attivita' negoziale tra le parti;

3) i beni immobili dei quali il progetto proposto non prevede l'utilizzo restano di proprieta' degli aventi diritto;

o) la previsione, nel rispetto dei principi dell'Unione europea, di specifiche clausole sociali volte a promuovere la stabilita' occupazionale del personale impiegato;

p) le specifiche modalita' procedimentali da seguire in caso di grandi derivazioni idroelettriche che interessano il territorio di due o piu' regioni, in termini di gestione delle derivazioni, vincoli amministrativi e ripartizione dei canoni, da definire d'intesa tra le regioni interessate; le funzioni amministrative per l'assegnazione della concessione sono di competenza della regione sul cui territorio insiste la maggior portata di derivazione d'acqua in concessione.

1-quater. Le procedure di assegnazione delle concessioni di grandi derivazioni idroelettriche sono avviate entro due anni dalla data di entrata in vigore della legge regionale di cui al comma 1-ter. Con decreto del Ministro dello sviluppo economico, di concerto con il Ministro dell'ambiente e della tutela del territorio e del mare e con il Ministro delle infrastrutture e dei trasporti, previa intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, da adottare entro il 31 dicembre 2021, sono individuate le modalita' e le procedure di assegnazione applicabili nell'ipotesi di mancato rispetto del termine di avvio, da parte della regione interessata, delle procedure di cui al primo periodo; il Ministero delle infrastrutture e dei trasporti, in applicazione dell'articolo 8 della legge 5 giugno 2003, n. 131, procede in via sostitutiva, sulla base della predetta disciplina, all'assegnazione delle concessioni, prevedendo che il 10 per cento dell'importo dei canoni concessori, in deroga all'articolo 89, comma 1, lettera i), del decreto legislativo 31 marzo 1998, n. 112, resti acquisita al patrimonio statale. Restano in ogni caso ferme le competenze statali di cui al decreto-legge 8 agosto 1994, n. 507, convertito, con modificazioni, dalla legge 21 ottobre 1994, n. 584, e di cui alla legge 1° agosto 2002, n. 166.

1-quinquies. I concessionari di grandi derivazioni idroelettriche corrispondono semestralmente alle regioni un canone, determinato con legge regionale, sentita l'Autorita' di regolazione per energia, reti e ambiente (ARERA), articolato in una componente fissa, legata alla potenza nominale media di concessione, e in una componente variabile, calcolata come percentuale dei ricavi normalizzati, sulla base del rapporto tra la produzione dell'impianto, al netto dell'energia fornita alla regione ai sensi del presente comma, ed il prezzo zonale dell'energia elettrica. Il compenso unitario di cui al precedente periodo varia proporzionalmente alle variazioni, non inferiori al 5 per cento, dell'indice ISTAT relativo al prezzo industriale per la produzione, il trasporto e la distribuzione dell'energia elettrica. Il canone cosi' determinato e' destinato per almeno il 60 per cento

alle province e alle citta' metropolitane il cui territorio e' interessato dalle derivazioni. Nelle concessioni di grandi derivazioni a scopo idroelettrico, le regioni possono disporre con legge l'obbligo per i concessionari di fornire annualmente e gratuitamente alle stesse regioni 220 kWh per ogni kW di potenza nominale media di concessione, per almeno il 50 per cento destinata a servizi pubblici e categorie di utenti dei territori provinciali interessati dalle derivazioni.

1-sexies. Per le concessioni di grandi derivazioni idroelettriche che prevedono un termine di scadenza anteriore al 31 dicembre 2023, ivi incluse quelle gia' scadute, le regioni che non abbiano gia' provveduto disciplinano con legge, entro un anno dalla data di entrata in vigore della presente disposizione e comunque non oltre il 31 marzo 2020, le modalita', le condizioni, la quantificazione dei corrispettivi aggiuntivi e gli eventuali altri oneri conseguenti, a carico del concessionario uscente, per la prosecuzione, per conto delle regioni stesse, dell'esercizio delle derivazioni, delle opere e degli impianti oltre la scadenza della concessione e per il tempo necessario al completamento delle procedure di assegnazione e comunque non oltre il 31 dicembre 2023.

1-septies. Fino all'assegnazione della concessione, il concessionario scaduto e' tenuto a fornire, su richiesta della regione, energia nella misura e con le modalita' previste dal comma 1-quinquies e a riversare alla regione un canone aggiuntivo, rispetto al canone demaniale, da corrispondere per l'esercizio degli impianti nelle more dell'assegnazione; tale canone aggiuntivo e' destinato per un importo non inferiore al 60 per cento alle province e alle citta' metropolitane il cui territorio e' interessato dalle derivazioni. Con decreto del Ministro dello sviluppo economico, sentita l'ARERA e previo parere della Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano, sono determinati il valore minimo della componente fissa del canone di cui al comma 1-quinquies e il valore minimo del canone aggiuntivo di cui al precedente periodo; in caso di mancata adozione del decreto entro il termine di centottanta giorni dalla data di entrata in vigore della presente disposizione, fermi restando i criteri di ripartizione di cui al presente comma e al comma 1-quinquies, le regioni possono determinare l'importo dei canoni di cui al periodo precedente in misura non inferiore a 30 euro per la componente fissa del canone e a 20 euro per il canone aggiuntivo per ogni kW di potenza nominale media di concessione per ogni annualita'.

1-octies. Sono fatte salve le competenze delle regioni a statuto speciale e delle province autonome di Trento e di Bolzano ai sensi dei rispettivi statuti e delle relative norme di attuazione";

b) i commi 2, 4, 8-bis e 11 dell'articolo 12 del decreto legislativo 16 marzo 1999, n. 79, sono abrogati;

c) i commi 5, 6 e 7 dell'articolo 37 del decreto-legge 22 giugno 2012, n. 83, convertito, con modificazioni, dalla legge 7 agosto 2012, n. 134, sono abrogati.

Art. 11-quinquies (Interpretazione autentica dell'articolo 3, comma 3, secondo periodo, della legge 12 luglio 2017, n. 113, e proroga del termine di cui all'articolo 27, comma 4, della legge 31 dicembre 2012, n. 247). - 1. L'articolo 3, comma 3, secondo periodo, della legge 12 luglio 2017, n. 113, si interpreta nel senso che, ai fini del rispetto del divieto di cui al predetto periodo, si tiene conto dei mandati espletati, anche solo in parte, prima della sua entrata in vigore, compresi quelli iniziati anteriormente all'entrata in vigore della legge 31 dicembre 2012, n. 247. Resta fermo quanto

previsto dall'articolo 3, commi 3, terzo periodo, e 4, della legge 12 luglio 2017, n. 113.

2. Per il rinnovo dei consigli degli ordini circondariali degli avvocati scaduti il 31 dicembre 2018, l'assemblea di cui all'articolo 27, comma 4, secondo periodo, della legge 31 dicembre 2012, n. 247, si svolge entro il mese di luglio 2019.

3. Dall'attuazione del presente articolo non devono derivare nuovi o maggiori oneri a carico della finanza pubblica.

Art. 11-sexies (Disposizioni urgenti in materia di enti del Terzo settore). - 1. All'articolo 4, comma 3, del decreto legislativo 3 luglio 2017, n. 112, dopo le parole: "ai sensi dell'articolo 2359 del codice civile" sono aggiunte le seguenti: ", ad eccezione delle associazioni o fondazioni di diritto privato ex Ipab derivanti dai processi di trasformazione delle istituzioni pubbliche di assistenza o beneficenza, ai sensi del decreto del Presidente del Consiglio dei ministri 16 febbraio 1990, pubblicato nella Gazzetta Ufficiale n. 45 del 23 febbraio 1990, e del decreto legislativo 4 maggio 2001, n. 207, in quanto la nomina da parte della pubblica amministrazione degli amministratori di tali enti si configura come mera designazione, intesa come espressione della rappresentanza della cittadinanza, e non si configura quindi mandato fiduciario con rappresentanza, sicche' e' sempre esclusa qualsiasi norma di controllo da parte di quest'ultima".

2. All'articolo 4, comma 2, del codice di cui al decreto legislativo 3 luglio 2017, n. 117, e' aggiunto, in fine, il seguente periodo: "Sono altresi' escluse dall'ambito di applicazione del presente comma le associazioni o fondazioni di diritto privato ex Ipab derivanti dai processi di trasformazione delle istituzioni pubbliche di assistenza o beneficenza, ai sensi del decreto del Presidente del Consiglio dei ministri 16 febbraio 1990, pubblicato nella Gazzetta Ufficiale n. 45 del 23 febbraio 1990, e del decreto legislativo 4 maggio 2001, n. 207, in quanto la nomina da parte della pubblica amministrazione degli amministratori di tali enti si configura come mera designazione, intesa come espressione della rappresentanza della cittadinanza, e non si configura quindi mandato fiduciario con rappresentanza, sicche' e' sempre esclusa qualsiasi forma di controllo da parte di quest'ultima".

Art. 11-septies (Modifica all'articolo 3 della legge 3 marzo 2009, n. 18, nonche' disposizioni in favore degli orfani di Rigopiano) - 1. All'articolo 3, comma 3, ultimo periodo, della legge 3 marzo 2009, n. 18, le parole: "non superiore" sono sostituite dalla seguente: "pari".

2. Con riferimento al disastro di Rigopiano del 18 gennaio 2017, sono considerati orfani tutti coloro i cui genitori, o anche un solo genitore, ovvero la persona che li aveva a proprio totale o principale carico, siano deceduti, dispersi o divenuti permanentemente inabili a qualsiasi proficuo lavoro a causa del predetto evento. Ai predetti orfani sono riconosciute le seguenti forme di protezione, assistenza e agevolazione:

a) attribuzione agli orfani di un genitore o di entrambi della quota di riserva di cui all'articolo 7, comma 2, della legge 12 marzo 1999, n. 68;

b) riconoscimento della condizione di orfano, ai sensi del presente comma, quale titolo di preferenza nella valutazione dei requisiti prescritti per le assunzioni nelle amministrazioni dello Stato e negli enti pubblici non attuate tramite concorso. Ai medesimi orfani si applicano le disposizioni di cui all'articolo 1, comma 2,

della legge 23 novembre 1998, n. 407, relativamente all'iscrizione negli elenchi al collocamento obbligatorio».

ANNEXE N°3

N° 237

Le 4 décembre 2017

PROPOSITION DE LOI

DE M. Thierry POYET,

RELATIVE A LA BLOCKCHAIN

EXPOSE DES MOTIFS

Technologie encore relativement récente, la blockchain est en passe de devenir un outil majeur du développement informatique, certains n'hésitant pas à considérer que son apport sera comparable à celui de l'Internet. A ce titre, il faut reconnaître que les développements consacrés à la blockchain prennent une ampleur considérable et que les potentialités offertes paraissent illimitées.

La blockchain reste néanmoins perçue comme quelque chose de complexe et de difficilement accessible, ce qui est vrai si l'on s'intéresse à la technique, mais qui l'est un peu moins si l'on se focalise sur ses atouts et ses utilisations potentielles. En outre, et à l'instar de toute innovation technologique majeure, elle suscite des craintes et soulève des interrogations, au demeurant fort légitimes. Ceci est accentué, tant par la philosophie même de la blockchain qui se présente comme une technologie disruptive, donc, littéralement, qui a la volonté de provoquer une rupture par rapport à divers modes de fonctionnement existant, que par certains événements qui ont pu affecter son image.

Pour autant, il faut bien avoir à l'esprit qu'une technologie est par principe neutre et que c'est l'utilisation qui en est faite qui peut, ou non, être sujette à discussion et nécessiter de poser des garde-fous. En toute hypothèse, la volonté clairement affichée de la présente proposition de loi est précisément d'ouvrir la discussion et de permettre l'expérimentation, de manière à poser les jalons d'une régulation à venir.

C'est pourquoi, sans prétendre donner une parfaite définition de ce qu'est la blockchain, une brève description de son fonctionnement semble utile pour introduire la présente proposition de loi.

Ainsi, on commencera par rappeler que la blockchain n'est, en réalité, pas une complète nouveauté, si l'on observe les technologies sur lesquelles elle repose, et notamment le système de partage « pair-à-pair » ou encore le recours à des clés cryptographiques asymétriques, c'est-à-dire clé publique et clé privée. L'innovation majeure réside donc dans la combinaison de ces diverses technologies, afin de créer un registre décentralisé, partagé et sécurisé.

On pourrait ainsi dire que la blockchain est un registre retraçant et collectant les transactions de ses utilisateurs. Une transaction est ainsi inscrite de manière cryptée par ces derniers au moyen d'une clé publique et d'une clé privée. Elle ne peut donc être effacée ou modifiée. Cette transaction figure au sein d'un « bloc » qui doit pouvoir être relié aux autres qui précèdent. Pour être reliée, ce qui va conduire à son horodatage et à l'attribution de son caractère infalsifiable, la transaction doit être validée par un système de consensus, lequel sera réalisé par les différents ordinateurs connectés en réseau « pair-à-pair ».

On s'aperçoit ainsi que, plus la blockchain comporte de membres, plus elle sera sécurisée, dans la mesure où le processus de certification – décentralisé – repose sur la validation majoritaire et qu'il est complexe de pouvoir contrôler autant d'utilisateurs. Il faut ici bien comprendre que la transaction est publique : la clé publique permettant d'accéder à la blockchain étant précisément connue de tous. En revanche, la clé privée, laquelle permet en quelque sorte de signer la transaction, est personnelle et confidentielle, de sorte que les membres de la blockchain ne connaîtront pas les auteurs de la transaction.

Ceci met en exergue les caractéristiques de la blockchain : une organisation partagée par chaque utilisateur, sécurisée par eux et décentralisée. La fiabilité de la blockchain repose donc, d'une certaine manière, sur le nombre et la transparence.

Du moins est-ce l'hypothèse d'une blockchain dite publique, laquelle, pour les puristes, correspond à la seule et véritable blockchain. Il existe cependant des modèles intermédiaires, lesquelles semblent avoir la préférence du tissu économique, ou au moins du secteur bancaire, en ce qu'elles permettent de réintroduire une forme d'instance centralisée à même de réguler les échanges et qui va, par les conditions générales qu'elle pose, restreindre l'accès à cette blockchain.

La blockchain la plus connue est sans nul doute celle qui a conduit à la création du Bitcoin. Historiquement, elle semble d'ailleurs être la première et son apparition semble déjà relever d'une certaine forme de mythologie, puisque créée par un certain Satochi Nakamoto, dont chacun s'accorde sur le fait qu'il s'agit d'un pseudonyme, et qui aurait enregistré la première transaction en janvier 2009. Cette dernière n'a eu de cesse de se développer depuis et la valeur attribuée au Bitcoin a connu une évolution exponentielle, ce dernier faisant désormais l'objet d'une spéculation importante.

Pour autant, réduire la blockchain au Bitcoin reviendrait, à peu de chose près, à réduire tous les écrits sur support informatique à un logiciel de traitement de texte : ce serait donc confondre l'outil avec la création, le moyen avec l'utilisation. Depuis l'avènement du Bitcoin, la technologie blockchain s'est continuellement développée et ses utilisations vont bien au-delà de la seule crypto-monnaie, laquelle ne révèle aucunement toutes les possibilités de la blockchain.

A ce titre, la doctrine juridique et les professionnels recensent généralement trois grands types de fonctionnalités :

- la transmission dématérialisée ;
- la conservation ;
- la mise en place de « *smart contract* ».

La transmission dématérialisée est la première à avoir été développée, en ce qu'elle correspond au transfert de Bitcoin et, plus généralement, des crypto-monnaies. Pour autant, cela ne se limite nullement à cela et la transmission peut concerner tout titre susceptible de représenter un droit (actions, droit d'auteurs ou même un vote). Ce n'est toutefois pas le point sur lequel il convient d'insister prioritairement.

La fonction de conservation, par la sécurité apportée et par l'existence d'une date certaine (horodatage), dispose d'un potentiel de développement important, susceptible d'avoir des retombées perceptibles pour chacun d'entre nous. C'est d'ailleurs en ce domaine que la blockchain peut marquer une rupture très conséquente, puisque, par la certification ou l'authentification qu'elle confère, elle pourrait être amenée à redéfinir le rôle actuellement joués par les « tiers de confiance ».

On recense ainsi, de par le monde, plusieurs développements possibles, notamment dans les domaines financier, médical, environnemental, juridique ou encore dans la relation entre l'Administration et l'administré :

- la blockchain pourrait accueillir le dossier médical des patients et, simultanément permettre le paiement automatique et instantané des professionnels de santé par les patients, les organismes sociaux et les mutuelles ;
- elle pourrait permettre d'intégrer différents éléments obtenus dans le cadre de la mise en œuvre des vérifications opérées préalablement à l'entrée en relation d'affaires en matière de lutte contre le blanchiment de capitaux ;
- elle permettrait d'assurer la traçabilité de l'approvisionnement en « énergie verte », par exemple pour la fourniture d'électricité ;
- elle pourrait servir d'instrument probatoire, dans la mesure où elle s'apparente à un écrit électronique ;
- elle permettrait la constitution d'un dossier administratif permanent contenant les éléments de l'état civil de la personne et autres pièces justificatives nécessaires à l'accomplissement de formalités administratives, à l'instar d'inscriptions scolaires, de demande de logement ou d'aides sociales ;
- elle peut tenir la fonction d'enregistrant des sociétés, du dépôt du capital social puis de tous changements ultérieurs, le cas échéant après contrôle des autorités, sans autre formalité.

En ce qui concerne les « *smart contracts* », leur développement est plus récent. Si le Bitcoin personnifie presque l'aspect de transaction économique, la blockchain Ethereum est sans nul doute celle qui a permis le développement des « *smart contracts* » et des applications décentralisées. Autant le dire immédiatement, la traduction littérale du « *smart contract* » est réalité trompeuse. En effet, juridiquement, il ne s'agit pas d'un contrat, mais davantage d'une modalité ou d'un aspect de son exécution. En d'autres termes, le « *smart contract* » va servir de support d'exécution à un contrat bien réel.

Son potentiel n'en demeure pas moins particulièrement conséquent. Il repose sur une logique bien connue qui se traduit sous la forme « *if..., then...* ». Selon les cas, le juriste y reconnaîtra un terme ou une condition.

Les exemples d'utilisation généralement cités sont ceux relatifs au transport. Ainsi, on peut imaginer que l'opérateur entre dans la blockchain que le retard ou l'annulation d'un vol ou celui d'un train déclenchera automatiquement le paiement d'une indemnité. On pourrait imaginer que le paiement d'un service par un achat en ligne génèrerait l'envoi de la TVA aux Services Fiscaux, dès la validation de la transaction. De la même manière, en présence d'un événement climatique causant d'importants dégâts, l'indemnisation pourrait être effectuée via la blockchain. Certes, dira-t-on, encore faut-il que l'élément réel, par exemple le retard ou l'événement climatique, puisse être considéré comme établi avec certitude. Aussi la mise en œuvre d'un « *smart contract* » nécessite-t-elle la présence de systèmes d'informations chargées d'intégrer la donnée extérieure à l'intérieur de la blockchain, potentiellement par consensus. On appelle ces systèmes les oracles.

Il ne s'agit en l'espèce que d'un bref échantillon des potentialités de la blockchain. On ne niera pas que ces dernières doivent encore être articulées avec le droit existant et que le chantier est conséquent. Néanmoins, pour quelles raisons cela ne serait-il pas possible ?

Ce qui sera donc déterminant est la manière avec laquelle la Principauté choisira d'appréhender la blockchain. Trois attitudes sont concevables en théorie, mais une seule est en adéquation avec les valeurs de Monaco : sécurité, transparence, modernité, avant-gardisme, entreprenariat…

La première consisterait surtout à ne rien faire. On retrouve fréquemment ce positionnement par la formule « il est urgent d'attendre ». La Principauté perdrait alors toute possibilité de faire partie du peloton de tête des Etats pionniers et avant-gardistes. La course a d'ores et déjà commencé, que l'on songe au Canton suisse de Zoug, à Dubaï, à l'Estonie, à Singapour qui n'hésitent pas à lancer des projets d'envergure et à se montrer « *blockchain friendly* ». Il s'agit d'un enjeu économique, mais aussi de souveraineté numérique. Dès lors, Monaco ne doit pas rester en retrait, cette option serait en contradiction avec la volonté de Monaco d'être un acteur des services numériques, alors que nous venons de lancer l'incubateur monégasque MonacoTech.

La deuxième consisterait à envisager dès à présent la régulation, à partir des premiers exemples de développements étrangers. Cette attitude est rationnelle, mais excessivement prudente et limitée, car faisant fi des particularismes de la Principauté et de la nécessité d'établir un système sur-mesure. En effet, les projets liés à la blockchain à Monaco ne peuvent être les mêmes que ceux d'autres Etats aux dimensions et moyens financiers qui n'ont pas de commune mesure avec les siens. Cela conduirait, en outre, à une perte de temps considérable et à disserter sur des problématiques qui ne concerneront que peu, ou pas du tout, la Principauté, dans un environnement juridique qui est encore bien flou. Cette option serait celle de la volonté de faire, sans se donner l'autorisation ou les moyens d'y aller. Au surplus, la plupart des Etats étrangers adoptent un point de vue pointilliste dans l'élaboration de la réglementation. Pour l'essentiel, ces Etats se focalisent sur les seules activités financières et perdent de vue les potentialités des applications des blockchains.

La troisième et dernière approche serait de favoriser l'expérimentation en sélectionnant des projets à fort potentiel pour la Principauté et à construire la régulation au fur et à mesure de ladite expérimentation, en procédant aussi en parallèle à une veille réglementaire mondiale, et notamment européenne. Il faut citer l'exemple de la France, qui est en train de procéder à la mise en place d'ordonnances, pour réglementer certaines activités financières effectuées au moyen de blockchains. Les enjeux spécifiques à Monaco, pour lesquels les blockchains devraient être source de progrès substantiels, comme le

développement durable ou la gestion des flux routiers et des parkings, ou encore le yachting, méritent que Monaco soit à l'origine de la première réglementation de portée générale.

Enfin, un argument de stratégie économique internationale milite fortement en faveur de l'adoption d'un cadre juridique large, ouvert à toutes les blockchains, financières et non-financières. La Principauté, si elle était le premier Etat au monde à promouvoir et à sécuriser l'activité des blockchains, ne manquerait pas d'attirer vers son territoire une activité économique prometteuse et à très haute valeur ajoutée. D'après un article récent, la blockchain *« va transformer les transactions commerciales de la même manière qu'Internet a transformé les communications »*, prédit Brigid McDermott, vice-présidente chargée du développement de la blockchain chez IBM. Aux Etats-Unis et ailleurs, de nombreuses entreprises testent cette technologie. Leurs domaines d'activité sont variés : la banque, l'assurance, la santé, la logistique, l'industrie, le transport aérien ou encore la gestion des contrats. D'après une étude menée par Juniper Research, 57 % des entreprises de plus de 20 000 employés déploient ou étudient le déploiement de la technologie. *« Les sociétés ont une bien meilleure compréhension de la blockchain par rapport à l'an passé »*, indique le cabinet de recherche dans son rapport. Cela s'explique par une augmentation de la recherche et développement en interne et avec des partenaires extérieurs (Le Monde ; Conçue pour le Bitcoin, la blockchain intéresse des secteurs de l'économie ; 23 novembre 2017).

Ainsi, en devenant le premier Etat au monde à réguler totalement les blockchains et à agir en faveur de leur usage sur le territoire, Monaco pourrait s'assurer sans coup férir un leadership réel dans une activité économique déterminante.

Monaco ne peut ni ne doit rater la formidable opportunité que représente l'économie des blockchains. Ce troisième scénario revêt une approche entrepreneuriale, pragmatique et empirique qui a, chacun le comprendra, la préférence des auteurs de la présente proposition de loi.

Tout l'objet de la proposition de loi est de permettre à Monaco de saisir cette chance de devenir un leader mondial.

Pour ce faire, la proposition de loi instaure une période d'expérimentation, au cours de laquelle il n'y aura aucune contrainte réglementaire. Parce que la blockchain peut concerner de nombreux secteurs d'activité, parce qu'elle est aussi une technologie disruptive, ce cadre ouvert a pour objectif de laisser libre cours à l'imagination de concepteurs de solution, sans définir et à priori un carcan administratif ou réglementaire. Pour autant, cela ne veut pas dire non plus que tout sera permis, sans limite : il semble évident aux auteurs de cette proposition qu'il faudra s'assurer d'une certaine éthique et de l'adéquation de l'activité à la « bonne moralité ». Cette période servira d'accélérateur afin d'attirer à Monaco toute société qui voudrait bénéficier d'un caractère protecteur des acteurs institutionnels, et ainsi, participer au développement de la blockchain et faire bénéficier la Principauté des services qu'elle peut offrir.

Dès lors, à l'échéance de l'expérimentation, le bilan permettra d'y mettre fin sans condition en cas de résultats non satisfaisants, d'en prolonger la durée si l'environnement n'était pas suffisamment mature ou encore, de passer en mode 'production', avec un cadre réglementaire adapté.

Autant le préciser de manière explicite, la mise en place d'un « bac à sable expérimental » permettra, c'est l'option retenue par les auteurs de cette proposition, de développer un nouveau secteur d'activité en Principauté et de permettre à Monaco de devenir la *« blockchain valley »*, attirant de nombreuses sociétés qui sont aujourd'hui à la recherche d'un cadre réglementaire souple, moderne, pragmatique.

La proposition de loi crée une Autorité Monégasque des Blockchains (AMB), organisme privé chargé d'une mission de service public. L'AMB assurera l'animation de l'expérimentation, en fédérant les acteurs, en sélectionnant les projets, tout en assurant une veille technologique et réglementaire, européenne et mondiale. Cette structure se veut être un organe permanent, regroupant en son sein des experts et des personnes de Monaco et d'autres horizons, directement concernées par les problématiques du numérique. Il est important que l'AMB puisse réunir un comité d'experts de grandes renommées, afin de nourrir la réflexion et la stratégie de la Principauté dans ces domaines. Ce serait en quelque sorte un « think tank » du numérique, chargé de la veille technologique, concurrentielle et réglementaire, tout en assurant une activité très opérationnelle avec l'animation du secteur de la blockchain.

Pour autant, la nécessité, voire même l'urgence, à lancer des projets sur la base de blockchains à Monaco ne nous autorise pas à attendre la concrétisation de ce texte dans l'arsenal juridique monégasque. Pour être un acteur de premier plan, il y a lieu d'être inventif et de procéder à la mise en place au plus vite d'une structure temporaire, qui va nous permettre d'initier la démarche.

Sous le bénéfice de ces observations générales, la proposition de loi appelle désormais les commentaires techniques exposés ci-après.

♦♦♦

Pour ce qui relève de son architecture générale, la présente proposition de loi comprend 13 articles.

Les quatre premiers articles sont consacrés aux définitions juridiques des termes techniques. Ainsi, l'article premier définit les « chaines de bloc » ou *blockchains*. L'article 2 s'intéresse au « contrats intelligents » ou *smarts contracts*. L'article 3 qualifie d'« entreprise algorithmique » les ensembles de *smart contracts* qui produisent de manière autonome des effets économiques. Sont enfin définies les crypto-monnaies dans l'article 4.

Les articles 5 et 6 posent les principes susceptibles de conférer une valeur juridique aux opérations effectuées sur une *blockchain*. Ainsi, l'article 5 pose le principe d'application de la loi de la Principauté à toutes les opérations dont un des éléments constitutifs ou une des conséquences intervient en Principauté. Il s'agit d'un élément précieux, dans la mesure où, par son caractère décentralisé et, dès lors, transfrontalier, les éléments d'extranéité ne manqueront pas d'être monnaie courante. Aussi ce rattachement au droit de la Principauté est-il un gage de sécurité juridique important. Ainsi nous acquerrons la

certitude que les citoyens et les entreprises monégasques demeureront protégés par notre ordre public interne. D'autant que la suite de l'article énonce le principe de la compétence matérielle et territoriale des juridictions de la Principauté puis confère un double privilège de juridiction aux tribunaux monégasques, en permettant d'attraire devant nos tribunaux les étrangers ou les monégasques ayant contracté des obligations hors du territoire à l'occasion de l'usage d'une *blockchain*, d'un *smart contract*, d'une entreprise algorithmique ou d'une crypto-monnaie (art.5-4).

L'article 6 règle la question cruciale de la preuve. Il confère une valeur probante et une date certaine aux actes inscrits dans une *blockchain*.

Les articles 7 à 12 sont consacrés à la mise en place d'une période d'expérimentation de trois années.

L'expérimentation se traduit d'abord par l'organisation d'un « bac-à-sable réglementaire » (« regulatory *sandbox* »), avec l'article 7. Cela se traduit, juridiquement, par le fait que l'Etat mette les entreprises qui le souhaitent en capacité de développer des projets liés à la *blockchain*, en acceptant de ne pas poser de barrières réglementaires techniques qui pourraient freiner le développement de ces projets. Bien évidemment, cela ne concernerait nullement les textes d'ores et déjà existants de sorte que, par exemple, les dispositions essentielles à l'ordre public économique sont bien évidemment maintenues ; par exemple en matière de lutte contre le blanchiment, contre la fraude, contre la criminalité technologique, en matière de protection d'informations nominatives, de sécurité nationale et de connaissance des clients.

Cette expérimentation sera conduite par un organisme privé chargé, en réalité, d'une mission de service public : l'Autorité Monégasque des Blockchains (AMB), laquelle est instituée sous l'article 8.

L'AMB aura un rôle multiple :

- en premier lieu, celui d'animer le secteur des *blockchains* et de s'assurer de l'accomplissement du programme d'actions dont les grandes lignes sont énoncées sous l'article 12. Il s'agit de favoriser le déploiement de la technologie dans les secteurs stratégiques pour la Principauté, savoir :

- Création d'un incubateur et d'un pôle de recherches universitaires dédiés ;
- L'autoconsommation et le trading d'énergies renouvelables et autres ressources ;
- La labellisation alimentaire ;
- La santé humaine et animale ;
- La préservation des espèces animales en danger ;
- L'environnement ;
- Le sport ;
- Les communications électroniques ;
- La ville intelligente ;
- L'émission de monnaie cryptographique ;
- La sécurité sociale ;
- La modernisation de l'Etat et la fiscalité ;
- Le travail ;
- Le tourisme ;
- Le yachting ;
- L'assurance et la réassurance ;
- La finance de marché et la finance d'entreprise ;
- Les paiements internationaux ;
- L'identité numérique ;
- L'intelligence numérique ;
- La propriété intellectuelle ;
- Contribuer au rayonnement international de la Principauté de Monaco et nouer des partenariats avec toute institution partageant l'objet de l'AMB.

- en second lieu, l'AMB aura un rôle de régulateur, pour le compte de l'Etat, des *blockchains*. Il lui appartient en effet de veiller, pour le compte de l'Etat, à l'application de la législation et de la réglementation en ces matières, et, lorsque c'est nécessaire, de contrôler et de transmettre aux autorités compétentes aux fins d'enquête et de sanction les manquements qu'elle constate.

Pour ce faire, l'article 9 prévoit que l'AMB sera composée de représentants du Gouvernement, de représentant de sociétés, d'associations et de syndicats intervenant dans le domaine du numérique, ainsi que de personnalités académiques et de praticiens reconnus en

cette matière. Notons que le Président de cette entité sera choisi, par ordonnance souveraine, parmi ces personnalités et praticiens. De manière générale, l'ensemble de ces personnes sera également nommé par ordonnance souveraine.

Bien évidemment, il est nécessaire, pour mener à bien les missions qui lui seront confiées, que cette entité dispose d'un personnel et de services, lesquels seront placés sous l'autorité d'un secrétaire général.

L'Article 10 est avant toute chose une disposition complémentaire de l'expérimentation dite « bac à sable réglementaire » figurant à l'article 7 et du programme d'actions de l'article 12.

L'article 11 prévoit de doter l'AMB des crédits nécessaires à son fonctionnement, qu'il s'agisse de ses dépenses de personnel, comme du bon accomplissement de ses missions. Ceux-ci seront inscrits sur le Budget de l'Etat, ce qui permettra au Conseil National de veiller, dans le cadre de ses attributions, au succès des futures missions de cette entité.

Enfin, après le programme d'action de l'article 12, déjà évoqué, l'article 13, complète utilement le dispositif en prévoyant les traditionnelles dispositions réglementaires d'application, destinées à traduire avec célérité les objectifs et principes qui auront été retranscrits par la future législation.

♦♦♦

Tel est l'objet de la présente proposition de loi.

DISPOSITIF

Article Premier

Les chaines de blocs sont des dispositifs d'enregistrement numériques partagés et cryptés reposant sur le consensus et permettant l'authentification et certification de transactions dans des conditions de sécurité.

Article 2

Les contrats intelligents sont des algorithmes disposant de la capacité à s'auto-exécuter de façon autonome pour déplacer de la valeur ou des informations à travers les chaînes de blocs. Ils constituent des actes juridiques et produisent des effets de droit. Ils obéissent, en tant que de raison, pour leur validité et leurs effets, aux règles qui gouvernent les contrats.

Article 3

L'entreprise algorithmique est l'opération par laquelle un ou plusieurs contrats intelligents, agissant dans un but déterminé au profit d'un ou plusieurs bénéficiaires, émettent ou reçoivent, transfèrent des actifs, des biens, des droits ou des sûretés, ou un ensemble d'actifs, de biens, de droits ou de sûretés, présents ou futurs, à des tiers.

Article 4

Une monnaie cryptographique est une unité de valeur électronique utilisable sur une chaine de blocs, fondée sur les principes de la cryptographie, que l'on peut émettre soi-même ou échanger et qui permet de régler des transactions.

Article 5

Le droit monégasque est applicable aux chaines de blocs, aux contrats intelligents, aux entreprises algorithmiques et aux monnaies cryptographiques qui produisent des effets sur le territoire de la Principauté de Monaco. L'effet est réputé se produire sur le

territoire de la Principauté de Monaco dès lors qu'un de ses faits constitutifs ou une de ses conséquences a eu lieu sur ce territoire.

Les juridictions de la Principauté de Monaco sont compétentes tout fait ou acte tout acte juridique relevant du droit monégasque.

L'étranger, même non résidant en Principauté de Monaco, pourra être cité devant les tribunaux monégasques, pour l'exécution des obligations par lui contractées ou l'inexécution d'obligations constatée, sur une chaine de blocs, par l'effet ou au moyen d'un contrat intelligent, dans le cadre d'une entreprise algorithmique ou en relation avec une entreprise algorithmique, ou du fait de la souscription ou de l'utilisation d'une monnaie cryptographique avec toutes personnes monégasques, exerçant une activité ou ayant son domicile dans la Principauté de Monaco, y compris lorsque ces obligations ont été contractées avec ces mêmes personnes en pays étranger.

Toute personne monégasque ou ayant son domicile en Principauté peut être traduit devant un tribunal de Monaco, pour des obligations par lui contractées en pays étranger sur une chaine de bloc, par l'effet ou au moyen d'un contrat intelligent, dans le cadre d'une entreprise algorithmique ou en relation avec une entreprise algorithmique, ou du fait de la souscription ou de l'utilisation d'une monnaie cryptographique, même avec un étranger.

Article 6

L'inscription d'un acte juridique dans une chaine de blocs est présumée constituer une copie fidèle, opposable et durable de l'original, portant une date certaine.

Article 7

La Principauté de Monaco encourage l'expérimentation en matière de chaine de blocs, de contrats intelligents, d'entreprises algorithmiques et de monnaies cryptographiques afin que les innovations prometteuses puissent se concrétiser, être testées sur le marché et avoir la possibilité d'être adoptées largement, tant à Monaco qu'à l'étranger.

A ce titre, la Principauté de Monaco organise à cet effet l'expérimentation pour une durée de trois années, par les entreprises qui le souhaitent de manière à favoriser le

développement de toutes solutions s'appuyant sur les chaines de blocs, les contrats intelligents, les entreprises algorithmiques ou les monnaies cryptographiques. Elle met ainsi à disposition desdites entreprises les moyens matériels nécessaires à cette expérimentation, en les assurant durant la période susmentionnée, de l'absence de contraintes d'ordre réglementaire.

Les résultats de cette expérimentation font l'objet d'une publication.

Article 8

Il est institué un organisme de droit privé, dénommée « Autorité Monégasque des Blockchains », en abrégé AMB, chargée, en matière de chaine de blocs, de contrats intelligents, d'entreprises algorithmiques et de monnaie cryptographique de veiller, pour le compte de l'Etat, à l'application de la législation et de la réglementation en ces matières, et, lorsque c'est nécessaire, de contrôler et de transmettre aux autorités compétentes aux fins d'enquête et de sanction le cas échéant, les manquements qu'elle constate. Elle assure également la bonne information du public et l'accompagne, en cas de besoin, grâce à un dispositif de médiation qu'elle met en place.

Article 9

L'AMB est composée de représentants du Gouvernement, de représentant de sociétés, d'associations et de syndicats intervenant dans le domaine du numérique, ainsi que de personnalités académiques et de praticiens reconnus en cette matière, parmi lesquelles figure le Président de l'AMB. Ces derniers sont nommés par ordonnance souveraine.

L'AMB dispose de services dirigés par un secrétaire général et placés sous son autorité. Le secrétaire général est chargé d'assurer le fonctionnement et la coordination desdits services.

L'AMB peut consulter toute personne susceptible d'éclairer ses travaux ou de l'assister dans l'exercice de ses missions.

Article 10

L'AMB est chargée de promouvoir la Principauté de Monaco en matière de chaines de blocs, de contrats intelligents, d'entreprises algorithmiques et de monnaies cryptographiques. L'AMB sera appelée à représenter la Principauté de Monaco auprès d'instances et organisations de nations étrangères ou internationales en tout ou partie de ces mêmes matières accompagnée des représentants étatiques appropriés.

L'AMB s'appliquera notamment à privilégier les applications qui s'inscrivent dans le programme d'action déterminé à l'article 12.

Six mois avant le terme de l'expérimentation de trois ans mentionnée à l'article 7, l'AMB présentera au Ministre d'Etat et au Conseil National un rapport d'étape sur les fruits de l'expérimentation.

L'AMB a la charge de rédiger et de soumettre à l'approbation du Ministre d'Etat un Règlement Général qui encadrera son action.

Article 11

L'Etat assure à l'AMB, par une dotation de fonctionnement inscrite au Budget de l'Etat, les crédits nécessaires à son fonctionnement et à l'accomplissement de ses missions.

Article 12

L'AMB s'efforce de favoriser l'expérimentation des chaines de blocs, des contrats intelligents, des entreprises algorithmiques et des monnaies cryptographiques notamment dans les champs d'activité prioritaires suivants :

- Création d'un incubateur et d'un pôle de recherches universitaires dédiés ;
- L'autoconsommation et le trading d'énergies renouvelables et autres ressources ;
- La labellisation et la traçabilité alimentaire ;
- La santé humaine et animale ;
- La préservation des espèces animales en danger ;
- L'environnement ;

- Le sport ;
- Les communications électroniques ;
- La ville intelligente ;
- L'émission de monnaie cryptographique ;
- La sécurité sociale ;
- La modernisation de l'Etat et la fiscalité ;
- Le travail ;
- Le tourisme ;
- L'assurance et la réassurance ;
- La finance de marché et la finance d'entreprise ;
- Les paiements internationaux ;
- L'identité numérique ;
- L'intelligence numérique ;
- La propriété intellectuelle ;
- Contribuer au rayonnement international de Monaco.

Article 13

Une ordonnance souveraine détermine les conditions d'application de la présente loi.

Thierry POYET

C. ROUGAIGNOU-VERNIN

THIERRY CROVETTO

Jean-Claude ALLAVENA

ANNEXE N°4

2019-7
20 mai 2019

PROJET DE LOI
RELATIVE A LA TECHNOLOGIE BLOCKCHAIN

EXPOSE DES MOTIFS

La technologie « *Blockchain* » est considérée comme une grande révolution, voire même la révolution technologique des débuts de ce 21ème siècle. Compte tenu des innovations qu'elle comporte et des nombreux usages qui pourraient en être faits, certains estiment que ladite technologie pourrait à l'avenir connaître un essor comparable à celui d'internet. Ainsi, certains ont pu parler de technologie disruptive ou de rupture à son sujet.

Cette technologie a pour objet de permettre à des utilisateurs de consulter et de mettre à jour un registre partagé (que l'on appelle une *blockchain* ou chaîne de blocs) dont le contenu est maintenu de façon décentralisée, sans la présence d'un tiers de confiance. C'est au travers d'un mécanisme de consensus que s'effectue la mise à jour de cette *blockchain*, ce qui assure un ordonnancement clair et sans ambiguïté des transactions et des blocs et garantit l'intégrité et la traçabilité du contenu de ce registre partagé entre les différents nœuds distribués du réseau.

Son potentiel et ses usages, sans cesse en développement, se doivent d'être régulés.

Cet impératif n'a pas échappé au Conseil National qui, lors de la séance publique du 21 décembre 2017, a adopté une proposition de loi ayant pour objet de décrire cette technologie et de l'encadrer.

Fort des orientations données, en matière de transition numérique de la Principauté, par Son Altesse Sérénissime le Prince Souverain, le Gouvernement a exprimé son désir de voir transformer cette proposition en projet de loi.

En déposant sur le bureau de l'Assemblée le présent projet de loi, le Gouvernement Princier entend ainsi continuer son processus de modernisation et de transition numérique initié avec la loi n° 1.383 du 3 août 2011 sur l'économie numérique et complété, plus récemment, avec le dépôt, des projets de loi relative à l'identité numérique d'une part et à la modification de la loi n° 1.383 du 3 août 2011, précitée, d'autre part.

Aux vues des données internationales et européennes, et selon le site « *blockchainfrance.wordpress.com* », la technologie *blockchain* est définie comme « *une technologie de stockage numérique et de transmission à coût minime, décentralisée et totalement sécurisée* » Dans le même sens, en mai 2017, le « *Vocabulaire de l'informatique* » français a défini officiellement la *blockchain* comme « *un mode d'enregistrement de données produites en continu, sous forme de blocs liés les uns aux autres dans l'ordre chronologique de leur validation, chacun des blocs et leur séquence étant protégés contre toute modification* ».

Il importe au Gouvernement de préciser que la *blockchain* est une technologie qu'il ne faut pas confondre avec les usages qui en sont fait, par des *blockchains* particulières se développant dans de nombreux secteurs d'activités, notamment la banque, la finance (*Bitcoin, Ethereum),* les registres fonciers, les documents et la logistique dans les transports maritimes ou encore la traçabilité des aliments et des produits.

Aussi, il convient tout d'abord de préciser que plusieurs grandes catégories de *blockchain* peuvent être crées.

En premier lieu, il existe les *blockchains* publiques, qui sont totalement décentralisées et auxquelles tout le monde peut accéder car il n'y a aucune barrière d'entrée, aucune permission à demander pour effectuer une transaction et où tous les acteurs sont en situation égalitaire dans leur participation au réseau comme *Bitcoin* ou *Ethereum*. Les *blockchains* publiques reposent sur l'anonymat des participants et l'absence de régulateur.

En second lieu, il y a les *blockchains* qui fonctionnent dans un réseau privé sur lequel le gérant peut modifier le protocole quand il le souhaite et où personne ne peut y participer sans y être autorisé par une autorité centrale.

Font partie de cette catégorie les *blockchains* utilisées par les banques au sein de leur réseau interne ou encore celles utilisées par certaines banques centrales pour les opérations de règlement de devises en monnaie d'une banque centrale.

Enfin, il existe les *blockchains* dites « *de consortium* » qui regroupent plusieurs acteurs mais qui ne sont pas publiques et ouvertes à tous. C'est une *blockchain* hybride où les droits d'écriture et de modification sont modifiables et certains nœuds peuvent être rendus publics tandis que d'autres restent privés. De fait, dans ce dernier type de *blockchain*, des organisations présélectionnées opèrent chacune un nœud différent et elles peuvent être restreintes à certains utilisateurs. Elles sont donc considérées comme étant partiellement décentralisées et s'adaptent particulièrement aux environnements régulés à l'instar du consortium bancaire R3 CEV qui regroupait plus de 80 banques internationales expérimentant la technologie.

De manière générale, la *blockchain* repose sur trois techniques éprouvées : une base de données (un registre partagé), des échanges de fichiers (échanges « *peer to peer* » *ou de* « *pair à pair* ») et l'utilisation de la cryptographie asymétrique pour signer les transactions garantissant ainsi l'identité du signataire et l'intégrité du contenu.

La caractéristique essentielle du dispositif est que ce registre est décentralisé et qu'ainsi, aucune autorité ne tient le rôle de tiers de confiance.

De fait, le registre est fiabilisé et sécurisé par ses utilisateurs, dans la mesure où chacun vérifie la validité de la chaîne. En outre, les données ne peuvent être modifiées.

S'il est historiquement admis que la technologie *Blockchain* est née avec la *blockchain bitcoin* en 2009, créée anonymement sous le pseudonyme « *Satoshi NAKAMOTO* » il n'en demeure pas moins que celle-ci ne peut être réduite au bitcoin ou autres crypto-monnaies, dans la mesure où ses utilisations peuvent être diverses et que son potentiel d'utilisation est considérable.

Dans cette optique, la question de la fiabilité et de la sécurité de la technologie est également un enjeu majeur, tant pour le développement de la *Blockchain* que pour ses utilisateurs. Car, en dépit du slogan des initiateurs de la *Blockchain*, selon lequel « *the code is law* » (le codage fait la loi), le développement de cette technologie ne saurait se faire en dehors de règles adaptées lorsque celles du droit commun s'avèrent insuffisantes, à l'instar d'ailleurs d'internet dont le fonctionnement est désormais régi par un corpus de règles spécifiques.

Hors de la Principauté, diverses initiatives ont d'ores et déjà été prises par plusieurs Etats pour réglementer la technologie *Blockchain* et ses applications, tantôt par les autorités des marchés financiers, comme en Suisse, à Malte ou aux États-Unis, tantôt avec l'adoption d'un cadre légal et réglementaire, comme en Italie, au Luxembourg, à Malte, et récemment en France.

Dans ce sillage, il est apparu hautement opportun au Gouvernement d'aller encore plus loin et de consacrer, avec le présent projet de loi, la force probante de la *blockchain* et l'encadrement des levées de fonds sous forme d'actifs numériques qui donnent lieu à l'émission de jetons sur cette technologie.

Ce choix s'explique par l'attrait qui se manifeste à Monaco pour ce nouveau mode de financement de l'activité économique des entreprises. La pratique révèle en effet que de nombreuses opérations de levées de fonds sous forme d'actifs numériques effectuées au moyen de la technologie *blockchain*, que l'on désigne couramment sous le terme « *d'Initial Coin Offerings* » (ICOs) connaissent dans le monde un succès croissant avec des montants collectés parfois considérables.

Or, de telles opérations, en principe réalisées sans intermédiaire financier, s'adressent souvent à un public averti mais peuvent parfois intéresser également le grand public, alors même que les fonds investis dans une ICO ne sont pas garantis et qu'il s'agit d'investissements présentant un risque de perte en capital. De même, la valeur des jetons émis, appelés communément en la matière « *tokens* », est susceptible de grandes variations, et la pratique a révélé des cas de fraudes, voire de risques de blanchiment de capitaux.

Compte tenu des risques potentiels présentés par les ICOs et afin de sécuriser ce nouveau mode de financement des entreprises à Monaco, le Gouvernement a donc souhaité poser un cadre légal destiné, d'une part, à protéger les investisseurs qui pourraient souhaiter participer à de telles opérations lancées par des sociétés installées à Monaco en leur fournissant une information de qualité, et d'autre part à favoriser le développement des sociétés dans ce domaine à la fois nouveau et complexe.

De fait, le présent projet de loi prévoit que les émissions de jetons sur une *blockchain* soient soumises à une autorisation administrative obligatoire, laquelle sera délivrée par le Ministre d'Etat sous la forme d'un label, après consultation d'une commission spécialement constituée à cet effet. Ladite commission examinera, en particulier, si une information suffisante des souscripteurs est envisagée par l'entreprise émettrice des jetons et si la levée de fonds présente toutes les garanties requises, notamment en ce qui concerne la technologie proposée, et les modalités de collecte et d'utilisation des fonds recueillis. Ces éléments d'information devront être réunis au sein d'un document d'informations appelé communément « *whitepaper* ».

De surcroît, il est apparu expédient au Gouvernement de veiller à ce que les différents opérateurs appelés à participer aux levées de fonds sur la *blockchain* respectent les standards de lutte contre le blanchiment de capitaux et le financement du terrorisme, applicables à Monaco, conformément à la loi n° 1.362 du 3 août 2009 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption, modifiée.

En conséquence, le Gouvernement entend, dans le présent projet loi, accompagner l'essor de cette nouvelle technologie en définissant d'une part, de manière générale la technologie *blockchain* et les usages qui en seront fait et d'autre part, en encadrant de manière précise le dispositif des offres de jetons.

Sous le bénéfice de ces observations d'ordre général, le présent projet de loi appelle les commentaires particuliers ci-après.

Le projet de loi comporte les six chapitres suivants :

- Chapitre I : Définitions ;

- Chapitre II : Régime et force probante ;

- Chapitre III : Des offres de jetons ;

- Chapitre IV : Du contrôle de la régularité des offres de jetons ;

- Chapitre V : Des sanctions ;

- Chapitre VI : Dispositions diverses et transitoires.

Le Chapitre I intitulé « *Définitions* » comprend les définitions nécessaires à la bonne compréhension de la loi.

L'article premier définit la terminologie employée dans le projet de loi. Outre une définition générale de la technologie *blockchain*, intitulée dans le projet de loi « *dispositif d'enregistrement numérique sur un registre partagé* », il explicite les termes habituellement employés pour définir les actifs basés sur cette technologie.

Pour définir les jetons, le Gouvernement a choisi de reprendre la distinction couramment admise entre « *security token* », « *utility token* » et « *coin* ».

Les « *security tokens* » sont des jetons qui revêtent la plus grande spécificité.

Concrètement ceux-ci désignent des jetons présentant une ou plusieurs caractéristiques des instruments financiers, tels que par exemple des droits de vote, ou des droits sur les résultats de l'exploitation sans conférer de part ou d'action dans le capital de la société. C'est d'ailleurs l'une des particularités des offres de jetons qui n'ont pas pour effet d'emporter la dilution des droits des actionnaires.

Quant aux « *utility tokens* », ceux-ci désignent les jetons qui sont représentatifs d'un droit d'usage sur des biens, des produits ou un droit d'accès à des services consentis par le porteur du projet.

S'agissant des *coins*, il s'agit de biens dont l'objet principal est de remplir l'une des trois fonctions traditionnellement attribuées à la monnaie.

Si aucun des biens inscrits sur la *blockchain* ne peut aujourd'hui être considéré comme remplissant l'ensemble de ces fonctions, d'où leur nature non-monétaire, certains d'entre eux s'en rapprochent et méritent à ce titre d'être distingués des autres. La définition proposée dans le présent projet de loi a pour objet de tenir compte de cette nature hybride en identifiant les biens qui, sans pouvoir être considérés comme d'authentiques devises, s'en rapprochent bel et bien.

Le Gouvernement a ensuite estimé opportun de définir un « *protocole contractuel numérique* », communément appelé « *smart contracts* », ou « *contrat intelligent* », à savoir une technique apparue avec la *blockchain* Ethereum se traduisant par des programmes informatiques parfois complexes utilisant la technologie *blockchain*. C'est en particulier via ces *smart contracts* que les offres de jetons sont la plupart du temps réalisées.

Les clés privée et publique sont quant à elles une technique préexistant à la technologie *blockchain* et reprise par la *blockchain* Bitcoin et les *blockchains* qui l'ont suivie. Les techniques cryptographiques asymétriques dont la clé privée est assortie permettent de garantir l'impossibilité d'accéder au « *wallet* » (portefeuille) correspondant par une personne ne disposant pas de cette clé.

La clé publique, quant à elle, est un corollaire indissociable de la clé privée permettant aux tiers de réaliser des transactions avec le détenteur de la clé privée et de vérifier son identité sans que ce dernier n'ait nul besoin de divulguer sa clé privée.

Etant rappelé que les offres de jetons sont des opérations de levées de fonds effectuées à travers une *blockchain* et qui donnent lieu à une émission de jetons, celles-ci sont définies en termes généraux, afin d'englober la grande diversité de techniques pouvant être mises en œuvre pour proposer à des personnes d'acquérir les jetons qui font l'objet de ces offres.

Les raisons de ce choix tiennent au fait qu'il est difficile d'identifier des traits communs à l'ensemble de ces offres, tant la nature du projet sous-jacent, que la technologie mise en œuvre, varie d'une offre à l'autre. La plupart d'entre elles se caractérisent cependant par l'échange des jetons faisant l'objet de l'offre contre des devises nationales ou des cryptomonnaies populaires (au premier rang desquelles l'ether et le bitcoin), un prix décoté par rapport à celui auquel ces jetons pourront être acquis postérieurement à l'offre le cas échéant, ainsi qu'une certaine implication des souscripteurs dans la réussite de l'offre et du développement futur du projet, dont la réussite dépend souvent du nombre de souscripteurs à l'offre et, une fois l'offre réalisée, de la fréquence d'utilisation et du volume d'échange des jetons.

Les Chapitres II et III intitulés « *Régime et force probante* » et « *Des offres de jetons* » comprennent les articles 2 à 7 et posent le cadre général de la *blockchain* et de l'offre de jetons.

L'article 2 pose un principe général de présomption simple de l'existence, du contenu et de la date des informations stockées sur la *blockchain*. Cette présomption est justifiée par l'inaltérabilité des transactions figurant sur la *blockchain*. Toutefois, cette présomption ne sera recevable que sous réserve du respect des exigences prévues au sein d'une Ordonnance Souveraine distincte, à l'instar de la loi italienne renvoyant la valeur probatoire du dispositif à sa conformité à l'article 41, relatif à l'horodatage électronique, du règlement eIDAS n°910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.

L'article 3, prévoit, quant à lui, une présomption simple de ce que toute transaction a été effectuée par le propriétaire de la clé privée correspondante, et participe du même esprit que celui de l'article 2. S'il est en effet impossible, en l'état actuel de la technologie, de réaliser une transaction sur la *blockchain* sans disposer de la clé privée qui permet cette réalisation, la divulgation ou le vol de cette clé pourrait hypothétiquement mettre en péril l'identification de la personne à l'origine de la transaction.

De ce fait, il incombe à la personne qui s'en prévaut, c'est-à-dire le propriétaire de la clé privée dans la plupart des cas, d'apporter la preuve de ce que cette clé a été volée ou divulguée à un tiers et utilisée aux fins de réaliser une transaction donnée. Le présent projet de loi a ainsi pris le parti de responsabiliser pleinement le détenteur de la clé privée en lui faisant supporter le risque de sa divulgation.

Cette solution est dans le droit fil de la philosophie sous-jacente à la technologie *blockchain*, qui donne tous pouvoirs au propriétaire de la clé privée pour réaliser toutes transactions au moyen de cette clé sans intervention possible d'une entité tierce. Il incombe dès lors à ce dernier de s'assurer qu'aucun tiers ne peut être mis en mesure de l'utiliser.

L'article 4 distingue les différents types possibles d'offres de jetons (publiques ou privées) et pose un principe d'interdiction de l'offre au public des *security tokens*. Ledit article fait peser sur l'émetteur la responsabilité de définir et de déterminer les caractéristiques générales de l'offre (nature des jetons, droits afférents et caractère public ou privé).

L'article 5 pose le principe selon lequel toute offre de jetons est subordonnée à l'obtention d'un label délivré par le Ministre d'État après l'avis consultatif d'une commission dédiée. Compte tenu du manque de sérieux dont ont pu faire preuve nombre d'émetteurs de jetons par le passé, et quoique le secteur ait connu une certaine professionnalisation sur la période récente, il est apparu nécessaire de soumettre les offres de jetons à une autorisation administrative préalable et obligatoire, délivrée sous la forme d'un label.

L'octroi du label certifie en effet la qualité de l'information fournie et des conditions de l'offre, sans toutefois offrir aux souscripteurs de garantie sur le succès économique de l'investissement proposé ou sur l'opportunité de participer à cette offre.

Ledit article fixe également les modalités de l'intervention de la commission consultative, laquelle doit disposer de toutes les informations lui permettant de rendre un avis éclairé. Outre la possibilité d'entendre les représentants de l'émetteur et de toute personne dont elle estime l'audition utile, est ainsi imposée la communication à la commission, des pièces nécessaires à l'instruction de la demande d'autorisation, parmi lesquelles figure un document d'informations destiné à l'information des souscripteurs, dit « *white paper* ».

Ce document, dont la communication aux souscripteurs est essentielle, doit notamment contenir des renseignements sur l'émetteur et sur l'offre elle-même, avec des précisions sur la nature des droits attachés aux jetons à émettre. La liste des pièces nécessaires à l'instruction de la demande ainsi que le contenu du « *white paper* » seront définis par ordonnance souveraine.

Il s'agit là d'une pièce centrale de l'offre de jetons. Les offres réalisées par le passé, et dans un contexte fortement non régulé, ont témoigné de ce que la qualité, la forme et le contenu de ce document ont pu grandement varier d'un émetteur à l'autre. Il est dès lors apparu nécessaire de requérir de l'émetteur qu'il y fasse figurer un certain nombre d'informations requises.

Parce qu'un « *white paper* » établi conformément aux dispositions réglementaires en la matière devra contenir toutes les informations nécessaires à la bonne compréhension du projet, sa communication à la commission consultative est destinée à lui donner une information précise sur le projet.

Dans le même sens, le contenu dudit « *white paper* » doit être clair, exact et non trompeur.

En considération des éléments portés à sa connaissance, la commission, appréciera si l'information des souscripteurs ne cherche pas à les induire en erreur, voire à masquer une partie des informations nécessaires.

La clarté de l'information peut en effet faire défaut même aux projets les plus sérieux et prometteurs lorsque, par exemple, les caractéristiques techniques des droits attachés aux jetons font l'objet d'une description trop imprécise pour que leur teneur soit suffisamment compréhensible pour les souscripteurs potentiels.

L'article 6 prévoit que seules des sociétés immatriculées sur le territoire de la Principauté peuvent réaliser une offre de jetons dans le cadre de la présente loi. Autrement dit, seules les sociétés domiciliées à Monaco pourront solliciter la délivrance du label délivré par le Ministre d'Etat aux fins d'initier une offre de jetons sur le fondement de la présente loi.

L'obligation, pour l'émetteur qui entend offrir des *security tokens*, d'être constitué sous forme de société par actions tient à certaines caractéristiques attachées à ces titres lesquels ne peuvent être émis que par des sociétés par actions.

Il importe par exemple d'éviter qu'une société à responsabilité limitée puisse émettre des titres négociables.

Enfin, il incombe à l'émetteur de garantir que la conservation des fonds et des actifs recueillis dans le cadre de l'offre, ainsi que leur suivi, peuvent être effectivement assurés. Cet impératif est d'autant plus essentiel qu'une malfaçon de la technologie sous-jacente aux jetons, voire une fraude quelconque conduisant à leur disparition ou distraction, devrait en principe donner lieu à une restitution des fonds aux souscripteurs. Quant à l'obligation d'assurer leur suivi, elle permet d'assurer que les fonds seront utilisés conformément aux conditions prévues par le projet d'offre.

L'article 7 prévoit le placement sous séquestre des fonds collectés pour toute la durée de l'opération. Il convient en effet de s'assurer que ces fonds pourront être restitués aux souscripteurs le cas échéant en cas d'échec de la levée de fonds ou d'abandon du projet, et qu'ils ne seront utilisés qu'une fois l'opération arrivée à terme, ou aux échéances prévues selon le calendrier fixé dans le « *white paper* ».

Dans la continuité de ce principe, l'article énonce plusieurs hypothèses dans lesquelles les fonds devront être restitués aux souscripteurs. Leur placement préalable sous séquestre permet de garantir le respect de cette obligation, et en particulier qu'ils ne pourront être utilisés que dans les conditions prévues par le « *white paper* ».

Le Chapitre IV, intitulé « *Du contrôle de la régularité des offres de jetons* », comprend les dispositions relatives au contrôle, par l'Etat, de la conformité des offres de jetons aux dispositions de la présente loi.

L'article 8 prévoit ainsi qu'il incombe à la Direction de l'Expansion Economique d'effectuer le contrôle du respect des obligations prévues par la loi. Ledit contrôle, effectué d'office ou sur signalement, est mené par des fonctionnaires ou agents spécialement commissionnés à cet effet et tenus au secret professionnel ainsi qu'à l'obligation de discrétion. Dans l'hypothèse où ils feraient appel à un expert, ce-dernier est soumis aux mêmes obligations.

L'article 9, vient, quant à lui, encadrer la procédure de contrôle, celle-ci pouvant être menée sur pièces ou sur place.

A cet effet, les agents de la Direction de l'Expansion Economique sont dotés du pouvoir d'obtenir communication de tous documents professionnels, de convoquer et entendre toute personne le cas échéant en ayant recours aux systèmes de visioconférence ou audioconférence, d'accéder aux locaux à usage professionnel et de recueillir des explications sur place, ainsi que tous documents. Ils sont également habilités à se faire communiquer la transcription des informations contenues dans les programmes informatiques des professionnels.

Enfin, il peut être procédé à toute constatation utile, notamment à partir d'un service de communication au public en ligne ou encore en consultant les données librement accessibles ou rendues accessibles, y compris par imprudence, par négligence ou par le fait d'un tiers. Ces données peuvent ainsi être retranscrites par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle.

En outre, les contrôles sur place doivent notamment respecter le principe de l'inviolabilité du domicile et respecter certains horaires.

Aux fins de préserver les droits de la défense, les contrôles *in situ* ne peuvent être effectués qu'en présence d'un représentant de la personne contrôlée. De même, toute personne convoquée peut se faire assister par un conseil de son choix.

Comme suite aux constatations, vérifications et visites menées en application de cet article, un procès-verbal est dressé contradictoirement lorsque les vérifications et visites sont effectuées sur place ou sur convocation.

En cas de manquement aux obligations prescrites par la loi et ses textes d'application, un rapport est adressé au Ministre d'État.

Les modalités d'application de cet article seront précisées dans une ordonnance souveraine.

L'article 10 prévoit, en cas de manquement aux obligations de la loi, constaté lors des contrôles, que le Ministre d'Etat transmet le rapport mentionné à l'article 9 à la Commission prévue à l'article 5, aux fins de recueillir son avis quant aux suites à donner et au prononcé éventuel d'une sanction.

La Commission est ainsi chargée de notifier les griefs susceptibles d'être formulés à la personne morale concernée et ses représentants légaux. L'article encadre également la procédure qui découle de cette transmission en prévoyant la possibilité de consultation des dossiers par les personnes mises en cause et l'assistance par un conseil. Le respect du contradictoire est garanti par une procédure d'échanges entre les représentants de la personne morale et la commission. Les représentants de la personne morale mise en cause sont convoqués par la commission en vue d'être entendus en leurs explications, ou dûment appelés à les fournir, étant précisé que toute audition donne lieu à la rédaction d'un procès-verbal consignant l'ensemble des explications.

La commission joue ici un rôle essentiel dans le dispositif, dans la mesure où il lui incombe de se prononcer sur la documentation fournie par l'émetteur et d'entendre les représentants de la société émettrice et, en cas de manquements avérés, de proposer une sanction.

Il importe au Gouvernement de relever que, sauf cas d'urgence conformément à l'article 11, aucune décision de révocation ou de suspension de l'autorisation ne pourra intervenir sans que cette commission n'ait entendu ou appelé le titulaire du label à faire valoir ses explications et rendu un avis préalable.

Des modalités complémentaires seront prévues par ordonnance souveraine.

Le Chapitre V, intitulé « *Des sanctions* » comprend les articles 11 à 15 et prévoit la possibilité de sanctions administratives et pénales.

L'article 11 prévoit, lorsque la personne morale ne respecte pas les conditions ou les limites de l'autorisation, ou si les fonds n'ont pas été placés sous séquestre ou encore dans l'hypothèse où l'offre ne serait plus conforme au « *white paper* » que le Ministre d'Etat puisse, sur proposition de la commission prévue par l'article 5, suspendre ou révoquer l'autorisation d'émettre une offre de jetons.

Il est ici question de s'assurer de ce que l'émetteur n'altère en aucune façon les conditions de l'offre, une fois l'autorisation délivrée. Il lui revient donc de définir précisément les modalités de l'offre et de veiller à la rédaction du *white paper*, lesquels devront être respectés lors de la réalisation de l'opération.

Le troisième alinéa permet au Ministre d'État, lorsque l'urgence le justifie, de suspendre provisoirement l'autorisation par décision motivée. Il appartiendra le cas échéant à l'émetteur, d'exercer un recours devant le Président du Tribunal de première instance statuant comme en matière de référé afin de solliciter la levée de la mesure prise par le Ministre d'Etat.

L'article 12 impose à l'émetteur de jetons de mettre un terme aux communications relatives à une offre dont l'autorisation aurait été suspendue ou révoquée. L'objectif est d'éviter qu'une offre qui ne satisferait plus les conditions de l'autorisation continue d'attiser l'intérêt de potentiels souscripteurs, voire que l'émetteur cherche à continuer de collecter frauduleusement des souscriptions sans y être autorisé.

L'article 13 permet au Ministre d'État de publier sur tout support approprié la ou les sanctions prononcées en application de l'article 11 sauf dans les cas où cette publication compromettrait une enquête pénale en cours ou lorsque le préjudice qui en résulterait serait disproportionné. Cette publication permet de renforcer le caractère dissuasif du dispositif, en particulier lorsqu'elle pourrait entraîner un préjudice réputationnel important pour l'émetteur.

Dans l'hypothèse où la publication compromettrait une enquête pénale ou ne serait disproportionnée que pour un court délai, le Ministre d'État peut décider de reporter cette publication à l'expiration de ce délai. Cette disposition permet de moduler l'application de la sanction dans le temps en évitant qu'une situation temporaire compromette l'efficacité du dispositif.

Enfin, tout ou partie des frais de publication peut être mis à la charge de la personne sanctionnée.

L'article 14 ajoute aux sanctions administratives une sanction pénale à l'encontre de toute personne ou des dirigeants des personnes morales qui procèdent ou tentent de procéder à une offre de jetons sans avoir obtenu préalablement l'autorisation d'y procéder. Dans la mesure où la sanction peut s'élever jusqu'au montant des fonds collectés, celle-ci apparaît proportionnée à la gravité de l'acte en cause. Une telle sanction est nécessaire pour assurer l'effectivité des obligations instituées par le présent projet de loi.

De même, une sanction pénale peut être prononcée à l'encontre des dirigeants des personnes morales qui procèdent ou tentent de procéder à une offre de jetons alors que l'autorisation dont ils étaient titulaires a été suspendue ou révoquée.

Ceux-ci encourent également une sanction pénale s'ils procèdent ou tentent de procéder à une offre de jetons autre que celle autorisée ou qui excède les limites de l'autorisation.

Les personnes morales déclarées responsables desdites infractions encourent une amende dont le montant est égal au quintuple de l'amende prévue pour leurs dirigeants.

L'article 15 vient compléter l'arsenal répressif en prévoyant une sanction pénale à l'encontre de toute personne faisant obstacle ou tentant de faire obstacle aux contrôles exercés en application de l'article 9 de la présente loi.

Enfin, le Chapitre VI intitulé « *Dispositions diverses et transitoires* » comprend les articles 16 et 17 venant poser d'une part, la soumission des sociétés titulaires d'une autorisation d'émission de jetons aux dispositions relatives à la règlementation en vigueur en matière de blanchiment et d'autre part, le délai de mise en conformité avec la présente loi.

L'article 16 soumet les sociétés titulaires d'une autorisation de procéder à une offre de jetons à l'ensemble des dispositions de la loi n° 1.362 du 3 août 2009 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption, modifiée.

Il incombera donc aux sociétés titulaires du label de respecter les obligations de vigilance définies par les dispositions légales et réglementaires en matière de lutte contre le blanchiment et le financement du terrorisme, de même que l'ensemble des prescriptions applicables en la matière.

Il est en effet apparu essentiel au Gouvernement de sécuriser les offres de jetons opérées par les sociétés installées sur son territoire au regard des risques en matière de blanchiment de capitaux et de financement du terrorisme.

De même, et à l'instar de la France, il échet également d'ajouter aux professionnels soumis à la loi n° 1.362 du 3 août 2009, modifiée, susmentionnée, toute personne qui, à titre de profession habituelle, se porte contrepartie ou agit en tant qu'intermédiaire en vue de l'acquisition ou de la vente d'actifs numériques.

Sont ici visées les plates-formes de conversion qui interviennent pour réaliser des opérations d'échange de crypto-monnaies contre de la monnaie légale, étant rappelé qu'une telle activité à Monaco nécessiterait la délivrance préalable d'un agrément de prestataire de service de paiement par l'Autorité de Contrôle Prudentiel et de Résolution (A.C.P.R.).

L'article 17 accorde un délai de six mois pour se mettre en conformité avec les dispositions de la présente loi, aux sociétés qui, au jour de l'entrée en vigueur de la loi, ont initié une offre de jetons sans toutefois que ceux-ci aient été émis. A cet égard, il leur incombe donc de déposer une demande de label dans les conditions des articles 4 à 7. A défaut, ils encourent les sanctions de l'article 11.

Tel est l'objet du présent projet de loi.

PROJET DE LOI

CHAPITRE I
DEFINITIONS

Article premier

Au sens de la présente loi on entend par :

- « *Actif numérique* » : des jetons tels que définis par la présente loi ainsi que toute représentation d'une valeur qui n'est pas émise ou garantie par une banque centrale ou par l'Etat, qui n'est pas nécessairement attachée à une monnaie ayant cour légal et qui ne possèdent pas le statut juridique d'une monnaie, mais qui est acceptée par des personnes physiques ou morales comme un moyen d'échange et qui peut être transférée, stockée ou échangée électroniquement ;

- « *Clé privée* » : mécanisme cryptographique permettant à son titulaire de signer des transactions dans le cadre d'un dispositif d'enregistrement numérique sur un registre partagé.

- « *Clé publique* » : mécanisme cryptographique permettant aux tiers de vérifier la signature de transactions réalisées dans un dispositif d'enregistrement numérique sur un registre partagé sans contraindre le signataire à révéler sa clé privée.

- « *Dispositif d'enregistrement numérique sur un registre partagé* » : un dispositif d'enregistrement numérique permettant de garantir la disponibilité, l'authentification, la traçabilité, l'intégrité, la confidentialité et la conservation des opérations ;

- « *Jeton* » : un bien incorporel, représentant sous un format numérique, un ou plusieurs droits, pouvant être émis, inscrits, conservés ou transférés au moyen d'un dispositif d'enregistrement numérique sur un registre partagé.

  Celui-ci peut représenter alternativement ou cumulativement :

  - une ou plusieurs des caractéristique(s) d'un instrument financier au sens de l'article 2 du Code de commerce ;

  - un droit d'usage sur des biens, des produits ou des services ;

  - une unité de valeur non monétaire.

- « *Offre de jetons* » : une proposition de souscrire à un ou plusieurs jetons, lesquels seront émis en utilisant un dispositif d'enregistrement numérique sur un registre partagé.

- « *Protocole contractuel numérique* » : un programme informatique utilisant un dispositif d'enregistrement numérique sur un registre partagé et permettant d'exécuter automatiquement une série d'actions prédéterminées lorsque les conditions prédéfinies dans le programme sont réunies ;

CHAPITRE II
REGIME ET FORCE PROBANTE

Article 2

Toute information enregistrée dans un dispositif d'enregistrement numérique sur un registre partagé vaut présomption simple de son existence, de son contenu et de sa date, jusqu'à preuve contraire sous réserve du respect des exigences fixées par ordonnance souveraine.

Article 3

Toute action réalisée au sein d'un dispositif d'enregistrement numérique sur un registre partagé au moyen d'une clé privée, vérifiée par la clé publique correspondante, est présumée l'avoir été par le titulaire de ladite clé privée jusqu'à preuve contraire.

CHAPITRE III
DES OFFRES DE JETONS

Article 4

Une offre de jetons peut être privée ou publique dans les conditions fixées par ordonnance souveraine.

Une offre au public sur des jetons revêtant une ou plusieurs caractéristiques d'instruments financiers réalisée par une personne morale domiciliée à Monaco est prohibée.

Il appartient à l'émetteur de déterminer :

- la nature du jeton à émettre et les droits y afférents et ;

- le caractère public ou privé de l'émission.

Article 5

La réalisation d'une offre de jetons est subordonnée à l'obtention d'un label revêtant la forme d'une autorisation administrative préalable délivrée par le Ministre d'Etat, après avis motivé d'une commission chargée d'instruire la demande d'autorisation, dont la composition est précisée par ordonnance souveraine.

La commission se prononce après réception des pièces constitutives de la demande d'autorisation parmi lesquelles figure notamment un document destiné à l'information des souscripteurs, portant sur l'émetteur et les risques présentés par l'offre. Le contenu dudit recueil doit être clair, exact et non trompeur.

La liste des pièces à joindre à la demande d'autorisation est précisée par ordonnance souveraine.

La commission peut entendre les représentants de la société émettrice ainsi que toute personne dont elle estime l'audition utile.

Article 6

Seule une personne morale immatriculée à Monaco peut présenter une offre de jetons.

Lorsque les jetons revêtent une ou plusieurs caractéristiques d'un instrument financier, l'offre ne peut être présentée que par une société par actions.

Dans le cadre de l'offre de jetons, la personne morale visée au premier alinéa devra notamment proposer des moyens permettant la sauvegarde des actifs et des fonds recueillis ainsi que le suivi de leur utilisation en conformité avec le projet présenté dans la demande d'autorisation.

Article 7

Les fonds collectés dans le cadre d'une offre de jetons sont placés sous séquestre à compter de l'émission des jetons pendant la durée de l'opération dans les conditions prévues par ordonnance souveraine.

En cas de révocation de l'autorisation, d'abandon du projet présenté ou lorsque le montant minimum n'est pas atteint, les fonds séquestrés sont restitués aux souscripteurs.

CHAPITRE IV
DU CONTROLE DE LA REGULARITE DES OFFRES DE JETONS

Article 8

Le contrôle de l'application des dispositions du Chapitre III et des mesures prises pour son application, est exercé par les agents de la Direction de l'Expansion Economique, spécialement commissionnés et assermentés à cet effet.

Dans l'exercice de ces contrôles, les agents visés au précédent alinéa ainsi que tout expert dont ils s'assurent le concours sont tenus au secret professionnel dans les conditions de l'article 308 du Code pénal. Ils sont en outre liés par l'obligation de discrétion pour tout ce qui concerne les faits et informations dont ils ont connaissance dans l'exercice de leurs fonctions.

L'expert ainsi désigné ainsi que les agents de la Direction de l'Expansion Economique ne doivent pas se trouver en situation de conflit d'intérêts avec les personnes contrôlées.

Article 9

A l'effet d'exercer la mission qui leur est dévolue, les agents peuvent effectuer des contrôles sur pièces et sur place, sans que le secret professionnel ne puisse leur être opposé sauf en ce qui concerne les informations couvertes par le secret applicable aux relations entre un avocat et son client, et notamment :

1°) se faire communiquer tous documents professionnels, quel qu'en soit le support, qu'ils estiment utiles à l'exercice de leur mission dont ils peuvent prendre copie par tous moyens ;

2°) convoquer et entendre toute personne susceptible de leur fournir des informations le cas échéant par un système de visioconférence ou d'audioconférence ;

3°) accéder aux locaux professionnels ou à usage professionnel à l'exclusion des parties de ceux-ci affectées au domicile privé et procéder à toutes les opérations de vérification qu'ils estiment nécessaires ;

4°) recueillir des explications sur place auprès des dirigeants ainsi que de toute personne, tous renseignements, documents ou justificatifs utiles à l'accomplissement de leur mission ;

5°) se faire communiquer la transcription, par tout traitement approprié, des informations contenues dans les programmes informatiques des professionnels, dans des documents directement utilisables pour les besoins du contrôle ainsi que la conservation de cette transcription sur un support adéquat ;

6°) ils peuvent à partir d'un service de communication au public en ligne, consulter les données librement accessibles ou rendues accessibles, y compris par imprudence, négligence ou par le fait d'un tiers, le cas échéant en accédant et en se maintenant dans des systèmes de traitement automatisé d'information le temps nécessaire aux constatations ; ils peuvent retranscrire les données par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle.

Dans le cadre des contrôles, la visite des locaux professionnels ou à usage professionnel, à l'exclusion des parties de ceux-ci affectés au domicile privé, ne peut être effectuée qu'entre six et vingt-et-une heures, ou, en dehors de ces heures, lorsque l'accès au public est autorisé ou lorsqu'une activité professionnelle est en cours. Cette visite ne peut en outre avoir lieu qu'en présence d'un représentant de la personne contrôlée.

Toute personne convoquée ou entendue a le droit de se faire assister d'un conseil de son choix.

A l'issue du contrôle sur place, les agents de la Direction de l'Expansion Economique rédigent le procès-verbal des constatations opérées, avec la précision de la nature, la date et du lieu de celles-ci. Il est signé par le ou les agents et par la personne concernée par les investigations. En cas de refus de celle-ci, mention en est faite au procès-verbal.

Indépendamment de ce procès-verbal, et lorsque des manquements sont constatés aux obligations prescrites par la présente loi et ses textes d'application, les agents mentionnés au premier alinéa consignent dans un rapport au Ministre d'État les opérations auxquelles ils ont procédé au cours de leurs contrôles.

Les modalités d'application du présent article sont précisées par ordonnance souveraine.

Article 10

Le rapport consignant les manquements constatés par les agents de la Direction de l'Expansion Economique lors du contrôle est transmis par le Ministre d'Etat, à la commission visée à l'article 5.

La personne mise en cause est informée par la commission, par tout moyen écrit, des griefs susceptibles d'être formulés à son encontre.

Lorsque les griefs sont notifiés à une personne morale, ils le sont également à ses représentants légaux.

La notification des griefs précise que la personne mise en cause peut prendre connaissance du contenu du dossier auprès de la commission et se faire assister à cette fin par un conseil de son choix.

La personne mise en cause est convoquée par la commission en vue d'être entendue en ses explications, ou dûment appelée à les fournir.

Lors de son audition, la personne mise en cause peut être assistée du conseil de son choix. Ses explications sont consignées dans un rapport établi par la commission, dans lequel celle-ci émet un avis sur l'existence d'un manquement, et dans l'affirmative, formule une proposition de sanction.

La commission délibère hors la présence du rapporteur désigné de l'affaire.

Les modalités d'application du présent article sont précisées par ordonnance souveraine.

CHAPITRE V
DES SANCTIONS

Section I
Des sanctions administratives

Article 11

Lorsqu'un manquement tenant notamment à la mise en œuvre d'une offre de jetons en méconnaissance des conditions ou des limites de l'autorisation prévue à l'article 5 est avéré, ou s'il advient que l'offre n'est plus conforme au document d'information prévu au même article, le Ministre d'Etat peut, sur proposition de la commission prévue à l'article 5, mettre fin à l'offre de jetons en révoquant l'autorisation visée à l'article 5 ou en suspendre les effets.

La décision privant d'effets ou suspendant les effets d'une autorisation ne peut être prise qu'après avis de la commission visée à l'article 5 conformément à l'article 10.

Toutefois, lorsque l'urgence le justifie, le Ministre d'État peut suspendre l'autorisation à titre provisoire par décision motivée sans que la commission soit saisie. Dans ce cas, toute personne intéressée à laquelle les mesures prescrites font grief, peut demander au Président du Tribunal de première instance saisi et statuant comme en matière de référé, d'ordonner la levée desdites mesures.

L'exercice de poursuites pénales n'ayant pas abouti à une décision de justice passée en force de chose jugée ne fait pas obstacle à l'application du présent article.

Les modalités d'application du présent article sont précisées par ordonnance souveraine.

Article 12

La décision privant d'effets ou suspendant les effets de l'autorisation visée à l'article 5 entraîne pour la personne autorisée l'obligation de mettre fin à toute communication concernant l'offre.

Article 13

Le Ministre d'État peut décider de procéder à la publication de sa décision au Journal de Monaco et, le cas échéant, sur tout autre support papier ou numérique.

Toutefois, les sanctions administratives prononcées par le Ministre d'État sont publiées de manière anonyme dans les cas suivants :

1°) lorsque la publication sous une forme non anonyme compromettrait une enquête pénale en cours ;

2°) lorsque le préjudice qui résulterait d'une publication sous une forme non anonyme serait disproportionné.

Lorsque les situations mentionnées aux chiffres 1°) et 2°) sont susceptibles de cesser d'exister dans un court délai, le Ministre d'État peut décider de différer la publication pendant ce délai.

Il peut également décider de mettre à la charge de la personne sanctionnée tout ou partie des frais de la publication visée à l'alinéa premier.

Section II
Des sanctions pénales

Article 14

Sont punis de l'amende prévue au chiffre 4° de l'article 26 du Code pénal dont le maximum peut être porté jusqu'au montant du profit éventuellement réalisé :

1°) les personnes ou les dirigeants des personnes morales qui procèdent ou qui tentent de procéder à une offre de jetons sans l'autorisation visée à l'article 5 ;

2°) les dirigeants des personnes morales qui procèdent ou qui tentent de procéder à une offre de jetons alors que l'autorisation dont ils étaient titulaires au titre de l'article 5 a été suspendue ou révoquée ;

3°) les dirigeants des personnes morales qui procèdent ou qui tentent de procéder à une offre de jetons autre que celle autorisée ou qui excède les limites déterminées par l'autorisation ou qui n'est pas conforme aux conditions mentionnées par celle-ci.

Les personnes morales déclarées responsables des infractions prévues au présent article encourent une amende dont le montant est égal au quintuple de l'amende prévue pour les dirigeants des personnes morales visées au précédent alinéa.

Article 15

Sont punis d'un emprisonnement d'un à six mois et de l'amende prévue au chiffre 4 de l'article 26 du Code pénal ou de l'une de ces deux peines seulement les dirigeants ainsi que toute personne qui font obstacle ou tentent de faire obstacle aux contrôles exercés en application de l'article 9 de la présente loi.

Les personnes morales déclarées responsables de l'infraction prévue au précédent alinéa encourent une amende dont le montant est égal au quintuple de l'amende prévue pour les dirigeants des personnes morales visées au dit alinéa.

CHAPITRE VI
DISPOSITIONS DIVERSES ET TRANSITOIRES

Article 16

Sont ajoutés à l'article premier de la loi n° 1.362 du 3 août 2009, modifiée, les chiffres 21°et 22°), rédigés comme suit :

« 21°) les personnes morales titulaires de l'autorisation de procéder à une offre de jetons visée à l'article 5 de la loi n° XXX du XXX ;

22 °) toute personne qui, à titre de profession habituelle, soit se porte elle-même contrepartie, soit agit en tant qu'intermédiaire, en vue de l'acquisition ou de la vente d'actifs numériques pouvant être conservées ou transférées dans le but d'acquérir un bien ou un service, mais ne représentant pas de créance sur l'émetteur ».

Article 17

Les personnes qui au jour de l'entrée en vigueur de la présente loi, ont initié une offre de jetons qui n'a pas encore donné lieu à leur émission, disposent d'un délai de six mois pour se conformer aux dispositions de la présente loi.

ANNEXE N°5

APRÈS ART. 40 **N° 434**

ASSEMBLÉE NATIONALE

15 août 2018

CROISSANCE ET TRANSFORMATION DES ENTREPRISES - (N° 1088)

Non soutenu

AMENDEMENT

N º 434

présenté par
M. Besson-Moreau

ARTICLE ADDITIONNEL

APRÈS L'ARTICLE 40, insérer l'article suivant:

Après l'unique alinéa de l'article 1358 du code civil, il est inséré un alinéa ainsi rédigé :

« Lorsqu'il est électronique, le moyen consiste notamment en l'usage d'un dispositif électronique d'enregistrement partagé, de nature publique ou privé, dès lors que ledit dispositif électronique d'enregistrement partagé répond à des conditions définies par décret en Conseil d'État. »

EXPOSÉ SOMMAIRE

A l'heure où, dans le monde entier, la « Blockchain » est adoptée par les États et les acteurs privés comme mode de preuve de l'existence et de la datation des éléments qui s'y trouvent enregistrés, la France, pionnière dans sa législation sous la dénomination de « Dispositif Électronique d'Enregistrement Partagé », doit, pour des motifs de sécurité juridique, en favoriser sa réception par ses acteurs économiques comme ses juridictions.

Afin d'éviter de fastidieuses, inutiles, longues et coûteuses expertises judiciaires, lesquelles nuiraient à la rentabilité économique de ces registres numériques d'un genre nouveau, nous proposons l'adoption du présent article, ce qui constituerait un signal fort pour la communauté de ses utilisateurs et un facilitateur pour nos juridictions.

En particulier, elle facilite l'établissement de la preuve de l'origine, de la date et de la nature des apports et contributions intellectuelles dans les processus d'innovation collaborative, pour lesquelles les enquêtes montrent que la crainte du vol ou du détournement de la propriété intellectuelle constitue un frein majeur.

Les juridictions sont également demanderesses de simplicité et de rapidité de traitement des contentieux à venir, répondant ainsi à l'objectif de désengorgement des services de la Justice, qui pourraient être redéployés sur des missions à plus forte valeur ajoutée.

Afin de s’assurer d’un contrôle par l’État des qualités essentielles que devront présenter les Dispositifs Électroniques d’Enregistrement Partagé bénéficiaires de la présomption de preuve ainsi édictée, un Décret en Conseil d’État en fixera les contours et conditions.

ASSEMBLÉE NATIONALE

30 août 2018

CROISSANCE ET TRANSFORMATION DES ENTREPRISES - (N° 1088)

Rejeté

AMENDEMENT

N º 773

présenté par
M. Fasquelle, M. Sermier, M. Vialay, Mme Beauvais, M. Gosselin, M. Menuel, Mme Levy, M. Dive, Mme Anthoine, M. Pauget, Mme Trastour-Isnart, M. Thiériot, M. Viry, M. Cherpion et M. Emmanuel Maquet

---

ARTICLE ADDITIONNEL

APRÈS L'ARTICLE 40, insérer l'article suivant:

Après l'unique alinéa de l'article 1358 du code civil, il est inséré un alinéa ainsi rédigé :

« Lorsqu'il est électronique, le moyen consiste notamment en l'usage d'un dispositif électronique d'enregistrement partagé, de nature publique ou privé, dès lors que ledit dispositif électronique d'enregistrement partagé répond à des conditions définies par décret en Conseil d'État. »

EXPOSÉ SOMMAIRE

À l'heure où, dans le monde entier, la « Blockchain » est adoptée par les États et les acteurs privés comme mode de preuve de l'existence et de la datation des éléments qui s'y trouvent enregistrés, la France, pionnière dans sa législation sous la dénomination de « Dispositif Électronique d'Enregistrement Partagé », doit, pour des motifs de sécurité juridique, en favoriser sa réception par ses acteurs économiques comme ses juridictions.

Afin d'éviter de fastidieuses, inutiles, longues et coûteuses expertises judiciaires, lesquelles nuiraient à la rentabilité économique de ces registres numériques d'un genre nouveau, nous proposons l'adoption du présent article, ce qui constituerait un signal fort pour la communauté de ses utilisateurs et un facilitateur pour nos juridictions.

En particulier, elle facilite l'établissement de la preuve de l'origine, de la date et de la nature des apports et contributions intellectuelles dans les processus d'innovation collaborative, pour lesquelles les enquêtes montrent que la crainte du vol ou du détournement de la propriété intellectuelle constitue un frein majeur.

Les juridictions sont également demanderesses de simplicité et de rapidité de traitement des contentieux à venir, répondant ainsi à l'objectif de désengorgement des services de la Justice, qui pourraient être redéployés sur des missions à plus forte valeur ajoutée.

Afin de s’assurer d’un contrôle par l’État des qualités essentielles que devront présenter les Dispositifs Électroniques d’Enregistrement Partagé bénéficiaires de la présomption de preuve ainsi édictée, un Décret en Conseil d’État en fixera les contours et conditions.

ASSEMBLÉE NATIONALE

3 septembre 2018

CROISSANCE ET TRANSFORMATION DES ENTREPRISES - (N° 1088)

Non soutenu

AMENDEMENT

N º 1309

présenté par
M. Hetzel et M. Viala

ARTICLE ADDITIONNEL

APRÈS L'ARTICLE 40, insérer l'article suivant:

Après l'unique alinéa de l'article 1358 du code civil, il est inséré un alinéa ainsi rédigé :

« Lorsqu'il est électronique, le moyen consiste notamment en l'usage d'un dispositif électronique d'enregistrement partagé, de nature publique ou privé, dès lors que ledit dispositif électronique d'enregistrement partagé répond à des conditions définies par décret en Conseil d'État. »

EXPOSÉ SOMMAIRE

A l'heure où, dans le monde entier, la « Blockchain » est adoptée par les États et les acteurs privés comme mode de preuve de l'existence et de la datation des éléments qui s'y trouvent enregistrés, la France, pionnière dans sa législation sous la dénomination de « Dispositif Électronique d'Enregistrement Partagé », doit, pour des motifs de sécurité juridique, en favoriser sa réception par ses acteurs économiques comme ses juridictions.

Afin d'éviter de fastidieuses, inutiles, longues et coûteuses expertises judiciaires, lesquelles nuiraient à la rentabilité économique de ces registres numériques d'un genre nouveau. L'adoption d'une telle mesure constituerait un signal fort pour la communauté de ses utilisateurs et un facilitateur pour nos juridictions.

En particulier, elle faciliterait l'établissement de la preuve de l'origine, de la date et de la nature des apports et contributions intellectuelles dans les processus d'innovation collaborative, pour lesquelles les enquêtes montrent que la crainte du vol ou du détournement de la propriété intellectuelle constitue un frein majeur.

Les juridictions sont également demanderesses de simplicité et de rapidité de traitement des contentieux à venir, répondant ainsi à l'objectif de désengorgement des services de la Justice, qui pourraient être redéployés sur des missions à plus forte valeur ajoutée.

Afin de s'assurer d'un contrôle par l'État des qualités essentielles que devront présenter les Dispositifs Électroniques d'Enregistrement Partagé bénéficiaires de la présomption de preuve ainsi édictée, un Décret en Conseil d'État en fixera les contours et conditions.

ANNEXE N°6

ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Compte rendu

Commission spéciale chargée d'examiner le projet de loi relatif à la croissance et la transformation des entreprises

Jeudi
13 septembre 2018
Séance de 15 heures

Compte rendu n° 18

SESSION EXTRAORDINAIRE DE 2017-2018

Présidence de Mme Olivia Grégoire, *Présidente*

ASSEMBLÉE NATIONALE

*La commission **adopte** l'amendement de précision CS653 de la rapporteure.*

*Puis elle **adopte** l'article 40 **modifié**.*

Après l'article 40

La commission examine ensuite l'amendement CS773 de M. Daniel Fasquelle.

M. Daniel Fasquelle. À l'heure où, dans le monde entier, la *blockchain* est adoptée par les États et les acteurs privés comme mode de preuve de l'existence et de la datation des éléments qui s'y trouvent enregistrés, la France, pionnière dans sa législation sous la dénomination de « *dispositif électronique d'enregistrement partagé* », doit, pour des motifs de sécurité juridique, en favoriser la réception par les acteurs économiques comme par les juridictions. Afin d'éviter de fastidieuses, inutiles, longues et coûteuses expertises judiciaires, lesquelles nuiraient à la rentabilité économique de ces registres numériques d'un genre nouveau, nous proposons l'adoption du présent article, ce qui constituerait un signal fort pour la communauté de ses utilisateurs et un facilitateur pour nos juridictions. Je ne comprends pas que ce sujet très important n'ait pas été traité dès l'abord dans le cadre du projet de loi. Nous avons cet après-midi l'occasion de réparer une telle lacune.

Mme Marie Lebec, rapporteure. Avis défavorable, dans la mesure où cela relève moins de la loi que de l'usage. Il ne me paraît pas utile de détailler les moyens électroniques concernés.

M. Bruno Le Maire, ministre de l'économie et des finances. M. Fasquelle a raison de souligner l'importance de l'utilisation de la *blockchain* dans l'établissement de la preuve de l'inventivité d'un brevet ou de toute autre forme d'invention. Mais nous traitons bien cette question dans le projet de loi PACTE, puisque nous avons adopté hier des mesures permettant d'encadrer les levées de fonds par jetons, les ICO *(Initial coin offering*), et que nous serons l'un des premiers pays en Europe à avoir un cadre juridique protégeant ces levées de fonds qui utilisent la *blockchain*. Même si le terme n'apparaissait pas, c'est bien dans un tel cadre que nous nous inscrivions.

Par ailleurs, le code civil prévoit explicitement que la preuve de l'origine, de la date et de la nature des contributions intellectuelles peut être apportée par tout moyen, sans n'en mentionner aucun à dessein. La rédaction actuelle du code civil présentant l'avantage d'une plus grande souplesse et couvrant, par définition, la *blockchain* ou toute autre forme de preuve qui pourrait être mise à disposition, je vous suggère de retirer votre amendement.

M. Daniel Fasquelle. C'est la preuve des faits qui se rapporte par tout moyen dans le code civil. S'agissant du reste, nous avons un système de preuves écrites relativement structuré et élaboré, qui s'est toujours adapté aux nouvelles techniques et aux nouvelles pratiques économiques. Je ne peux donc pas me satisfaire de votre réponse, monsieur le ministre. Vous avez dit que nous avions traité hier du sujet des monnaies électroniques. Soit ! Mais il n'englobe pas toute la question de la *blockchain*.

Quant à dire, madame la rapporteure, que cela relève de la coutume et des usages et n'a pas à être encadré par le droit, avouez que c'est très court comme réponse...

*La commission **rejette** l'amendement.*

Puis elle en vient à l'amendement CS1085 de M. Jean-Marc Zulesi.

Membres présents ou excusés

Commission spéciale chargée d'examiner le projet de loi relatif à la croissance et la transformation des entreprises

Réunion du jeudi 13 septembre 2018 à 15 heures

Présents. – M. Patrice Anato, M. Didier Baichère, M. Jean-Noël Barrot, Mme Marie-Noëlle Battistel, Mme Sophie Beaudouin-Hubiere, M. Philippe Bolo, M. Ian Boucard, Mme Anne-France Brunet, M. Anthony Cellier, M. Philippe Chassaing, M. Charles de Courson, M. Pierre Dharréville, Mme Coralie Dubost, M. M'jid El Guerrab, M. Daniel Fasquelle, M. Éric Girardin, Mme Olga Givernet, Mme Valérie Gomez-Bassac, Mme Olivia Gregoire, M. Stanislas Guerini, Mme Nadia Hai, M. François Jolivet, M. Guillaume Kasbarian, Mme Fadila Khattabi, M. Michel Lauzzana, Mme Célia de Lavergne, Mme Marie Lebec, M. Roland Lescure, Mme Graziella Melchior, Mme Patricia Mirallès, M. Patrice Perrot, M. Laurent Pietraszewski, M. Dominique Potier, M. Laurent Saint-Martin, M. Jacques Savatier, M. Denis Sommer, M. Adrien Taquet, M. Boris Vallaud, Mme Marie-Christine Verdier-Jouclas, M. Éric Woerth, M. Jean-Marc Zulesi

Excusés. – Mme Élodie Jacquier-Laforge, M. Arnaud Viala

Assistaient également à la réunion. – M. Damien Adam, Mme Isabelle Florennes, Mme Christine Hennion, M. Hubert Julien-Laferriere, M. Denis Masséglia, M. Stéphane Peu, M. Damien Pichereau

ANNEXE N°7

APRÈS ART. 40 **N° 1317**

ASSEMBLÉE NATIONALE

3 septembre 2018

CROISSANCE ET TRANSFORMATION DES ENTREPRISES - (N° 1088)

AMENDEMENT

N º 1317

présenté par
M. Mis, Mme Hérin, M. Rudigoz, Mme Le Peih, M. Buchou, M. Son-Forget, Mme Gipson, Mme Couillard, M. Martin, M. Cesarini, Mme Cazarian, M. Trompille, M. Tan, M. Bois, M. Borowczyk, Mme Frédérique Dumas et Mme Fontenel-Personne

---

ARTICLE ADDITIONNEL

APRÈS L'ARTICLE 40, insérer l'article suivant:

Après l'unique alinéa de l'article 1358 du code civil, insérer un alinéa ainsi rédigé :

« A cet effet, tout fichier numérique enregistré dans un dispositif électronique d'enregistrement partagé (DEEP), de nature publique ou privée vaut preuve de son existence et de sa date, jusqu'à preuve contraire, dès lors que ledit DEEP répond à des conditions définies par décret ».

EXPOSÉ SOMMAIRE

Cet amendement vise à reconnaitre valeur de preuve à tout fichier numérique enregistré dans un Dispositif Électronique d'Enregistrement Partagé, de nature publique ou privée afin de sécuriser les opérations effectuées par les entreprises utilisant ce DEEP.

A l'heure où, dans le monde entier, la « Blockchain » est adoptée par les États et les acteurs privés comme mode de preuve de l'existence et de la datation des éléments qui s'y trouvent enregistrés, la France, pionnière dans sa législation sous la dénomination de « Dispositif Électronique d'Enregistrement Partagé », doit, pour des motifs de sécurité juridique, en favoriser sa réception par ses acteurs économiques comme devant les diverses juridictions. En effet, à l'heure où nous souhaitons favoriser et protéger l'expérimentation de nos entreprises nous devons pouvoir lever leurs craintes quant à la valeur juridique des échanges ou des solutions qu'elles proposent lorsqu'elles sont supportées par un DEEP.

Afin d'éviter de fastidieuses, inutiles, longues et coûteuses expertises judiciaires, lesquelles nuiraient à la rentabilité économique de ces registres numériques d'un genre nouveau cet amendement est aussi un moyen d'envoyer un signal fort à la communauté des utilisateurs de ce DEEP, qui d'ailleurs a déjà investi le droit des titres financiers avec l'ordonnance relative à la transmission et la représentation de titres financiers au moyen d'un DEEP,ou bien encore à l'instar de ce qui a été réalisé en matière de mini bons.

Les avantages de cette preuve par DEEP sont nombreux :

- La traçabilité : l'ancrage de l'empreinte de données permet de se pré-constituer facilement une preuve (ex : preuve de l'antériorité d'une œuvre, preuve d'une répartition des droits à l'origine des contributions d'une œuvre collective, preuve d'une chaîne de droits qui ne sera pas falsifiable, preuve en matière de supplychain, …).

- Le coût : l'inscription d'une information dans la blockchain est moins coûteuse qu'un constat d'huissier, un dépôt chez le notaire ou auprès d'agents assermentés.

- La désintermédiation : les éléments de preuve sont attachés à une transaction - validée selon un consensus au sein du réseau (variable selon le protocole) - qui ne requiert pas en principe l'intervention d'un tiers de confiance.

- La fluidité : certaines preuves traditionnelles manquent de fluidité, peuvent se révéler lourdes administrativement avec un formalisme contraignant. La blockchain quant à elle fonctionne souvent grâce une plateforme interface qui permet simplement d'ancrer une donnée.

- L'accès au registre : il est disponible sans limites géographiques ou temporelles.

Par ailleurs, les juridictions étant demandeuses de simplicité et de rapidité de traitement des contentieux à venir, cet amendement permet de répondre à l'objectif de désengorgement des services de la Justice, qui pourraient être redéployés sur des missions à plus forte valeur ajoutée.

Afin de s'assurer d'un contrôle par l'État des qualités essentielles que devront présenter les DEEP bénéficiaires de la présomption de preuve ainsi édictée, un Décret en Conseil d'État en fixera les contours et conditions.

ASSEMBLÉE NATIONALE

31 octobre 2018

LOI DE PROGRAMMATION 2019-2022 ET DE RÉFORME POUR LA JUSTICE - (N° 1349)

Retiré

AMENDEMENT

N º CL380

présenté par
M. Mis, M. Borowczyk, M. Vignal, Mme Sarles, Mme Thourot, Mme Bureau-Bonnard, M. Jacques, Mme Tuffnell, Mme Vanceunebrock-Mialon, M. Rebeyrotte, M. Rudigoz, M. Galbadon, M. Fauvergue, M. Pont, M. Blanchet, M. Freschi, Mme Abba, Mme Hérin et Mme Brugnera

---

ARTICLE ADDITIONNEL

APRÈS L'ARTICLE 14, insérer l'article suivant:

L'article 1358 du Code civil est complété par un alinéa ainsi rédigé :

« A cet effet, tout fichier numérique enregistré dans un dispositif électronique d'enregistrement partagé de nature publique ou privée vaut preuve de son existence et de sa date, jusqu'à preuve contraire, dès lors qu'il répond à des conditions définies par décret ».

EXPOSÉ SOMMAIRE

Cet amendement vise à reconnaitre valeur de preuve à tout fichier numérique enregistré dans un Dispositif Électronique d'Enregistrement Partagé, de nature publique ou privée afin de sécuriser les opérations effectuées par les entreprises utilisant ce DEEP.

A l'heure où, dans le monde entier, les registres distribués et dématérialisés sont adoptés par les États et les acteurs privés comme mode de preuve de l'existence et de la datation des éléments qui s'y trouvent enregistrés, la France, pionnière dans sa législation sous la dénomination de « Dispositif Électronique d'Enregistrement Partagé », doit, pour des motifs de sécurité juridique, en favoriser leur réception par les acteurs économiques comme devant les diverses juridictions. En effet, à l'heure où nous souhaitons favoriser et protéger l'expérimentation de nos entreprises nous devons pouvoir lever leurs craintes quant à la valeur juridique des échanges ou des solutions qu'elles proposent lorsqu'elles sont supportées par un DEEP.

Afin d'éviter de fastidieuses, inutiles, longues et coûteuses expertises judiciaires, lesquelles nuiraient à la rentabilité économique de ces registres numériques, cet amendement est aussi un moyen d'envoyer un signal fort à la communauté des utilisateurs de ce DEEP, qui d'ailleurs a déjà investi le droit des titres financiers avec l'ordonnance relative à la transmission et la représentation de titres financiers au moyen d'un DEEP,ou bien encore à l'instar de ce qui a été réalisé en matière de mini bons.

Les avantages de cette preuve par DEEP sont nombreux :

- La traçabilité : l'ancrage de l'empreinte de données permet de se pré-constituer facilement une preuve (ex : preuve de l'antériorité d'une œuvre, preuve d'une répartition des droits à l'origine des contributions d'une œuvre collective, preuve d'une chaîne de droits qui ne sera pas falsifiable, preuve en matière de supplychain, …).

- Le coût : l'inscription d'une information dans un registre distribué est moins coûteuse qu'un constat d'huissier, un dépôt chez le notaire ou auprès d'agents assermentés.

- La désintermédiation : les éléments de preuve sont attachés à une transaction - validée selon un consensus au sein du réseau (variable selon le protocole) - qui ne requiert pas en principe l'intervention d'un tiers de confiance.

- La fluidité : certaines preuves traditionnelles manquent de fluidité, peuvent se révéler lourdes administrativement avec un formalisme contraignant. Le registre distribué quant à lui fonctionne souvent grâce à une plateforme interface qui permet simplement d'ancrer une donnée.

- L'accès au registre : il est disponible sans limites géographiques ou temporelles.

Par ailleurs, les juridictions étant demandeuses de simplicité et de rapidité de traitement des contentieux à venir, cet amendement permet de répondre à l'objectif de désengorgement des services de la Justice, qui pourraient être redéployés sur des missions à plus forte valeur ajoutée.

Afin de s'assurer d'un contrôle par l'Etat des qualités essentielles que devront présenter les DEEP bénéficiaires de la présomption de preuve ainsi édictée, un Décret en Conseil d'Etat en fixera les contours et conditions.

ANNEXE N°8

Public Act 101-0514

HB3575 Enrolled LRB101 11071 RJF 56276 b

AN ACT concerning business.

Be it enacted by the People of the State of Illinois, represented in the General Assembly:

Section 1. Short title. This Act may be cited as the Blockchain Technology Act.

Section 5. Definitions. As used in this Act:

"Blockchain" means an electronic record created by the use of a decentralized method by multiple parties to verify and store a digital record of transactions which is secured by the use of a cryptographic hash of previous transaction information.

"Cryptographic hash" means a mathematical algorithm which performs a one-way conversion of input data into output data of a specified size to verify the integrity of the data.

"Electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

"Electronic record" means a record created, generated, sent, communicated, received, or stored by electronic means, including a blockchain or a smart contract.

"Record" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

"Smart contract" means a contract stored as an electronic record which is verified by the use of a blockchain.

Section 10. Permitted use of blockchain.

(a) A smart contract, record, or signature may not be denied legal effect or enforceability solely because a blockchain was used to create, store, or verify the smart contract, record, or signature.

(b) In a proceeding, evidence of a smart contract, record, or signature must not be excluded solely because a blockchain was used to create, store, or verify the smart contract, record, or signature.

(c) If a law requires a record to be in writing, submission of a blockchain which electronically contains the record satisfies the law.

(d) If a law requires a signature, submission of a blockchain which electronically contains the signature or verifies the intent of a person to provide the signature satisfies the law.

Section 15. Limitations to the use of blockchain.

(a) If parties have agreed to conduct a transaction by use of a blockchain and a law requires that a contract or other record relating to the transaction be in writing, the legal effect, validity, or enforceability of the contract or other record may be denied if the blockchain containing an electronic

record of the transaction is not in a form that is capable of being retained and accurately reproduced for later reference by all parties or other persons who are entitled to retain the contract or other record.

(b) Except as otherwise provided in subsection (f), if a law other than this Act requires a record to be posted or displayed in a certain manner, to be sent, communicated, or transmitted by a specified method, or to contain information that is formatted in a certain matter, the use of a blockchain to post, display, send, communicate, transmit, or store such a record does not satisfy the requirement of the other law.

(c) If a person inhibits the ability of another person to store or retrieve information contained in a blockchain, such information is not enforceable by the person who inhibited the storage or retrieval.

(d) Regardless of whether a smart contract was used to establish the relationship between the parties to an agreement, a requirement that a notice or an acknowledgment or other response to a notice be in writing is not satisfied by providing or delivering the notice or recording an acknowledgment or other response to the notice by the use of a blockchain if the notice is a notice of:

(1) the cancellation or termination of service by a public utility;

(2) default, acceleration, repossession, foreclosure, or eviction, or the right to cure, under a credit agreement

secured by or a rental agreement for, a primary residence of a natural person;

(3) the cancellation or termination of a policy of health insurance, benefits received under a policy of health insurance, or benefits received under a policy of life insurance, excluding annuities; or

(4) the recall of a product, or material failure of a product, that risks endangering the health or safety of a person.

(e) A requirement that a document be in writing is not satisfied by the use of a blockchain if the document is required to accompany any transportation or handling of hazardous materials, pesticides, or other toxic or dangerous materials.

(f) The requirements of this Section may not be varied by agreement, except that:

(1) to the extent a law other than this Act requires that a contract or other record relating to a transaction be in writing, but permits that requirement to be varied by agreement, the provisions of subsection (a) concerning the denial of legal effect, validity, or enforceability of the contract or other record relating to the transaction may also be varied by agreement; and

(2) a requirement under a law other than this Act to send, communicate, or transmit a record by first-class mail, postage prepaid, or regular United States mail, may

be varied by agreement to the extent permitted by the other law.

Section 20. Local government restrictions.

(a) A unit of local government shall not:

(1) impose any tax or fee on the use of a blockchain or smart contract by any person or entity;

(2) require any person or entity to obtain from the unit of local government any certificate, license, or permit to use a blockchain or smart contract; or

(3) impose any other requirement relating to the use of a blockchain or smart contract by any person or entity.

(b) Nothing in this Section prohibits a unit of local government from using a blockchain or smart contract in the performance of its powers or duties in a manner not inconsistent with the provisions of this Act.

ANNEXE N°9

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE LA JUSTICE

DIRECTION
DES AFFAIRES CRIMINELLES ET DES GRÂCES

SOUS-DIRECTION DE LA JUSTICE PÉNALE SPÉCIALISÉE

Bureau du droit économique, financier et social,
de l'environnement et de la santé publique

Paris, le 18 octobre 2018

Le directeur des affaires criminelles et des grâces

à

POUR ATTRIBUTION

Mesdames et Messieurs les procureurs généraux près les cours d'appel
Monsieur le procureur de la République près le tribunal supérieur d'appel
Mesdames et Messieurs les procureurs de la République
près les tribunaux de grande instance
Madame la procureure de la République financier
près le tribunal de grande instance de Paris

POUR INFORMATION

Mesdames et Messieurs les premiers présidents des cours d'appel
Monsieur le président du tribunal supérieur d'appel
Mesdames et Messieurs les présidents des tribunaux de grande instance
Monsieur le membre national d'Eurojust pour la France

OBJET: Dépêche relative au recensement des procédures d'escroqueries aux faux investissements dans les cryptoactifs

ANNEXE : Tableau de recensement

N/REF: 2018/F/0090/FC1

DACG

13, place Vendôme
75042 Paris Cedex 01
Téléphone : 01 44 77 60 60

L'attention de la direction des affaires criminelles et des grâces a été appelée sur l'émergence d'une nouvelle forme d'escroqueries : les escroqueries aux faux investissements financiers dans les cryptoactifs.

Les cryptoactifs[1], dont le plus connu est le *bitcoin* créé en 2009, sont des biens numériques immatériels utilisant la cryptographie pour valider des transactions sans la médiation d'un tiers de confiance, tel une banque.

A l'image du phénomène observé à la suite de l'ouverture aux particuliers du « FOREX[2] » ou encore lors du développement de l'offre en ligne d'investissement dans les diamants, le bitcoin et les autres cryptoactifs sont devenus le support d'escroqueries aux faux investissements.

En effet, au-delà des infractions propres au fonctionnement de la technologie associée, relevant de la cybercriminalité et pouvant revêtir notamment les qualifications « d'introduction dans un système de traitement automatisé de données » ou de « modification d'un système automatisé de traitement de données », la nouveauté et la complexité du fonctionnement des cryptoactifs, ainsi que la médiatisation de leurs cours volatiles et parfois exorbitants[3], en font un produit de choix pour démarcher puis escroquer des particuliers souhaitant réaliser des investissements financiers.

Ces escroqueries relèvent d'un mode opératoire classique, par la création de sites internet fallacieux[4] ou un démarchage direct par lesquels des particuliers sont incités à investir dans un cryptoactif, contre la promesse d'un fort rendement financier. Les sommes obtenues, qui ne sont pas investies dans des cryptoactifs, sont ensuite transférées vers des comptes bancaires étrangers. Les gains financiers pour les victimes sont nuls ou seulement temporaires pour les inciter à verser des sommes plus importantes dans le cadre d'un schéma dit de « pyramide de Ponzi ».

Selon l'office central de répression de la grande délinquance financière (OCRGDF) ce phénomène a débuté en France en octobre 2017. En presque un an le préjudice global connu s'élèvait à plus de 25 millions d'euros, représentant plusieurs centaines de plaintes enregistrées.

De nature à concerner de multiples victimes sur l'ensemble du territoire national et à nécessiter des investigations complexes, ces plaintes, lorsqu'elles présentent des éléments de recoupement pertinents (site internet, société, circuit de blanchiment, démarcheurs communs) pourraient utilement faire l'objet de regroupements dans l'intérêt d'une bonne administration de la justice.

Dans cette perspective, je vous saurais gré de bien vouloir recenser les procédures en cours dans vos ressorts et susceptibles de se rattacher aux infractions et modes opératoires évoqués,

---

[1] La notion de cryptoactifs ou crypto-actifs, recouvre celle, impropre, de « cryptomonnaies » ainsi que leurs dérivés financiers. Elle est inclue dans la notion utilisée par le code monétaire et financier à l'article L561-2 et définie comme *« tout instrument contenant sous forme numérique des unités de valeur non monétaire pouvant être conservées ou être transférées dans le but d'acquérir un bien ou un service, mais ne représentant pas de créance sur l'émetteur ».*

[2] *« Foreign Exchange market »,* voir la dépêche *« relative au recensement des procédures relatives aux escroqueries au « FOREX » » n°*2017/F/0310/FC1 ; 2016/F/1017/FC1 ; 2016/F/0735/FC1

[3] Au 13 août 2018, le prix unitaire du bitcoin s'élevait à 6 369,72 dollars, il a pu atteindre près de 20 000 dollars en décembre 2017.

[4] L'AMF a publié une liste noire des sites concernés et identifiés : https://www.amf-france.org/Epargne-Info-Service/Proteger-son-epargne/Listes-noires#title_paragraph_4

en relevant le numéro de parquet, la nature de la procédure (enquête préliminaire ou information judiciaire), le service saisi, les infractions visées, ainsi que le nom des principaux mis en cause. Un tableau de recensement est joint à la présente dépêche afin de faciliter votre retour.

****

Je vous prie de bien vouloir transmettre ces éléments au bureau du droit économique, financier et social, de l'environnement et de la santé publique, à l'adresse suivante *liste.information.dacg-BEFISP@justice.gouv.fr* **avant le 16 novembre 2018**

Je vous saurais gré de m'informer, sous le timbre du bureau du droit économique, financier et social, de l'environnement et de la santé publique, de toute difficulté rencontrée lors de l'exécution de la présente dépêche.

Par avance merci !

Rémy HEITZ,

Le directeur des affaires criminelles et des grâces

ANNEXE N°10

http://www2.assemblee-nationale.fr/questions/detail/15/QE/22103

ASSEMBLÉE NATIONALE

15ème legislature

Question N° : 22103	De **M. Daniel Fasquelle** (Les Républicains - Pas-de-Calais)	**Question écrite**

Ministère interrogé > Numérique	**Ministère attributaire** > Justice

Rubrique >numérique	**Tête d'analyse** >Dispositifs d'enregistrement électroniques pa	**Analyse** > Dispositifs d'enregistrement électroniques partagés.

Question publiée au JO le : **30/07/2019**
Réponse publiée au JO le : **10/12/2019** page : **10774**
Date de changement d'attribution : **03/09/2019**

Texte de la question

M. Daniel Fasquelle attire l'attention de M. le secrétaire d'État auprès du ministre de l'économie et des finances et du ministre de l'action et des comptes publics, chargé du numérique, sur les dispositifs d'enregistrement électroniques partagés (DEEP). Conformément à ses déclarations, le Gouvernement envisage de poursuivre une régulation intelligente des « DEEP » communément appelés *blockchain*. Alors que des efforts en ce sens ont été remarqués avec le vote définitif des articles 26 et 26 bis B de la loi PACTE le 11 avril 2019, qui définissent et encadrent les offres publiques de jetons *via* la technologie *blockchain*, force est de constater que ce texte laisse subsister certaines zones d'ombre. Le mécanisme des *blockchains* permet de sécuriser des transactions *via* une authentification des échanges par les autres opérateurs du marché selon une méthode de consensus algorithmique. Cette technologie investit tous les secteurs professionnels (finance, santé, assurance, énergie, logistique) et ne connaît aucune frontière. La technologie *blockchain* est scientifiquement attestée et réputée inviolable. Beaucoup d'États étrangers ont déjà encadré cette pratique en reconnaissant sa valeur légale. De son côté, la France reste en retrait. En effet, ce mécanisme n'est toujours pas reconnu comme preuve en cas de conflit devant les tribunaux. Il devient urgent de prendre toute la mesure de la révolution technologique *blockchain*. La *blockchain* peut devenir un instrument de sécurité juridique des transactions et des échanges si le Gouvernement reconnaît sa valeur légale de preuve. Il souhaite savoir comment le ministère de l'économie et des finances entend encadrer juridiquement la *blockchain*, lui donner une définition et une force probante légale.

Texte de la réponse

La blockchain ou chaîne de blocs, technologie de création et de gestion de bases de données sécurisées, décentralisées et réputées infalsifiables, est l'une des déclinaisons des dispositifs d'enregistrement électroniques partagés. Elle combine trois technologies relativement anciennes à l'échelle d'Internet : la cryptologie, les bases de données et le pair-à-pair (peer-to-peer). Son utilisation suscite depuis quelques années un intérêt croissant et de nombreux acteurs privés comme publics expérimentent cette technologie pour apprécier ses apports notamment en matière de création d'actifs, de certification, d'horodatage et de création de contrats à exécution automatique (smart contracts). Il convient de rappeler que la France a eu un rôle relativement précurseur dans l'intégration de cette technologie à son système juridique. En effet, l'ordonnance du 28 avril 2016 n° 2016-520 relative aux bons de caisse dispose, dans son article 2, la possibilité d'inscrire l'émission et la cession de minibons dans un dispositif d'enregistrement électronique partagé permettant l'authentification de ces opérations. Or, en 2016, peu d'Etats

avaient inscrits dans leur ordonnancement juridique cette technologie. Depuis lors, la France a chaque année enrichi le corpus de ses textes juridiques prenant spécifiquement en considération les technologies de type blockchain : l'ordonnance n° 2017-1674 du 8 décembre 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers, le décret n° 2018-1226 du 24 décembre 2018 relatif à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers et pour l'émission et la cession de minibons et la loi n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises dite loi PACTE. En matière probatoire, si aucun texte juridique ne mentionne spécifiquement la blockchain, il n'en résulte pour autant aucun vide juridique. En effet, le code civil pose le principe de la liberté de la preuve des faits juridiques (article 1358) et des actes sous signatures privées, dont le montant est inférieur à 1 500 euros (article 1359). En outre, si un écrit est nécessaire pour les contrats dont l'enjeu est supérieur à ce montant, le code civil pose un principe de non-discrimination de l'écrit électronique par rapport à un écrit sur support papier (article 1366), dès lors que peut être identifiée la personne dont cet écrit émane et que celui-ci est établi et conservé dans des conditions de nature à en garantir l'intégrité. La preuve des obligations est également libre entre commerçants en application de l'article L. 110-3 du code de commerce. Par conséquent, les preuves issues des chaînes de blocs peuvent aujourd'hui être légalement produites en justice. Il appartient au juge d'évaluer leur valeur probante, sans que celui-ci ne puisse les écarter au seul motif qu'elles existent sous forme numérique. Dans les cas où une preuve par écrit est imposée, la technologie blockchain peut répondre à certaines des exigences réglementaires posées en la matière. Le règlement européen n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, dit règlement eIDAS, impose, pour bénéficier d'une présomption de fiabilité en matière de signature et d'horodatage, qu'il soit fait usage d'un tiers de confiance, ce que cette technologie ne prévoit pas. Pour autant, cela ne signifie pas que les signatures électroniques et autres inscriptions utilisées dans les chaînes de blocs – qui peuvent recouvrir des réalités techniques et obéir à des règles de gouvernance très variées selon le type de chaînes en cause – sont dépourvues de valeur probante mais seulement qu'elles ne bénéficient pas de cette présomption. Leur valeur probante sera appréciée par le juge conformément au droit commun de la preuve. Notre droit permettant d'appréhender de manière satisfaisante les questions probatoires soulevées par les chaînes de blocs, il ne nous paraît donc ni nécessaire, ni opportun de créer un cadre légal spécifique. Par ailleurs, la fiabilité des blockchains est dépendante de l'absence de faille dans le code informatique (plusieurs cas de détournements de crypto-monnaies ont déjà été observés) et de l'évolution des connaissances en matière de cryptographie. Au surplus, rien ne permet de s'assurer de la véracité d'un élément inséré dans une blockchain : seule la date de l'insertion et l'identité du document produit par rapport à la trace conservée dans la blockchain sont garanties par ce procédé. Enfin, elle ne peut être assimilée à un acte authentique, en ce que l'officier ministériel participe à l'élaboration de l'acte authentique, garantissant dans une certaine mesure sa validité, son absence de contrariété à l'ordre public ainsi qu'aux droits des tiers, ce qui n'est absolument pas assuré par les blockchains.

ANNEXE N°11

Dennemeyer
The IP Group

Hangzhou Internet Court
Province of Zhejiang
People's Republic of China

Judgment

In the matter:

Plaintiff 1: Hangzhou Huatai Yimei Culture Media Co., Ltd.

./.

Defendant 1: Shenzhen Daotong Technology Development Co., Ltd.

Case No.: 055078 (2018) Zhe 0192 No. 81

June 27, 2018

This court concludes that the disputes in this case include: I. Is Huatai Yimei Company qualified as a plaintiff; II. Did Daotong Company infringe the right to dissemination over an information network; III. If the infringement is confirmed, are the damages claimed by Huatai Yimei Company in a reasonable amount.

I. Is Huatai Yimei Company qualified as a plaintiff

With regard to the Dispute No. 1, this court concludes that the article at issue includes interview, description, summary and review of social phenomena, and the included photos reflect selections and arrangements made by the author in perspective, composition and light, all of which are unique, comply with the provisions on work requirements by China's Copyright Law, and belong to literature and photography protected by the Copyright Law. This court does not support the allegation made by Daotong Company in the answer that the work at issue is a report of current events. Both the texts and photos at issue were published on the City Express. The two reporters under whose names the work was published both stated that the City Express owns the copyright of the work. The labor contract presented by the City Express and the statement by the authors can form a complete chain of evidence to show that the City Express owns the copyright of the work. This court does not support the allegation made by Daotong Company in the answer that the City Express does not own the copyright of the work at issue. The City Express granted an exclusive right to Huatai Yimei Company to execute the right to dissemination over an information network of the work at issue, and specifically stated that Huatai Yimei Company may file actions on its own behalf against alleged infringing actions. Therefore, Huatai Yimei Company is qualified as an entity to file this action.

II. Did Daotong Company infringe the right to dissemination over an information network

Huatai Yimei Company obtained evidence, through a third-party evidence preservation platform, Baoquan.com, with regard to the infringing webpages of Daotong Company, and proved the integrity of the electronic data and that the electronic data were not tampered with by storing the electronic data in blockchain. To determine whether the infringing action did take place, therefore, it is necessary to determine whether Huatai Yimei Company's approaches of securing evidence and storing evidence comply with electronic data-related provisions and determine how strong the evidence is. Referring to Article 8 of the Electronic Signature Law of the People's Republic of China, the following factors should be considered when examining the authenticity of digital messages as evidence: (1) reliability of methods for generating, storing or transmitting digital messages; (2) reliability of methods for maintaining the content integrity; (3) reliability of methods for identifying a sender; and (4) provisions on other relevant factors. As a result, this court will determine as follows the efficacy of the electronic evidence at issue from three aspects: examination of qualifications of the evidence preservation platform, examination of credibility of technical means for obtaining evidence on the infringing webpages, and examination of integrity of blockchain electronic evidence preservation.

(1) Regarding the examination of qualifications of the evidence preservation platform

According to investigations, the shareholder of Huatai Yimei Company is Zhejiang Huamei Holding Co., Ltd. Numchain [editor's note: the owner of the platform Baoquan.com]

has the following natural person shareholders: Yuan Wen, Hang Gao, Qiaofeng Li, and Chunquan Lu, and the following enterprise shareholders: Anji Numchain Investment Management Partnership, Hangzhou Numchain Investment Management Partnership, Xinyu Youchuang Investment Management Center, and Hangzhou Shuimu Zehua Venture Capital Partnership. The shareholders and business scope of Numchain are relatively independent of Huatai Yimei Company and the City Express, so Numchain is neutral and has passed the integrity identification and inspection by the National Quality Supervision and Testing Center of Cyber and Information Security Products. Baoquan.com operated by Numchain possesses the qualifications as a third-party electronic evidence preservation platform.

(2) Regarding the examination of credibility of technical means for obtaining evidence on the infringing webpages

Turn on a command window on a computer, type in a command, "ping www.baoquan.com," and the returned IP is 112.74.234.54. According to investigations, the physical location of the IP is the Aliyun BGP Data Center. Therefore, it can be seen that Baoquan.com is deployed inside Aliyun. As a general cloud platform, Aliyun can ensure that servers are not infected or invaded by viruses or Trojans in normal situations; moreover, Baoquan.com has obtained a certificate of the Website Security Class I Certification and record evidence of Information System Security Class Protection III awarded by the Third Research Institute and the National Quality Supervision and Testing Center of Cyber and Information Security Products of the Ministry of Public Security. Therefore, it should be determined that this website has a secure environment for storing electronic data, unless proved wrong by evidence to the contrary. Upon receiving an infringing webpage URL, the Baoquan.com server would automatically request a target address under the Internet environment, and the target address automatically returns a state code and webpage information to confirm a valid accessible address of the requested URL, thereby ensuring that the capture of the infringing link is performed in the Internet environment.

Baoquan.com captures images from a target webpage by automatically invoking Puppeteer, an open source program of Google, and at the same time, acquires the source code of the target webpage by invoking curl. According to investigations, Puppeteer is a Node library formally produced by Google that controls headless Chrome through the DevTools protocol, which can collect data by using API provided thereby as a crawler to access webpages. The Curl command acquires information like webpage content and version by simulating an HTTP request through a file transfer tool working in the command line according to the URL rule. This evidence securing system is equally open to all people, and anyone can use the system. Moreover, the operation process thereof is automatically completed by a machine according to a program preset by the evidence obtaining system. The likelihood that relevant links are tampered with by humans throughout the evidence obtaining and evidence securing process is relatively low. Therefore, the source of the electronic data has relatively high credibility; meanwhile, Chain Forensic Science identified and confirmed the technicality of using the Puppeteer and Curl programs for webpage screenshots and source code retrieval in Baoquan.com. In the absence of evidence to the contrary, therefore, this court confirms that the approach by Baoquan.com to parse a domain name for a target webpage to generate and store digital messages by using public open source capture programs from Google is reliable. In this case, the webpage screenshots captured through Puppeteer show that the alleged infringing article published by the "First Female Fashion Network" in 2017 is substantially consistent with the article at issue. The source code address of the target webpage acquired through Curl is "www.ladyfirst.com"

[editor's note: "www.ladyfirst.com.cn"]. According to investigations, the name of the website "www.ladyfirst.com" [editor's note: "www.ladyfirst.com.cn"] is "First Female Fashion Network" and the entity on record is Daotong Company.

(3) Regarding the examination of integrity of blockchain electronic evidence preservation

Baoquan.com packaged and compressed the webpage screenshots, source code and access information, calculated the SHA256 value and then uploaded the same to the FACTOM blockchain and the Bitcoin blockchain to ensure that the electronic data is not changed. To examine the reliability of this approach to maintain content integrity, it is necessary to first analyze and judge the blockchain technology.

As a decentralized database, blockchain is a string of data blocks generated by using a cryptography method in an associated manner. Each data block contains information of an online transaction for verifying the validity (authenticity) of the information and generating the next block. Specifically, a blockchain network is a network formed by using servers of a plurality of institutions or companies as nodes. A node on the network will package data generated within a time period to form a first block, and then synchronize the block to the entire blockchain network. Other nodes on the network verify the received block and, when the verification passes, add the block to a local server. Subsequently, a node would package newly generated data and information of existing blocks on the local server together to form a second block. After other nodes receive the block and the verification of the block passes, the second block is added to a local server. The first block and the second block are associated. Subsequent data inside the network are all packaged into blocks in the same manner as described above, and the blocks are connected end to end to form a chain. The chain is a blockchain. If data in a block needs to be changed, the content of all blocks after the block needs to be changed, and data backup by all the institutions and companies on the blockchain network needs to be changed as well. Therefore, the feature of a blockchain is that it is difficult to be tampered with or deleted. When it is confirmed that the electronic data at issue has been saved to a blockchain, the approach to maintain content integrity is reliable. In this case, to confirm that the electronic data has indeed been uploaded to the blockchain, this court performed examination in two aspects: whether the electronic data has truly been uploaded and whether the uploaded electronic data is the electronic data at issue.

1. Examination of whether the electronic data has truly been uploaded

To determine whether the electronic data at issue has truly been uploaded, a search can be conducted in the FACTOM blockchain according to the transaction hash value provided by Huatai Yimei Company to check the hash content and generation time of the transaction. According to the block height submitted by Huatai Yimei Company, it can be found through query that the hash content of the transaction has been stored into the block height, and the time of uploading the content can also be found. Moreover, the uploading time is reasonable relative to the time displayed in the invocation log of using Puppeteer and Curl to automatically acquire webpage screenshots and source code, and the block height generation time is consistent with the time logic between the invocation log generation time and the FACTOM rules.

The transaction hash value of the Bitcoin blockchain is anchored according to the block height, and it is found through query in the Bitcoin blockchain that the content contained in the block node is consistent with the hash value of the content stored in FACTOM. Therefore, this court confirms that Baoquan.com has uploaded the electronic data to the FACTOM blockchain and the Bitcoin blockchain.

2. Examination of whether the uploaded electronic data is the electronic data at issue

The hash value is calculated for the file that packages and compresses the webpage screenshots, source code and invocation information downloaded in Baoquan.com. According to the comparison, the value is consistent with the hash value of the electronic data for blockchain preservation as submitted by Huatai Yimei Company. Therefore, it can be confirmed that the electronic data at issue has been uploaded to the FACTOM blockchain and the Bitcoin blockchain, and that the integrity of the electronic data at issue has been preserved with no change since the upload to the blockchains.

In summary, this court concludes that electronic data saved and secured using technical means like blockchain should be analyzed and determined case by case with an attitude of being open and neutral. The technologies like blockchain should not be dismissed or the standard of determination thereof should not be raised because they are novel and complex technical means at present, nor should the standard of determination thereof be lowered because it is difficult to tamper with or delete the technology. The effectiveness of evidence thereof should be determined, in a comprehensive manner, according to relevant legal provisions on electronic data, wherein the emphasis should be on examination of the source of electronic data and content integrity thereof, security of the technical means, reliability of the methods, legitimacy of formation, and degree of association with other evidence for mutual corroboration, thereby determining the effectiveness of evidence. In this case, Numchain is a civil entity independent of the parties, and Baoquan.com operated thereby is a third-party evidence preservation platform that complies with legal provisions. Baoquan.com uses open source programs from Google that have relatively high credibility to secure electronic data, such as the infringing work, and the webpage screenshots, source code information, and invocation log formed by the technical means through capturing the target webpages can corroborate with each other, and can clearly reflect the source of the data and the generation and transfer routes. It should be determined that the electronic data generated in such a manner is reliable. Meanwhile, Baoquan.com uses the blockchain technology that satisfies relevant standards to preserve and secure the above electronic data, which ensures the integrity of the electronic data. Therefore, the above electronic data can be used as a basis for determination of infringement in this case. Namely, this court finds that the work at issue is published on the “First Female Fashion Network” operated by Daotong Company.

It is stipulated in Article 10, Paragraph (12) of the Copyright Law of the People's Republic of China that “the right to dissemination over an information network is a right to provide works to the public in a wired or wireless manner, such that the public can obtain the works at a time and location selected by each individual thereof;” (1) in the case of duplicating, issuing, performing, showing, broadcasting, compiling, and disseminating, without consent of a copyright owner, the owner’s work via an information network, unless otherwise stipulated by this law…” As a statutory copyright, the right to dissemination over an information network is a propriety right of an owner and is an absolute right in nature. If

any action of dissemination over an information network subject to the control of the propriety right is carried out without consent of the right owner and in the absence of statutory or stipulated exception, such an action constitutes infringement. The establishment of the infringing action is not dependent on factors such as a fault made by an actor or profits obtained by an actor. In this case, it has been proved that Daotong Company provides the work at issue on a website operated thereby to the public, and online users can acquire the work by means of downloading, browsing, and like via an information network at a time and location selected by each individual thereof. The action of Daotong Company is a dissemination of the work at issue over an information network.

Daotong Company alleged that its action of dissemination of the work at issue over an information network is of a nature for public welfare and belongs to reasonable uses. However, its action does not comply with any one of reasonable uses prescribed in Article 22 of the Copyright Law or meet the requirements for reasonable use prescribed in Article 21 of the Rules for Implementation of the Copyright Law. Therefore, this court rejects this allegation in the answer by Daotong Company.

III. Are the damages claimed by Huatai Yimei Company in a reasonable amount

It is stipulated in Article 48 of the Copyright Law of the People's Republic of China that “a party that has conducted any of the following infringing actions shall be liable for civil liabilities such as stopping the infringement, effect elimination, apologies, and damages…: (1) in the case of duplicating, issuing, performing, showing, broadcasting, compiling, and disseminating, without consent of a copyright owner, the owner’s work via an information network, unless otherwise stipulated by this law…”. In this case, Daotong Company shall be liable for stopping the infringement, deleting the alleged infringing article, and damages for the infringing actions that have taken place. Daotong Company alleged that it had deleted the article at issue, and Huatai Yimei Company withdrew this claim in the case hearing process, which is approved by the court and will not be further judged.

With regard to the amount of damages, Huatai Yimei Company does not present any evidence to prove losses suffered thereby as a result of the infringement or profits obtained by Daotong Company as a result of the infringement, and requests that statutory damages be applied and the amount be determined by this court appropriately by comprehensively considering relevant factors, such as market influence and reputation of the text work and photo work at issue, degree of the infringement by Daotong Company, and the like. Meanwhile, this court has noticed the following facts: 1. The text work at issue has a word count of about 3010 words and took up 1 page of the City Express when published; 2. One of the photos at issue is a guide sign, which did not require a professional photographer to shoot; 3. The alleged infringing article uses the article at issue in its entirety; 4. The text work at issue contains a lot of conversations with interviewees; 5. The source of the work was indicated clearly by Daotong Company when forwarding the work; 6. Daotong Company was established on June 5, 2013 with a registered capital in the amount of 500,000 Yuan; 7. Huatai Yimei Company obtained and verified the evidence for this case and retained attorneys for the litigation with the attorneys’ fees agreed at 2500 Yuan.

In summary, pursuant to Article 10, Article 11, Article 48, and Article 49 of the Copyright Law of the People's Republic of China, Article 8 of the Electronic Signature Law of the People's Republic of China, Article 64 of the Civil Procedure Law of the People's Republic of China, and Article 108 of the Interpretation of the Supreme People's Court of Several Issues concerning the Application of the Civil Procedure Law of the People's Republic of China, the following judgment is made:

I. The defendant Shenzhen Daotong Technology Development Co., Ltd. shall compensate the plaintiff Hangzhou Huatai Yimei Culture Media Co., Ltd. for economic losses (including reasonable expenses for stopping infringement) in an amount of 4000 Yuan within 10 days after the effective date of this judgment;

II. Other claims by the plaintiff Hangzhou Huatai Yimei Culture Media Co., Ltd. are dismissed.

If the payment obligation is not fulfilled within the period specified herein, a debt interest shall be paid in a doubled amount for the delayed period pursuant to Article 253 of the Civil Procedure Law of the People's Republic of China.

The defendant Shenzhen Daotong Technology Development Co., Ltd. shall be liable for 18 Yuan of the case processing fee in the amount of 25 Yuan (already reduced by half), while the plaintiff Hangzhou Huatai Yimei Culture Media Co., Ltd. shall be liable for 7 Yuan.

The plaintiff Hangzhou Huatai Yimei Culture Media Co., Ltd. shall file an application for refund with this court within 15 days after the effective date of the judgment; the defendant Shenzhen Daotong Technology Development Co., Ltd. shall pay this court the litigation fee for which it is liable within 7 days after the effective date of the judgment.

Any party having an objection to the judgment may file an appeal with the Intermediate People's Court of Hangzhou City, Zhejiang Province by submitting the appeal petition to this court within 15 days after the day of service of the judgment and providing copies thereof consistent with the number of opposing parties.

Judge Li Sha

It has been verified that this copy is identical with the original June 27, 2018

ANNEXE N°12

VERMONT **GENERAL ASSEMBLY**

The Vermont Statutes Online

Title 12 : Court Procedure

Chapter 081 : Conduct Of Trial

Subchapter 001 : Generally

(Cite as: 12 V.S.A. § 1913)

§ 1913. Blockchain enabling

(a) As used in this section:

(1) "Blockchain" means a cryptographically secured, chronological, and decentralized consensus ledger or consensus database maintained via Internet, peer-to-peer network, or other interaction.

(2) "Blockchain technology" means computer software or hardware or collections of computer software or hardware, or both, that utilize or enable a blockchain.

(b) Authentication, admissibility, and presumptions.

(1) A digital record electronically registered in a blockchain shall be self-authenticating pursuant to Vermont Rule of Evidence 902, if it is accompanied by a written declaration of a qualified person, made under oath, stating the qualification of the person to make the certification and:

(A) the date and time the record entered the blockchain;

(B) the date and time the record was received from the blockchain;

(C) that the record was maintained in the blockchain as a regular conducted activity; and

(D) that the record was made by the regularly conducted activity as a regular practice.

(2) A digital record electronically registered in a blockchain, if accompanied by a declaration that meets the requirements of subdivision (1) of this subsection, shall be considered a record of regularly conducted business activity pursuant to Vermont Rule of Evidence 803(6) unless the source of information or the method or circumstance of preparation indicate lack of trustworthiness. For purposes of this subdivision (2), a record includes information or data.

(3) The following presumptions apply:

(A) A fact or record verified through a valid application of blockchain technology is authentic.

(B) The date and time of the recordation of the fact or record established through such a blockchain is the date and time that the fact or record was added to the blockchain.

(C) The person established through such a blockchain as the person who made such recordation is the person who made the recordation.

(D) If the parties before a court or other tribunal have agreed to a particular format or means of verification of a blockchain record, a certified presentation of a blockchain record consistent with this section to the court or other tribunal in the particular format or means agreed to by the parties demonstrates the contents of the record.

(4) A presumption does not extend to the truthfulness, validity, or legal status of the contents of the fact or record.

(5) A person against whom the fact operates has the burden of producing evidence sufficient to support a finding that the presumed fact, record, time, or identity is not authentic as set forth on the date added to the blockchain, but the presumption does not shift to a person the burden of persuading the trier of fact that the underlying fact or record is itself accurate in what it purports to represent.

(c) Without limitation, the presumption established in this section shall apply to a fact or record maintained by blockchain technology to determine:

(1) contractual parties, provisions, execution, effective dates, and status;

(2) the ownership, assignment, negotiation, and transfer of money, property, contracts, instruments, and other legal rights and duties;

(3) identity, participation, and status in the formation, management, record keeping, and governance of any person;

(4) identity, participation, and status for interactions in private transactions and with a government or governmental subdivision, agency, or instrumentality;

(5) the authenticity or integrity of a record, whether publicly or privately relevant; and

(6) the authenticity or integrity of records of communication.

(d) The provisions of this section shall not create or negate:

(1) an obligation or duty for any person to adopt or otherwise implement blockchain technology for any purpose authorized in this section; or

(2) the legality or authorization for any particular underlying activity whose practices or data are verified through the application of blockchain technology. (Added 2015, No. 157 (Adj. Sess.), § I.1; amended 2017, No. 205 (Adj. Sess.), § 1.)

BIBLIOGRAPHIQUE

Dictionnaires

Black's Law Dictionnary 1381, 6th ed. 1990

Blay M., Dictionnaire des concepts philosophiques, Larousse, 2013

Cornu G., Vocabulaire juridique, Puf, 2014

Cornu G., Vocabulaire juridique, Puf, 12e éd., 2018

Cornu G. (dir.), Vocabulaire juridique de l'Association Henri Capitant, 8e éd, 2007

Dictionnaire de l'Académie française, t. 1, Firmin Didot, 6e éd. 1835

Rey A., Tomi M., Hordé T., Tanet C., Dictionnaire historique de la langue française, Le Robert, mars 2000 (réimpression)

Roland H., Boyer L., *Adages du droit français*, Litec, 4e éd., 1999

Fascicules / Repertoires

Aubry-Caillaud F., Fasc. 560 : normes techniques et certifications, JCl. Europe Traité, Lexis Nexis, avr. 2018

Blanchet O., Bariani X., Fasc. 10 : huissiers de justice, JCl. Encyclopédie des Huissiers de Justice, Lexis Nexis, avr. 2011 (maj 5 juill. 2019), n°182.

Bonhomme R. (Maj par Bouteille-Brigant M.), Fasc. 90 : transfert de la propriété et des risques, JCl. Contrats – Distribution, Lexis Nexis, mars 2017

Brahic Lambrey C., Fasc. 10 : Vérification d'écriture. Faux et inscription de faux, JCl. Procédures Formulaire, Lexis Nexis, 18 sept. 2015

Dorol S., Fasc. 30 : Constat d'huissier de justice, JCl. encyclopédie des Huissiers de Justice, Lexis Nexis, avr. 2015

Dorol S., Fasc. 20 : Preuve. Modes de preuve, JCl. des Huissiers de Justice > Preuve, Lexis Nexis, févr. 2015

Ferrand F., Preuve, répertoire de procédure civile, Dalloz, dec. 2013

Grynbaum L., Fasc. 10 : La preuve littérale, JCl. Civil Code – Art. 1316 à 1316-4, Lexis Nexis, 19 dec. 2011

Guével D., Fasc. 40 : Contrats et obligations. Preuve testimoniale. Liberté des preuves en matière commerciale, JCl Civil Code, Lexis Nexis, 7 sept. 2010

Guével D., Fasc. 50 : contrats et obligations, Preuve testimoniale, Commencement de preuve par écrit, JCl. Civil Code, art. 1341 à 1348, Lexis Nexis, juin 2013

Guével D., Fasc. unique : Contrats et obligations – Actes sous seing(s) privé(s) – Règles générales, JCl. Civil Code, art. 1322 à 1324, Lexis Nexis, mars 2012

Guével D., Fasc. unique : Contrats et obligations – Preuve. Charges de la preuve et règles générales, JCl. Civ., Lexis Nexis, 25 juill. 2014

Guével D., Fasc. unique : Contrats et obligations – Preuve par serment, JCl. Civil Code > Art. 1384 à 1386-1, Lexis Nexis, juin 2016

Hovasse H., Le Normand-Caillère S., Fasc. 1950 : Bons de caisse, JCl. Banque, crédit, bourse, Lexis Nexis, sept. 2017

Jarrosson C. et Le Bars B., Fasc. 10 : Arbitrage - Arbitrage commercial - Droit interne, JCl. Notarial Formulaire, Lexis Nexis, oct. 2013

Legeais D., Fasc. 534 : Blockchain, JCl. Commercial, Lexis Nexis, 7 mars 2017

Legeais D., Fasc. 535 : Actifs numériques et prestataires sur actifs numériques, JCl. Commercial, Lexis Nexis, oct. 2019

Legeais D., Fasc. 2160 : Blockchain, JCl. Sociétés, Lexis Nexis, 29 mai 2018 (maj 29 Janv. 2019)

Loquin E., Fasc. 1024 : Arbitrage - Conventions d'arbitrage - Conditions de fond. Litige arbitrable, JCl. Procédure civile, Lexis Nexis mai 2016

Penneau A., Voinot D., fasc. 970, Normalisation, JCl. Concurrence - Consommation, Lexis Nexis, oct. 2010

Pétel-Teyssié I., Dauxerre L., Fasc. unique : preuve des obligations, Modes de preuve, Actes sous seing privé unilatéraux, Mention de la somme ou de la quantité, JCl. Civil Code, art. 1376, Lexis Nexis, juill. 2017

Pétel-Teyssié I., Fasc. unique : preuve des obligations, Modes de preuve, Actes sous seing privé synallagmatiques, formalité du double original, JCl. Civil Code art. 1375, Lexis Nexis, juill. 2017

Quémener M., Fasc. 35 : la preuve numérique dans le cadre pénal, JCl. Communication, Lexis Nexis, 18 avr. 2019

Racine J.-B., Fasc. 191 : Convention d'arbitrage - Formation, JCl. Contrats Distribution, Lexis Nexis, janv. 2012

Ouvrages spéciaux

Alizart M., *Cryptocommunisme*, perspectives critiques, Puf, fevr. 2019

Antonopoulos A. M., *Mastering Bitcoin : Unlocking Digital Cryptocurrencies*, O'Reilly Media, Inc., 3 dec. 2014

Arrows K., *The limits of organizations*, harvard university press, 1974

Bertrand C. (dir.), Brett R., Pulliero F., Wagener N., « Droit et anarchie », Éditions L'Harmattan, coll. « Presses universitaires de Sceaux », 2013

Brunton F., Nissenbaum H., Obfuscation, A User's Guide for Privacy and Protest, MIT Press, sept. 2015

Caré S., *Les libertariens aux États Unis : sociologie d'un mouvement asocial*, Pur, coll. Res publica, 2010

De Filippi P., Wright A., *Blockchain and the Law*, Harvard University Press, 2018

Hayek F., *Droit, législation et liberté*, Puf, Trad. française, 1979

Huguet B., Favier J., Takkal A., *Bitcoin - Métamorphoses - De l'or des fous à l'or numérique ?, Dunod*, oct. 2018

Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S., *Bitcoin and Cryptocurrency Technologies*, Princeton University Press, 2016

Nozick R., *Anarchie, État et Utopie*, Puf, trad. française E. d'Auzac de Lamartine et P.-E. Dauzat (1e éd. 1974), 2016

Parance B., de Saint Victor J. (dir.), *Repenser les biens communs*, CNRS Editions, 2014

Peugeot V., *Les communs. Une brèche politique à l'heure du numérique*, Presses des Mines, 2013

Proudhon P.-J., *Manifeste électoral du peuple*, in œuvres complètes de P.-J Proudhon, Tome XVII, Mélanges, Articles de journaux 1849-1852, Premier volume, Librairie internationale, 1848

Proudhon P.-J., *Qu'est-ce que la propriété ? ou recherche sur le principe du droit et du gouvernement*, Garnier Frères Libraires, 1849

Rifkin J., *La troisième révolution industrielle – Comment le pouvoir latéral va transformer l'énergie, l'économie et le monde*, Les liens qui libèrent, 2011

Schrepel T., Anarchy, State, and *Blockchain* Utopia: Rule of Law Versus Lex Cryptographia (chapitre 15), *in* General Principles and Digitalisation, Libraire SSRN, 12 nov. 2019, p.353.

Stirner M., *L'Unique et sa propriété*, coll. Etudes, 2013

Takkal Bataille A., Favier J., Bitcoin. *La monnaie acéphale*, CNRS Editions, 2017

Werbach K., T*he blockchain and the new architecture of trust*, MIT Press, Information Policy, nov. 2018

Ouvrages généraux

Altan H., *A tort et à raison. Intercritique de la science et du mythe*, Points, Seuil, 1986

Aubert J.-L., *Introduction au droit et thèmes fondamentaux du droit civil*, Coll. U, Armand Colin, 10e éd. Paris 2004

Aubry C., Rau C., *Cours de droit civil français*, t. 12, par P. Esmein, 6e ed., 1958

Audit B., d'Auvout L., *Droit international privé*, coll. Traités, LGDJ, sept. 2018

Audic O., *Les fonctions du document en droit privé*, bibliothèque de l'Institut André Tunc, t. 3, LGDJ, 2004

Aynès A., Vuitton X., *Droit de la preuve. Principes et mise en œuvre processuelles*, Droit & Professionnels, Lexis Nexis, 2018

Bachelard G., *Le nouvel esprit scientifique*, PUF, 1971

Benabent A., *Droit des obligations*, Lextenso, sept. 2018

Bentham J., *Traité des preuves judiciaires*, t. I, Bossange Frères, Paris 1823

Bergson E., *Essai sur les données immédiates de la conscience*, thèse, Félix Alcan, coll. Bibliothèque de philosophie contemporaine, 1889.

Beudant R., Lerebourg Pigeonnière P., *Cours de droit civil français : Les Contrats et les obligations*, t. 9, 2e ed., 1953

Bitan H., *Droit et expertise du numérique*, Wolters Kluwer, coll. Lamy Axe Droit, 2015

Bollard G., *Droit et pratique de la procédure civile*, Dalloz Action, 2012-2013

Boneh D., Shoup V., *A Graduate Course in Applied Cryptography*, Université de Stanford, sept. 2017

Bonnier E., *Traité pratique du droit des preuves en droit civil et en droit criminel*, t. 1, 3e éd., 1862

Bonnier E., *Traité théorique et pratique des preuves en droit civil et en droit criminel*, Joubert, Librairie de la cour de cassation, 1843

Bonneau T., Rouaud A.-C., Pailler P., Vabres R., Tehrani A., *Droit financier*, Précis Domat coll. droit privé, LGDJ, 2e ed., oct. 2019

Boulez J., *Expertises judiciaires*, Encyclopédie Delmas, 17e ed., 2016

Bugnet M., tome 2, Cosse et Marchal, 2e éd., 1861

Bureau D., Muir Watt H., *Droit international privé*, t. I, Partie générale, 4e ed., Puf, Thémos Droit, 2017

Bredin J.-D., *Le doute et l'intime conviction*, Droits, 1996

Cabrillac R., *Droit des obligations*, 6e éd, Cours, Dalloz, 2004

Cadiet L., Jeuland E., *Droit judiciaire privé*, 5e éd., Litec, 2006

Cadiet L., Normand J. et Amrani- Mekki S., *Théorie générale du procès*, 2e éd., Puf, coll. Thémis, 2013

Camus A., *Discours de Suède*, coll. Folio, Gallimard, 1997

Carbonnier J., *Droit civil, Introduction*, Puf, 27ème éd., 2002

Carbonnier J., *Sociologie juridique*, PUF, coll. Thémis, 1978

Césaro J.-F., *Le doute en droit privé*, préf. B. Teyssié, Éd. Panthéon-Assas, LGDJ, 2003

Chagnollaud de Sabouret D., *La constitution de la Ve république. Droit constitutionnel contemporain*, t.2, Cours Dalloz, 8e éd., sept. 2017

Chevalier J., *La charge de la preuve. Cours de droit civil approfondi*, Les Cours de droit, 1958-1959

Coipel-Cordonnier N., *Les conventions d'arbitrage et d'élection de for en droit international privé*, LGDJ, 1999

Colin A. , Capitant H. , *Cours élémentaire de droit civil français*, t. 1, Dalloz, Paris 1914

Coppens P., *Normes et fonction de juger*, Bruylant, LGDJ, coll. La pensée juridique, 1998

Cornu G., La vérité et le droit, *in* L'art du droit en quête de sagesse, Puf, coll. Doctrine juridique, 1998

Cornu G., Rapport de synthèse, *in* La vérité et le droit, Actes des conférences Journées canadiennes à Montréal, 1987, éditions Association Henri Capitant, Economica, 1989

Couret A., Le Nabasque H., *Droit financier*, Dalloz, 1ère éd., 2008

Croze H., *Le procès civil*, 2e ed., Dalloz, 2004

Dabin J., *La technique de l'élaboration du droit positif spécialement en droit privé*, Bruxelles, Bruylant, 1935

Demolombe C. , *Traité des contrats ou des obligations conventionnelles*, t. 6, Paris, 1876

Deumier P., *Introduction générale au droit*, 2e éd., LGDJ, 2013

Diderot D., *Lettre à Sophie Volland*, 26 sept. 1762

Dissaux N., Jamin C., *Réforme du droit des contrats, du régime général et de la preuve des obligations. Commentaire des articles 1100 à 1386-1 du Code civil*, Supplément au Code civil Dalloz 2017, août 2016

Domat J., *Les loix civiles dans leur ordre naturel*, Première partie, L.III, Titre VI, 1689

Domat J., *Lois civiles*, 1ère partie, Livre III, Tome 6, édition Rémy, II, 1828

Dumoulin L., *L'expert dans la justice. De la genèse d'une figure à ses usages*, Economica, 2007

Dupeyroux H., *Les grands problèmes du Droit*, APD, 1938

Estaunie E., *L'empreinte*, 1896

Fabre-Magnant M., *Introduction au droit*, 2016

Favro K., Lobé Lobas M., Markus J.- P. (ss. dir.), *L'expert dans tous ses états. À la recherche d'une déontologie de l'expert*, coll. Thèmes et commentaires, Dalloz, nov. 2016

Feuer G., Cassan H., *Droit international du développement*, Precis Dalloz, 1985

Flour J., Aubert J.-L., Flour Y., Savaux E., *Le rapport d'obligation*, Sirey, 4e éd., 2005

Foucault M., Dits et écrits, 1954-1988, t.3, Gallimard, coll. Bibliothèque des sciences humaines, 1994

Ghestin J. et Goubeaux G., Traité de droit civil. Introduction générale, avec le concours de Fabre-Magnan M., LGDJ, 4e éd., 1994

Girard F., *Essai sur la preuve dans son environnement culturel*, PUAM, 2013

Goblot E., *Traité de logique*, Librairie Armand Colin, 1918

Gómez J., *Codage et cryptographie. Mathématiciens, espions et pirates informatiques*, coll. Le monde est mathématique, RBA, Ed. L'Obs août 2019

Gueraroui R., *L'algorithmique répartie : à la recherche de l'universalité perdue*. *Leçon inaugurale prononcée au Collège de France le jeudi 25 octobre 2018*, OpenEdition Books, 4 dec. 2019

Guinchard S., Chainais C., Ferrand F., *Procédure*, Dalloz, 30e éd., 2010

Guinchard S., *Droit et pratique de la procédure civile. Droit interne et européen*, Dalloz Action, 9e éd., 2017/2018

Guinot T., *L'huissier de justice : normes et valeurs*, EJT, coll. Droit et Procédures, mars 2017

Hélié V. F., *Traité de l'instruction criminelle ou théorie du Code d'instruction criminelle*, Tome IV, 2e éd., Plon, Paris, 1866

Hennette Vauchez S., Encinas de Munagorri R., Leclerc O., Herrera C., Miguel Herrera C, *L'analyse juridique de (x): Le droit parmi les sciences sociales*, Kimé. Kimé, 2016

Héron J., T. Le Bars, *Droit judiciaire Privé*, 3e éd., Montchrestien-Lextenso, Domat, Droit privé, 2006

Jarrosson C., *La notion d'arbitrage*, LGDJ, 1987

Jeuland E., *Droit processuel général*, LGDJ Précis Domat, dec. 2014

Kant E., *Critique de la raison pure*, Trad. française par A. Tremesaygues et B. Pacaud 1905

Katz J., Lindell Y., *Introduction to Modern Cryptography*, CRC Press, nov. 2014

Larguier J., Levy-Brulh H. cités par J. Pradel, *Procédure pénale*, Cujas, 14e éd. 2008-2009

Larroumet C., *Droit civil. Introduction à l'étude du droit privé*, t. 1, Economica, Paris, 4e éd. 2004

Laurent F. , *Principes de droit civil français*, t. XIX : Durand et Pedone, 1878

Le Baron Locré M., *La Législation civile, commerciale et criminelle de la France*, tome 7, Treuttel, 1828

Leclerc O., *Le juge et l'expert. Contribution à l'étude des rapports entre le droit et la science*, LGDJ, coll. Bibliothèque droit privé, 2005

Leclerc O., Wigmore J., *Un jalon vers une « science de la preuve ». La représentation graphique des raisonnements probatoires*, Tiré à part, Dalloz, févr. 2019

Legeais R., *Les règles de preuve en droit civil, permanence et transformation*, LGDJ, 1955

Lessig L., Code Version 2.0, Basic Books, USA, 1999

Lévy J.-P., Castaldo A., *Histoire du droit civil*, Dalloz 2002

Lévy-Bruhl H., *La Preuve judiciaire. Étude de sociologie juridique*, Librairie Marcel Rivière et Cie, 1964

Louis-Lucas P., *Vérité matérielle et vérité juridique*, *in* Mélanges R. Savatier, Dalloz, 1965

Loussouarn Y., Bourel P., Vareilles-Sommières P.de, *Droit international privé*, Dalloz, 10e ed., 2013

Malaurie P., Aynès L., Stoffel-Munck P., *Les obligations*, 4e éd., Defrénois, Lextenso éditions, coll. Droit civil, 2009

Malaurie P., *Droit de la famille*, LGDJ, 6e ed., janv. 2018

Mayer P., Heuzé V., *Droit international privé*, 11e ed., LGDJ, coll. Domat droit privé, 2014

Mekki M., Cadiet L., Grimaldi C. (dir.), *La preuve : regards croisés*, Thèmes et commentaires, Dalloz, 2015

Montesquieu, *De l'esprit des lois*, 1963

Moussa T., Arbellot F., Delbano F., Loriferne D., Martin J.-P., Matet P., Vigneau V., *Droit de l'expertise 2016/2017*, ss. dir. de T. Moussa, 3e ed., Dalloz action, dec. 2015

Moussa T., *Dictionnaire juridique expertise – Matières civile et pénale*, 2e éd., Dalloz, 1988

Oram A., *Peer-to-peer: harnessing the benefits of a disruptive technology 4-5*, 2001

Perelman C. et Foriers P. (dir.), *La preuve en droit*, coll. Travaux du Centre national de recherches de logique, Bruylant, 1981

Planiol M., Ripert G., *Traité pratique de droit civil français*, t.7, 2e ed., 1952

Popper K., *La connaissance objective*, trad. J.-J. Rosat, Flammarion, coll. Champs essais, 1998

Popper K., *Le réalisme et la science*, Hermann, 1990

Puigelier C. (dir.), *La preuve. Etudes juridiques*, Economica, 2004

Racine J.-B., *Droit de l'arbitrage*, Thémis droit, Puf, 2016

Ricœur P., *Histoire et vérité*, Seuil, 1955, p.156.

Ripert G., Boulanger J., *Traité de droit civil*, t.2, LGDJ, 1957

Ripert G., *Les forces créatrices du droit*, Paris, Librairie générale de droit et de jurisprudence, 1955

Ripert G., *Traité pratique de droit civil français*, t. 6, 1952

Rivero J., *Fictions et présomptions en droit public français*, *in* C. Perelman, P. Foriers (ss. dir.), Bruxelles, Bruylant, 1974

Schuhl F., *Cyberdroit. Le droit à l'épreuve de l'Internet*, Praxis Dalloz, 2018-2019

Shelton D. L., *Soft law*, *Handbook of International Law*, Routledge Press, 2008

Sirius R. U., Jude S., *How to Mutate and Take Over the World*, Ballantine Books, févr. 1996

Stoffel-Munck P., Malaurie P., Aynès L., *Droit des obligations*, 9e éd., LGDJ, coll. Droit civil, sept. 2017

Tarde J.-G., *La philosophie pénale*, Paris Cujas, coll. Bibliothèque internationale de criminologie, 4e ed., 1972

Terré F., *Introduction générale au droit*, Dalloz coll. « Précis », 2015

Terré F., Simler P., Lequette Y., *Droit civil, Les obligations*, Coll. Précis Dalloz, 10e éd. 2009

Tissier A., *Le rôle social et économique des règles de la procédure civile. Les méthodes juridiques*, *in* Leçons faites aux Collège libre des sciences sociales, Girard et Brière, 1910-1911

Trébulle F. G. , *L'émission de valeurs mobilières*, Economica, 2002

Truilhé-Marengo E., *Preuve scientifique, preuve juridique*, Bruxelles, Larcier, 2011

Vergès E., *Procédure pénale*, Lexis Nexis, 2011, n°111

Vergès E., Vial G., Leclerc O., *Droit de la preuve*, Puf, coll. Thémis, 2015

Vignal T., *Droit international privé*, Sirey, coll. Sirey Université, 4e ed., 2017

Vigneau V., *Droit de l'expertise*, Dalloz action, 2016/2017

Waline M., « Le pouvoir normatif de la jurisprudence », *La technique et les principes du droit public. Études en l'honneur de Georges Scelle*, Paris, LGDJ, 1950

Articles spéciaux :

« Question à Olivier Le Guen sur la perquisition et la saisie des crypto-actifs », Dossier : la justice pénale à l'épreuve des crypto-monnaies, Dalloz IP/IT n°10, oct. 2019

Autrey G., Marchant G., « Admissibility of Blockchain Evidence », Arizona State University - College of Law, nov. 2018

Back A., « A partial hash collision based postage scheme », 1997

Back A., Corallo M., Dashjr L., Friedenbach M., Maxwell G., Miller A., Poelstra A., Timón J., Wuille P., « Enabling blockchain innovations through pegged sidechains », 2014

Barbet-Massin A., « Réflexions autour de la reconnaissance juridique de l'horodatage blockchain par le législateur italien », RLDI n°157, mars 2019

Barbet-Massin A., Brosset J., « La souscription de crypto-actifs et de jetons d'ICOs : les recours des investisseurs », RLDA n°6531, suppl. n°140, sept. 2018

Barbet-Massin A., Chafiol F., « La blockchain à l'heure de l'entrée en application du règlement général sur la protection des données », Dossier données à caractère personnel, quelle circulation de demain, Dalloz, Dalloz IP/IT n°12, dec. 2017

Barbet-Massin A., Dahan V., « Les enjeux de la blockchain en droit d'auteur », BRDA 8/18, 15 avr. 2018

Barbet-Massin A., Khatab A., « Les « brevets blockchain » : état des lieux et perspectives », Expertises des systèmes d'informations, mai 2018

Barbet-Massin A., Lorentz P., Brosset J., « Les activités sur actifs numériques issues de la loi PACTE », RLDA, sept 2019

Barbet-Massin A., Lorentz P., Bensoussan A., « La mise en œuvre d'une ICO : les étapes en pratique », Etude n°1, RDBF n°1, janv.-févr. 2019

Barbet-Massin A., O'Rorke W., Fiche pratique n°4317 - blockchain et données personnelles, Lexis Nexis, juill. 2019

Barlow J.-P., « Déclaration d'Indépendance du Cyberespace », 8 févr. 1996

Baron R., « Introduction aux technologies *blockchain* supports des crypto-monnaies », Dossier « Monnaies », RDBF n°4, juill. 2019

Barraud B., « Les *blockchains* et le droit », RLDI n°147, avr. 2018

Ben-Sasson E., Chiesa A., Garman C., Green M., Miers I., Tromer E., Virza M., « Zerocash: Decentralized Anonymous Payments from Bitcoin », 2014

Berbain C., « La blockchain : concept, technologies, acteurs et usages », Annales des mines - réalités industrielles, août 2017

Bictin N., « Quelle place pour la blockchain en droit français de la propriété intellectuelle », Propriétés intellectuelles n°65, oct. 2017

Bonneau T., « Le bitcoin, une monnaie ? », Rev. Banque et droit, 2015

Butterin V., « A next-generation smart contract and decentralized application platform », dec. 2013

Canas S., « Blockchain et preuve : le point de vue du magistrat », Dalloz IP/IT, févr. 2019

Canivet G., « Présentation de la table ronde "Preuve et blockchain" », Dossier Blockchain et preuve, Dalloz IP/IT n°2, févr. 2019

Cattalano G., « Smart contracts et droit des contrats », AJ contrat n°7, Dossier « blockchain, smart contract et droit », juill. 2019

Causse H., Perspective colloque AFDIT, CRED « Qualification et état de la blockchain », le 24 avr. 2019

Chaum D. « Blind signatures for untraceable payments », Advances in Cryptology Proceedings of Crypto, vol. 82, n°3, 1982

Clément-Fontaine M., « Le smart contract et le droit des contrats dans l'univers de la mode », Dalloz IP/IT 2018

Coiffard D., « Didier Coiffard, président du Conseil supérieur du notariat : "La blockchain a un sens pour répartir une partie de la confiance en rendant une information infalsifiable mais cette confiance est très en deçà de celle conférée par le notaire" », RLDC n°147, 1er avr. 2017

Corbion-Condé L., « De la défiance à l'égard des monnaies nationales au miroir du bitcoin», RDBF n°2, dossier 13, mars 2014

Cremers T., « Qualifications juridiques de valeurs numériques et titres inscrits en DEEP », BJB n°6, n°118s0, nov. 2019

Dai W., « B-Money », 1998

De Filippi P., « The interplay between decentralization and privacy: the case of blockchain technologies, Journal of Peer Production », Alternative Internets n°7, 2016

De Filippi P., « What Blockchain Means for the Sharing Economy », Harvard Business Review, 15 mars 2017

De Filippi P., Jean B., « Les *Smart contracts*, les nouveaux contrats augmentés ? », Revue de l'ACE n°137, septembre 2016

De Monbynes Y., « Anarchie, cypherpunk et libertés : les racines philosophiques de bitcoin », Contrepoints, mars 2018

De Monbynes Y., « L'enfance mystérieuse du bitcoin », Contrepoints, déc. 2017

De Thésut Dufournaud S., « La blockchain de consortium », RLDA n°129, sept. 2017

Delahaye J.-P., « Crypto-monnaies décentralisées raisonnables », Blogs pour la science, janv. 2020

Delahaye J. P., « Les *blockchains*, clefs d'un nouveau monde », Logique et calcul, Pour la Science n°449, mars 2015

Dempuré F., « Où en est la révolution Blockchain ? », JCP N n°18-19, 4 mai 2018

Deroulez J., « Blockchain et preuve », Dalloz avocats - Exercer et entreprendre n°2, févr. 2017

Dondero B., « La blockchain et le droit des sociétés », BJS mai 2019

Dorol S., « Blockchain et métiers du droit : la fin des tiers de confiance ? », Dossier « Blockchain et métiers du droit : une force vive ou subversive ? », Dalloz IP/IT n°2, févr. 2020

Douville T., « *blockchains* et preuve », D.2018, 22 nov. 2018

Douville T., « Blockchain et protection des données à caractère personnel », AJ Contrat, dossier, juill. 2019

Drummond F., « Loi PACTE et actifs numériques », BJB n°4, juill. 2019

Evans A., Kantrowitz W., Weiss E., « A User Authentication Scheme Not Requiring Secrecy in the Computer », Communications of the ACM 17(8):437–442, 1974

Fauchoux V., Gouazé A., « Pourquoi la blockchain va révolutionner la propriété intellectuelle ? Application pratique au secteur de la mode », Propriétés intellectuelles n°65, oct. 2017

Favreau A., « L'avenir de la propriété intellectuelle sur la blockchain », Propriétés intellectuelles n°67, avr. 2018

Fisher M., Lynch N., Paterson M., « Impossibility of consensus with one faulty process », Journal of the ACM, vol. 32, n°2, 1985

Frison-Roche M.-A., « Analyse des *blockchains* au regard des usages qu'elles peuvent remplir et des fonctions que les officiers ministériels doivent assurer », Defrénois n°25, juin 2019

Guerlin G., « Considération sur les smart contracts », Dalloz IP/IT n°512, oct. 2017

Grégoire O., « Loi PACTE », Dossier spécial sur la loi relative à la croissance et la transformation des entreprises, JCP E n°26, 27 Juin 2019

Griffin J. M., Shams A., « Is Bitcoin Really Un-Tethered ? », Librairie SSRN, juin 2018

Grimaldi A-S., « Les contraintes du droit des obligations sur les opérations d'ICO », D. n°21, le 7 juin 2018

Guégan D., « Blockchain Publique versus Blockchain Privée : Enjeux et Limites », Documents de Travail du Centre d'Economie de la Sorbonne, june 2017

Guo A., « Blockchain Receipts : Patentability and Admissibility in Court », Chicago-Kent Journal of Intellectual Property Volume n°16, Issue n°2, Article 9

G'Sell F., « Comment traiter juridiquement la décentralisation ? Les ordonnances blockchain et la Lex Cryptographia », Blog de Florence G'Sell, dec. 2017

Haber S. et Stornetta W.S., « How to Time-Stamp a Digital Document », Journal of Cryptology, vol. 3, janv 1991

Hugh E., « A Cypherpunk's Manifesto », 1993

Jault-Seseke F., « La blockchain au prisme du droit international privé, quelques remarques », Dalloz IP/IT n°10, oct. 2018

Jomni A., « crypto-tracking : les nouveau outils d'enquête pour les forces de l'ordre », Revue de la gendarmerie nationale n°263, dec. 2018

Julienne M., « Pratique notariale et numérique : état des lieux », Dalloz IP/IT n°2, fevr. 2019

Kirtchev C. A., « Cyberpunk Manifesto », 1997

Kiviat T. I., « Beyond bitcoin: issues in regulating blockchain transactions », Duke Law Journal, Vol. 65:569, 2015

Lamport L., « Time, clocks, and the ordering of events in a distributed system », Communications of the ACM, vol. 21, issue 7, 1978

Lamport L., Shostak R., Pease M., « The Byzantine Generals Problem », 4 ACM Transactions on Programming Languages and Systems at 382, vol. 4, issue 3, juill. 1982

Lasserre-Capdeville J., « Le Bitcoin », JCP E, 2014

Ledieu M.-A., « La Baas démocratise la blockchain », Expertises des systèmes d'information n°440, nov. 2018

Legeais D., « Aspects juridiques », Dossier n°30 « Les monnaies », actes de conférence, RDBF n°4, juill.-août 2019

Legeais D., « Loi PACTE : les dispositions relatives aux actifs numériques et aux prestataires de services numériques », Dossier spécial sur la loi relative à la croissance et la transformation des entreprises, JCP E n°26, 27 Juin 2019

Lessig L., « Code Is Law. On Liberty in Cyberspace », Harvard Magazine, janv. 2000

Löber K., « Central bank considerations around digital currencies », Dossier « Monnaies », RDBF n°4, juill. 2019

Magnier V., « Enjeu de la blockchain en matière de propriété intellectuelle et articulation avec les principes généraux de la preuve », Dossier Blockchain et preuve, Dalloz IP/IT n°2, févr. 2019

Malaurie-Vignal M., « Blockchain et propriété intellectuelle », Prop. Ind. n°10 étude 20, oct. 2018

Manas A., Bosc-Haddad Y., « La (ou les) blockchain (s), une réponse technologique à la crise de confiance », Annales des mines – réalités industrielles 2017/03, août 2017

Marain G., « Le bitcoin à l'épreuve de la monnaie », AJ Contrat, dec. 2017

Marin-Dagannaud G., « Le fonctionnement de la blockchain », Annales des Mine, 3 août 2017

Marraud des Grottes G., « Preuve blockchain : et si la soft law était une première étape ? », Wolters Kluwer, Actualités du droit, 6 dec. 2019

Martinon J., « Crypto-actifs : la justice pénale à l'épreuve des crypto-monnaies », Dossier : la justice pénale à l'épreuve des crypto-monnaies, Dalloz IP/IT n°10, oct 2019

Martinon J., « Phénomènes criminels célèbres ou exotiques dans le champ des crypto-actifs (illustrations extraites de la présentation de Patrice Réveillac, Europol) », Dossier : la justice pénale à l'épreuve des crypto-monnaies, Dalloz IP/IT n°10, oct 2019

Mathis B., « Blockchain : un décret pour rien », RLDI, févr. 2019

Matonis J., « Why Are Libertarians Against Bitcoin ? », The Monetary Future, 16 juin 2011

Mattila J., « The Blockchain Phenomenon – The Disruptive Potential of Distributed Consensus Architectures », Berkeley rountable on the international economie (BRIE) Working Paper 2016-1, Université de Berkeley, mai 2016

Matzutt R., Hiller J., Henze M., Ziegeldorf J.-H., « A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin », Data Protection Research Institute, Goethe University, Frankfurt, fevr. 2018

Maury J., « Observation sur la jurisprudence en tant que source du droit », *in* Etude offertes au Professeur Ripert, LGDJ, Tome 1, 1950

May T., « Crypto Anarchist Manifesto », 1988

Mekki M., « Blockchain : l'exemple des smart contracts. Entre innovation et précaution », 15 mai 2018

Mekki M., « Blockchain, smart contracts et notariat : servir ou asservir ? », JCP N n°27, 6 juill. 2018

Mekki M., « Blockchain et métiers du droit en questions », Dossier « Blockchain et métiers du droit : une force vive ou subversive ? », Dalloz IP/IT n°2, févr. 2020

Mekki M., « Le contrat, objet des smart contrats (partie 1) », Dalloz IP/IT, juill.-août 2018

Mekki M., « Les mystères de la blockchain », D. n°37, 2 nov. 2017

Mekki M., « Le smart contract, objet du droit (partie 2) », Dalloz IP/IT, janv. 2019

Merkle R. C., « A Digital Signature Based on a Conventional Encryption Function » *in* Advances in Cryptology - CRYPTO '87, Lecture Notes in Computer Science book series, LNCS, volume 293, 1987

Mis J.-M., « Crypto-monnaie : une régulation/réglementation « contre-nature » ou « naturellement indispensable » à son développement ? », Dossier : la justice pénale à l'épreuve des crypto-monnaies, Dalloz IP/IT n°10, oct 2019

Moody D., « NIST status update on Elliptic Curves and Post-Quantum Crypto », mars 2019

Mostert F., Wang J., « The Application and Challenges of *Blockchain* in Intellectual Property Driven Businesses in China », Tsinghua China Law Revue, vol. 11, dec. 2018

Nakamoto S., « Bitcoin : A Peer-to-Peer Electronic Cash System », 2008

Narayanan A., « What happened to the crypto dream ? », Part 2, IEEE Security & Privacy, Vol. 11, Issue 3, mai-juin 2013

Neally D. J., Hodg M. L., « Blockchain in the Courts », Center for Law, Science and Innovation, Sandra Day O'Connor College of Law Arizona State University, nov. 2018

Netter E., « Blockchain et professions réglementées », Cahiers de droit de l'entreprise n°3, Dossier 21, mai 2018

O'Dair M. et al., Music On The Blockchain, Blockchain For Creative Industries Research Cluster, Middlesex University, report n°1, juill. 2016.

O'Whielacronx Z., « introducing BLAKE2 – an alternative to SHA-3, SHA-2 and MD5 », 21 déc. 2012

Orcutt M., « Some crypto-criminals think jumping across *blockchains* covers their tracks. Big mistake », MIT Technology Review, 22 août 2019

Parouty J.-L., Bitcoin J.-L., « Éléments de compréhension technique », CNRS-IBS, 2016

Pavel I., « La blockchain – les défis de son implémentation », Annales des mines - réalités industrielles, août 2017

Penneau A., « Normalisation. 3 questions : l'accessibilité aux documents AFNOR en question », JCP E n°18, n°320, 4 mai 2017, p.5

Pérez Marco R., « Blockchain : l'autre révolution venue du bitcoin », CNRS Le Journal, mai 2016

Perez Marco R., « Blockchain time and Heisenberg Uncertainty Principle », 2016

Perez Marco R., « Ricardo Perez-Marco : "95 % des monnaies créées aujourd'hui vont disparaître" », bitcoin.fr, juill. 2018

Peyrat O., Legendre J.-F., « Pourquoi la normalisation s'intéresse-t-elle à la blockchain ? », Annales des Mines - Réalités industrielles, août 2017

Pion C., Blemus S., « Blockchain, minibons et titres financiers », RDBF n°1, étude n°2, janv. 2019

Polydor S., « Blockchain Evidence in Court Proceedings in China – A Comparative Study of Admissible Evidence in the Digital Age (as of June 4, 2019) », Stanford Journal of *Blockchain* Law and Policy, jan. 2020

Purdy G. B., « A High Security Log-in Procedure », Communications of the ACM 17(8):442–445, 1974

Raskin M., « The Law and Legality of *Smart contracts* », Georgetown Law Technology Review 304, 2017

Roussille M., « le bitcoin : objet juridique non identifié », Rev. Banque et droit n°159, 2015

Sannino P., « « Disruption », Justice prédictive, Blockchain, legaltech : de nouvelles opportunités pour la profession ? », Procédure n°12, entretien 1, dec. 2017

Schiller S., Cremers T., « Effectivité de ma représentation et de la transmission des titres financiers non cotés par une blockchain ainsi que des minibons », JCP G 2019

Schrepel T., « Anarchy, State, and Blockchain Utopia: Rule of Law Versus Lex Cryptographia », *in* General Principles and Digitalisation (chapitre 15), Libraire SSRN, 12 nov. 2019

Schrepel T., « Is Blockchain the Death of Antitrust Law ? The Blockchain Antitrust Paradox », Georgetown Law Technology Review / 3 Geo. L. Tech. Rev. 281, juin 2018

Sinclair L., « Arbitrage et nouvelles technologies : « rien ne se perd, rien ne se crée, tout se transforme » », Journal de l'arbitrage de l'Université de Versailles - Versailles University Arbitration Journal n°1, étude 5, janv. 2019

Streiff V., « Blockchain et authenticité : pour une copie non certifiée conforme », Dossier *blockchain* et métiers du droit : une force vive ou subversive, Dalloz IP/IT n°95, févr. 2020

Stucki D., Clavé S., « Le nouveau statut du prestataire de services en crypto-actifs », RB n°830, mars 2009

Szabo N., « Secure Property Titles with Owner Authority », 1998

Szabo N., « Smart contracts : building blocks for digital markets », 1996

Szabo N., « Unenumerated: Bit gold », 2005

Tenyson J., « What is the impact of *blockchains* on privacy ? », Open Data Institute, dec. 2015

Tasca P., Claudio Tessone J., « Taxonomy of Blockchain Technologies. Principles of Identification and Classification », mars 2018

Treppoz E., « Quelle régulation internationale pour la blockchain ? Code is law v. Law will become Code », *in La blockchain : big bang de la relation contractuelle*, Dalloz, coll. Thèmes et commentaires, 2019

Valot C., « Accuracy of distributed timestamps », Rapport de recherche n°1804, Programme 1 Architecture parallèles, Bases de données, Réseaux et systèmes distribués, Inria, dec. 1992

Wright A., de Filippi P., « Decentralized Blockchain Technology and the Rise of Lex Cryptographia », Librairie SSRN, 12 mars 2015

Wüst K., Gervais A., « Do you need a Blockchain ? », actes de colloque *in* Crypto Valley Conférence sur la Technologie Blockchain Technology 2018

Zolynski C., « Blockchain et smart contracts : premiers regards sur une technologie disruptive », RD Banc. Fin., Dossier 4, janv. 2017

Articles généraux

Abbott K. W., Keaohane R. O., Moravcsik A., Slaughter A.-M., Snidal D., « The Concept of legalization », International Organization, vol. 54, n°3, Summer 2000

Actualité : 113e congrès des notaires de France : le notaire au cœur des mutations de la société, Defrénois, n°def129c3, 28 sept. 2017

Algan Y., Cahuc C., « La société de défiance : comment le modèle social français s'autodétruit », ENS, 2007

Allais M., « Autorité de la science ou autorité en matière de science ? L'immense danger d'une domination oppressive des pseudo-vérités établies », *in L'autorité*, ss. dir. J. Foyer, G. Lebreton et C. Puigelier, Puf, coll. Cahiers des sciences morales et politiques, 2008

Amrani-Mekki S., « Les chantiers de la justice numérique, procédure civile et réseau des juridictions : le rationnel est-il toujours raisonnable ? », Gaz. Pal., 6 févr. 2018

Autrey G., Marchant G., « Admissibility of *Blockchain* Evidence », Arizona State University - College of Law, nov. 2018

Aynès A., « Conventions sur la preuve : validité limitée », *in* dossier Réforme du droit de la preuve, Droit et patrimoine n°250, sept. 2015

Aynès A., Bretzner J.-D., « Droit de la preuve septembre 2016 - janvier 2017 », D.2017

Aynès A., Bretzner J.-D., « Droit de la preuve juin 2015 - juin 2016 », D.2016

Aynès L., « Avons-nous besoin de l'acte authentique ? », Defrénois, n°20, 30 oct. 2013

Beaufrere J.-M., « Faut-il demander à l'expert une "déclaration d'indépendance" », 2007

Belaïd S., « Essai sur le pouvoir créateur et normatif du juge », Revue internationale de droit comparé, 1975

Bitan H. « La signature électronique : comment la technique répond-elle aux exigences de la loi », Gaz. Pal. 19/20 ; juill. 2000

Blanchet T., **«** La réalisation du minutier central des notaires de France (la conservation des actes authentiques électroniques) **»**, LPA n° PA20051941729, sept. 2005

Bloch P., « L'obligation de transférer la propriété dans la vente », RTD civ. 1988

Boccara V., « Du droit de la preuve au droit à la preuve, question de mots ou changement de cap ? », LPA n°PA201310902, 31 mai 2013

Boulanger J., « Notation sur le pouvoir créateur de la jurisprudence civile », RTD Civ., 1961

Brenner C., « La réforme de la procédure civile : un chantier de démolition ? », D. 2018

Byk C., « Justice et expertise scientifique : un dialogue organisé dont il faut renouveler les fondements », RRJ 2013

Cadiet L., « Observations sur l'internationalisation du droit de la preuve », *in* Studi di diritto processuale civile in onore di Giuseppe tarzia, Tome I, II, III, giuffrè. editore, 2005

Caprioli E., « La loi française sur la preuve et la signature électroniques dans la perspective européenne, Dir. 1999/93/CE du Parlement européen et du Conseil 13 décembre 1999 », JCP G n°18, 3 mai 2000

Caprioli E. « La loi type de la CNUDCI sur les signatures électroniques », chron. 27, Com. com. élect., déc. 2001

Caprioli E., « Preuve des copies numériques. De la fiabilité des copies numériques », Comm. com. électr. n°2, comm. 19, févr. 2017

Caprioli E., Cantero A., « Traçabilité et droit de la preuve électronique », Droit et patrimoine n°93, 1er mai 2001

Caratini M., « Experts et expertise dans la législation civile française. Principes généraux », Gaz. pal., 22 janv. 1985

Caron C., « Les licences de logiciels dits « libres » à l'épreuve du droit d'auteur français », D. 2003

Castet-Renard C., « Quelles nouveautés en matière de preuve numérique », in Justice et cassation, Revue annuelle des avocats au Conseil d'État et à la Cour de cassation, Dossier La preuve, mai 2017

Catala P., « Le formalisme et les nouvelles technologies », Defrénois 2000

Catala P., Gautier P.-Y., « L'audace technologique à la Cour de cassation vers la libéralisation de la preuve contractuelle », JCP E n°23, 4 juin 1998

Cayre F., « Cryptographie, du chiffre et des lettres », Revue DocSciences n°5, Les clés de la révolution numérique, CRDP de l'académie de Versailles, nov. 2008

Chainais C., Lagarde X. (dir.), « Réformer la justice civile : séminaire de droit processuel – actes du colloque du 6 février 2018 », JCP G 2018

Charbonneau C., Pansier J.-F., « La signature électronique, signature sous surveillance (à propos du décret n°2001-272 du 30 mars 2001) », Petites affiches n°69, 6 avr. 2001

Chatzistavrou F., **«** L'usage du soft law dans le système juridique international et ses implications sémantiques et pratiques sur la notion de règle de droit », Open Edition, Le Portique, janv. 2005

Constantin A., « Bourses de valeurs - Affaire Madoff : les belles questions de droit posées par la propriété des titres Luxalpha », etude doctr. n°434, JCP G n°15, 11 avr. 2011

Contis N., Gayrard J., « Invoquer la nullité d'un rapport d'expertise judiciaire », JCP n°5, févr. 2016

Costes L., « Pas de violation du droit à la vie privée de caissières de supermarché espagnoles filmées à leur insu par des caméras de sécurité », Actualités du droit, oct. 2019

Croze H., « Informatique, preuve et sécurité », D. 1987

Croze H., « La preuve par huissier de justice », Gaz. pal. n°148, mai 2013

De Leyssac L., « Les conventions sur la preuve en matière informatique », *in* Informatique et droit de la preuve, Des Parques, 1987

De Leyssac L., « Plaidoyer pour un droit conventionnel de la preuve en matière informatique », Cahiers du Barreau de Paris, oct. 1987

David R., « La Commission des Nations unies pour le droit commercial international », JDI, 1980

Douville T., « Informatique - Le règlement européen sur l'identification électronique et les services de confiance (eIDAS) – Etude », JCP E n°1, 5 Janv. 2017

Douville T., « Nouveau droit des contrats (fiabilité des copies) : publication du décret d'application », D.2016

Duguit L., « L'acte administratif et l'acte juridictionnel », RDP, 1906

Dumortier T., « La certification au service de l'administration : essai de typologie et enjeux juridiques », RDP, nov. 2012

Dumoulin L., « L'expertise judiciaire dans la construction du jugement : de la ressource à la contrainte », Droit et Société n°44-45, Persée, 2000

Duparc C., « L'adaptation de l'huissier de justice à l'économie digitale », AJCA, avr. 2016

Edmond E., « Les experts : auxiliaires ou substituts du juge ? », coll. Centre français de droit comparé, Revue internationale de droit comparé. Vol. 61 n°3, 2009

Eisemann P. M. , « The gentleman's Agreement comme source du droit international », JDI, 1979

Estrella-Faria J.-A., « The work of the United Nations Commission on International Trade Law (U.N.C.I.T.R.A.L.) », RDU, 1996

Fabre-Magnan M., « Le mythe de l'obligation de donner », RTD civ. 1996

Flückiger A. « Pourquoi respectons-nous la *soft law* ? », Revue européenne des sciences sociales XLVII-144, Openedition, 2009

Francès-Magre M., « Caractère subsidiaire de l'expertise par rapport aux mesures d'instruction exécutées par un technicien », JCP, 1975

Gaillard A., « Le sapiteur ou l'assistance technique », CNECJ, janv. 2007

Garcias M., Chouzier M., « La preuve informatique – Quelles nouveautés techniques pour quelles évolutions juridiques », Lexbase Hebdo édition affaires n°280, janv. 2012

Gautier P.-Y., « Les œuvres du crooner dans la « maison » de l'internaute : promenade collective, mais non autorisée, sur un site numérique », D. 1996

Gautier P. Y., Linant de Bellefonds X., « De l'écriture électronique et des signatures qui s'y attachent », JCP G, 2000

Gautrais V., « Preuve des reproductions : vues d'ailleurs ! », Cahiers Droit, Sciences & Technologies, 2014

Girardet A., « La réalité de l'indépendance judiciaire », mai 2007

Goldman B., « Les travaux de la Commission des Nations unies pour le droit commercial international », JDI, 1979

Grignon Dumoulin S., « L'office du juge civil dans la recherche de la preuve », Justice & Cassation, Revue annuelle des avocats au Conseil d'État et à la Cour de cassation, Dossier la preuve, Dalloz, 2017

Grimaldi C., « L'acte sous-seing privé, l'acte authentique et l'acte contresigné par un avocat : quelle utilité », JCP E n°1, 7 janv. 2010

Groud T. H., « La preuve en droit international privé », revue internationale de droit comparé vol. n°53, oct.-dec. 2001

Guerlin G., « La procédure civile en chantier », RLDC 2018

Hayek F. A., « The Use of Knowledge in Society », The American Economic Review Vol. 35, n°4, sept., 1945

Herzog-Evans M., « La perception de l'expertise par les JAP : une recherche empirique », AJ pénal, 2014

Hong X., « *Online Dispute Resolution for E-Commerce in China: Present Practices and Future Developments* », Hong Kong Law Journal, 2004

Houin R., « Le progrès de la science et le droit de la preuve », Revue internationale de droit comparé, Vol. 5 n°1, janv.-mars 1953

Huet J. , « Des différentes sortes d'obligations et plus particulièrement de l'obligation de donner, la mal nommée, la mal-aimée », *in* Études J. Ghestin, LGDJ 2001

Huet J., « Preuve et sécurité juridique en cause dans l'immatériel », Arch. phil. droit n°43, 1999

Huet J., « Vers une consécration de la preuve et de la signature électronique », D. 2000

Jallamion C., « L'apport des notaires dans l'émergence et la formulation des contrats innomés », Defrénois n°20, n°113z6, 30 oct. 2013

Jolowicz J. A., « Adversarial and Inquisitorial Models of Civil Procedure », JCLQ, vol. 52, avr. 2003

Kahn P., « La modélisation au service de la fonction normative de la CNUDCI : la modélisation comme instrument », LPA n°252, 18 dec. 2003

Kenfack H., « La limitation des textes de la C.N.U.D.C.I aux relations internationales », LPA n°252, dec. 2013

Khalil L. J., « Signature électronique : certificats qualifiés « publics » ou certificat qualifiés « privés », Com. Com. élec. n°4, avr. 2003

Lachkar J. D., « La force probante de l'acte d'huissier de justice », JCP N n°5, févr. 2013

Lagarde F., « règlementation, normalisation, certification, labellisation… : élément de définition », Jurisport n°188, juill./août 2018

Lagarde X., « La preuve en droit », *in* Le temps des savoirs, Odile Jacob, 2003

Lagarde X., « Vérité et légitimité dans le droit de la preuve », Droits, 1993

Lardeux G., « Commentaire du titre IV bis nouveau du livre III du code civil intitulé "De la preuve des obligations" ou l'art de ne pas réformer », D. avr. 2016

Lardeux G., « Preuve : règles de preuve », RTD civ., Dalloz, oct. 2018

Lardeux G., « Preuve civile et vérité », *in* Le droit en autonomie et ouverture. Mél. En l'honneur de J.-L. Bergel, Bruylant, 2013

Larguier J., « La preuve d'un fait négatif », RTD civ. 1953

Lassere-Kiesow V., « La vérité en droit civil », D. 2010

Le Nabasque H., Reygrobellet A., « L'inscription en compte des valeurs mobilières », RDB 2000

Legoux A., « Vérité médicale, vérité juridique », Gaz. pal. n°277, oct. 2014

Legrain J., « Le constat d'huissier sur Internet », JCP G n°39, sept. 2010

Lerner J. et Tirole J. , « The scope of open source licensing », Journal of Law, Economics, and Organization, Oxford University Press, 2005

Loquin V., « Les experts auxiliaires ou substituts du juge ? », *in* rapport de synthèse, Les experts : auxiliaires ou substituts du juge, Centre français de droit comparé, 2009

Loyac F., « Les frais d'expertise », Rev. jur. Ouest 1991

Luby M., « La CNUDCI et l'intégration régionale », LPA n°252, 18 dec. 2003

Ludes B., « La situation de conflit d'intérêts intra-personnelle », Experts, déc. 2012

Marguénaud J.- P., « Le droit à l'expertise équitable », D. 2000

Mariez J.-S., « Une nouvelle étape vers un accès transfrontalier aux preuves numériques : l'initiative européenne « e-evidence » ou la recherche d'un équilibre entre efficacité des enquêtes pénales, droit des personnes concernées et sécurité », RLDI n°146, mars 2018

Mathias J.-D., « L'authenticité électronique », LPA, 2 avr. 2001

Mathieu F., « L'acte authentique électronique : état des lieux et perspectives », RLDC n°175, nov. 2019

Meiller C., V. Chapuis, « Brevet : sale temps pour la juridiction unifiée du brevet », Dalloz actualité, 8 avr. 2020

Mekki M., « Charge de la preuve et présomptions légales – L'art de clarifier sans innover », Dr. et patrimoine sept. 2015

Mekki M., « La gestion contractuelle du risque de la preuve (2e partie) », Revue des contrats n°2, avr. 2009

Mekki M., « Notaire - Congrès MJN 2017-2018 : rapport de synthèse », JCP N n°47, 24 nov. 2017

Mekki M., « Réflexions sur le risque de la preuve en droit des contrats (1ère partie), Revue des contrats n°3, juill. 2008

Mekki M., « Retour vers le futur de l'acte authentique !. - à propos du rapport de la commission de réflexion sur l'authenticité », JCP G n°42, 14 oct. 2013

Mekki M., « Vérité et preuve. Rapport français », *in* La preuve. Journées internationales 2013 d'Amsterdam, Pays-Bas et Liège, Belgique, coll. Travaux Henri Capitant, vol. LXIII, Paris / Bruxelles, LB2V et Bruylant, 2015

Mekki M., « Voyage au pays de l'authenticité. - quelques réflexions à partir du rapport de la commission présidée par le professeur laurent aynès », JCP N N°41, 11 oct. 2013

Melin-Soucramanien F., « Le principe d'égalité dans la jurisprudence du Conseil constitutionnel. Quelles perspectives pour la question prioritaire de constitutionnalité ? », Cahiers du conseil constitutionnel n°29, Dossier : la question prioritaire de constitutionnalité, 2010

Merkin C., de Saint Mars B., « Transfert de propriété sur le marché des valeurs mobilières », RD bancaire et bourse, janv. 94

Michelet A., « La juridiction unifiée du brevet : où en sommes-nous ? », Popr. Indus. n°3, étude 5, mars 2018

Migayron S., « Informatique – pratique contentieuse. De l'information numérique à la preuve », Comm. com. électr. n°4, avr. 2017

Moury J., « Les limites de la quête en matière de preuve : expertise et *jurisdictio* », RTD civ., 2009

Moussa T., « L'expertise judiciaire et les autres expertises au regard du principe de la contradiction », Rencontres université – Cour de cassation, BICC hors-série, 23 oct. 2004

Mousseron J.-M., « La gestion des risques », RTD civ. 1988

Olivier M., « Aspects juridiques et déontologiques du rapport d'expertise vétérinaire », *in* De l'expertise civile et des experts, t.2, Berger-Levrault, 1995

Olivier M., « L'expertise en matière civile », *in De l'expertise civile et des experts*, t.2, Berger-Levrault, 1995

Oppeti B., « Les rôles respectifs du juge et du technicien dans l'administration de la preuve en droit privé, *in* Institut d'Etudes Judiciaires, Les rôles respectifs du juge et du technique dans l'administration de la preuve, Puf, 1976

Passant E., « La loi du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique : nouvelle donne pour le droit de la preuve », Cahiers Lamy droit de l'informatique et des réseaux n°125, mai 2000

Perrot R., « Constatations purement matérielles », Procédures n°5, mai 2014

Perrot R., « Le constat d'huissier de justice », CNHJ, 1985

Perrotin F., « L'authenticité à l'heure du numérique », LPA, 30 avr. 2015

Pinchon F., « Point de procédure expertale concernant les sapiteurs », Gaz. Pal. 11 févr. 2003

Poillot-Peruzzetto S., « Les méthodes de la CNUDCI : le choix de l'instrument », LPA n°252, 18 dec. 2003

Ponthoreau M.-C., « Réflexions sur le pouvoir normatif du juge constitutionnel en Europe continentale sur la base des cas allemand et italien », Cahier du conseil constitutionnel n°24, Dossier : le pouvoir normatif du juge constitutionnel, juill. 2008

Pontier J.-M., « La politique de labellisation », AJDA 30/2017, sept. 2017

Pradel J., « La responsabilité pénale de l'expert judiciaire », RSC, 1986

Protais C., « Le réajustement du rapport juge/expert : entre consensus et domination », Revue internationale interdisciplinaire, 2008

Quemener M., Dalle F., « L'accès à la preuve numérique, enjeu majeur de toute enquête pénale : pratique et perspectives », Dalloz IP/IT, juill.-août 2018

Raynouard A., « Adaptation du droit de la preuve aux technologies de l'informatique et à la signature électronique », Defrénois, mai 2000

Reynis B., « L'acte authentique électronique », Defrénois, 15 avr. 2005

Rials S., « Ouverture. L'office du juge », Droits. Revue française de théorie juridique, n°9, « La fonction de juger », PUF, 1989

Robine D., « La réforme du transfert de propriété des valeurs mobilières in l'ordonnance n°2004-604 du 24 juin 2004 portant réforme du régime des valeurs mobilières », LPA, 22 sept.2005

Roussel P., « L'emploi de l'informatique dans l'administration de la preuve », Etude 11, Droit pénal n°9, sept. 2005

Samman T., Neveux N., « La signature électronique : mythe et réalité » Expertises, févr. 2001

Schwerer F., « Réflexions sur la preuve et la signature dans le commerce électronique », Contrats, Conc., Consom., déc. 2000

Tallon D., « Le surprenant réveil de l'obligation de donner – à propos des arrêts de la chambre commerciale de la Cour de cassation en matière de détermination du prix », D. 1992

Théron J., « Améliorer et simplifier la procédure civile : comment regagner la confiance des justiciables ? Aperçu rapide », JCP G 2018

Théry P., « Les finalités du droit de la preuve », Droits 1996

Tricot D., « Qualification et indépendance de l'expert », *in* Les experts : auxiliaires ou susbtituts du juge, coll. Centre français de droit comparé, 2009

Ustor E., « Développement progressif du droit commercial international : un nouveau programme juridique de l'O.N.U. », AFDI, 1980

Vedel G., « L'égalité », *in* La déclaration des droits de l'homme et du citoyen de 1789, ses origines, sa pérennité, La documentation française, 1990

Vergès E., « Droit de la preuve : une réforme en trompe-l'œil », JCP n°17, 17 avr. 2016

Vergès E., « Éléments pour un renouvellement de la théorie de la preuve en droit privé », *in* Mélanges J.-H Robert, Lexis Nexis 2012

Vergès E., « La réforme du droit de la preuve civile : enjeux et écueils d'une occasion à ne pas manquer », D. 2014

Vergès E., « Loyauté et licéité, deux apports majeurs à la théorie de la preuve pénale », D. 2014

Articles de presse

« The trust machine », The Economist, 31 oct. 2015, https://www.economist.com/leaders/2015/10/31/the-trust-machine

Babinet G., La technologie est-elle « neutre » ?, 12 nov. 2019, https://www.lesechos.fr/idees-debats/cercle/la-technologie-est-elle-neutre-1147002 (consulté le 31/05/2020)

Biseul X., « *Blockchain* as a Service : quelle solution choisir pour se lancer ? », JDN, 14 mars 2018, https://www.journaldunet.com/solutions/cloud-computing/1206955-*blockchain*-as-a-service-quelle-solution-choisir/

Castelon E., « Le banquier, l'anarchiste et le bitcoin », Le Monde diplomatique, mars 2016

Ching J., Is *Blockchain* Evidence Inadmissible Hearsay? », janv. 2016, http://www.law.com/sites/jamesching/2016/01/07/is-*blockchain*-evidence-inadmissible-hearsay/

Colin N., « Crypto-monnaies, un peu de cohérence », L'Obs, 25 janv. 2018 https://www.nouvelobs.com/chroniques/20180126.OBS1279/crypto-monnaies-un-peu-de-coherence.html

Douville T., Verbiest T., « *Blockchain* et tiers de confiance », Planet-Fintech, mai 2018, https://www.planet-fintech.com/*Blockchain*-et-tiers-de-confiance%C2%A0_a819.html

Eschapasse B., « Attention aux voleurs de crypto-monnaies », Le Point, 16 dec. 2017, http://www.lepoint.fr/economie/attention-aux-voleurs-de-crypto-monnaies-16-12-2017-2180508_28.php#

Raymond G., « Première vente immobilière via *blockchain* en France », Capital, 24 juin 2019, https://www.capital.fr/immobilier/premiere-vente-immobiliere-via-*blockchain*-en-france-1342764

Xia S., « China's Internet Courts are Spreading; Online Dispute Resolution is Working », China Law Blog, 23 dec. 2018, https://www.chinalawblog.com/2018/12/chinas-internet-courts-are-spreading-online-dispute-resolution-is-working.html

Avis / rapports

AMF, Document de consultation sur les *Initial Coin Offerings* (ICOs), le 26/10/2017 ; AMF, Synthèse des réponses à la consultation publique portant sur les *Initial Coin Offerings* (ICO) et point d'étape sur le programme « UNICORN », 22 fevr. 2018

Assemblée Nationale, Commission de réflexion et de propositions sur le droit et les libertés à l'âge numérique, Numérique et libertés : Un nouvel âge démocratique, rapport n°3119, président par C. Paul et C. Féral-Schuhl, oct. 2015

Assemblée Nationale, Rapport d'information, par la commission des finances, de l'économie générale et du contrôle budgétaire en conclusion des travaux d'une mission d'information relative aux monnaies virtuelle, présenté par Eric Woerth et Pierre Person, avant-propos du Président, 30 janv. 2019

Assemblée Nationale, Rapport d'information n°1501, par la mission d'information commune sur les chaînes de blocs (*blockchains*), présenté par L. De La Raudière et J.-M. Mis, 12 déc. 2018

Banque de France, La monnaie digitiale de banque central, janv. 2020

BCE, Virtual currency schemes, oct. 2012

Cambridge Centre for Alternative Finance, 2nd Global Enterprise Blockchain Benchmarking Study, ss. dir. M. Rauchs, A. Blandin, K. Bear, S. McKean, 2019

Cambridge Centre for Alternative Finance, University of Cambridge Judge Business School, Global blockchain benchmarking study, ss. dir. G. Hileman, M. Rauchs, 2017

Club des Juristes, Rapport sur l'arbitrage en ligne, Commission ad hoc, Groupe de travail présidé par T. Clay, avr. 2019

CNIL, Premiers éléments d'analyse de la CNIL. Blockchain, 24 sept. 2018

Committee on Payments and Market Infrastructures, Markets Committee, Central bank digital currencies, mars 2018

Conseil d'État, Étude annuelle 2017, Puissance publique et plateformes numériques : accompagner l' « ubérisation », le 13 juill. 2017

Conseil de l'Europe, CEPEJ, Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement, Adoptée lors de la 31e réunion plénière de la CEPEJ, 3-4 déc. 2018

Cour de cassation, Rapport annuel, La preuve, 2012

Cour de cassation, Rapport La vérité, 2004

CSPLA, Rapport de la mission sur l'état des lieux de la *blockchain* et ses effets potentiels pour la propriété littéraire et artistique, janv. 2018

Direction Générale de la Santé, M.-D. Furet, Rapport sur l'indépendance et la valorisation de l'expertise venant à l'appui des décisions en santé publique, juin 2008

GIP Droit et Justice, « La technologie de l'écrit électronique : synthèse et évaluation critique », janv. 2001

Groupe de travail « article 29 » sur la protection des données, Avis 05/2014 sur les Techniques d'anonymisation, adopté le 10 avr. 2014

EU Blockchain Observatory and Forum, Blockchain and digital identity, le 2 mai 2019

EU Blockchain Observatory and Forum, Blockchain and the GDPR, oct. 2018

EU Blockchain Observatory and Forum, Blockchain innovation in Europe, 27 juill. 2018

EU Blockchain Observatory and Forum, Legal and regulatory framework of blockchain and smart contracts, le 28 sept. 2019

EU Blockchain Observatory and Forum, Scalability interoperability and sustainability of blockchain, le 6 mars 2019

European Central Bank, exploring anonymity in central bank digital currencies, in Focus, Issues n°4, dec. 2019

European Commission, Evaluation roadmap, Report on the Application of the eIDAS Regulation, Ref. Ares(2019)6019401, 27 sept. 2019

France Stratégie, Rapport, Les enjeux des *blockchains*, Présidente du groupe de travail Joëlle Toledano, juin 2018

Government Office for Science, Distributed Ledger Technology: Beyond Block Chain, A Report by the UK Government Chief Scientific Adviser, 2016

Institut Sapiens, Y. de Monbynes et G. Grandval, Rapport Bitcoin totem et tabou. Que présage l'essor des crypto-monnaies ?, févr. 2018

Ministre de l'Économie et des Finances, Les crypto-monnaies, Rapport au Ministre de l'Économie et des Finances Jean-Pierre Landau avec la collaboration d'Alban Genais, juill. 2018

Ministère de l'Économie et des Finances, Rapport J.-P.Landau avec la collaboration d'A. Genais, Les crypto-monnaies, 4 juill. 2018

OPECST, Rapport (par V. Faure-Muntian, C. de Ganay, R. Le Gleut) Les enjeux technologiques des *blockchains* (chaînes de blocs), 20 juin 2018

Queen Mary University of London, School of International Arbitration, International Arbitration Survey: Improvements and Innovations in International Arbitration, White and Case, 2015

Rapport « Amélioration et simplification de la procédure civile », *in* J.-F. Beynel et a. (dir.), Rapport sur les « Chantiers de la Justice », Documentation française, 2018.

Rapport d'information n°495 au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale, par la mission d'information sur le redressement de la justice, de M. P. Bas, E. Benbassa, J. Bigot, F.-N. Buffet, C. Cukierman, J. Mézard et F. Zocchetto, déposé le 4 avril 2017

Rapport de la Commission sur la libération de la croissance française, ss. dir. J. Attali, XO Editions, La Documentation Française, 2008

Rapport de la mission de réflexion confiée par Madame Christiane Taubira, garde des Sceaux, à l'Institut des hautes études sur la justice, sur l'évolution de l'office du juge et son périmètre d'intervention, « La prudence et l'autorité l'office du juge au XXIe siècle », mai 2013

Rapport de la mission interministérielle sur les verrous technologiques des *blockchains*, Task Force *Blockchain*, 10 fevr. 2020

Rapport Giulano-Lagarde sur la convention de Rome relative à la loi applicable aux obligations contractuelles, JO des Communautés européennes, n°C282/1

Rapport l'authenticité. Droit, histoire, philosophie, ss. dir. L. Aynès, La documentation française, 2e ed., janv. 2014

Rapport sur les obstacles à l'expansion économique, ss. dir. J. Rueff et L. Armand, présenté par le comité institué par le décret n°59-1284 du 13 nov. 1959

Rapport sur les professions du droit, ss. dir. J.-M. Darrois, mars 2009

Sénat, Commission des finances, Rapport d'information fait au nom de la commission des finances sur les enjeux liés au développement du bitcoin et des autres monnaies virtuelles, P.

Marini, F. Marc, « La régulation a l'épreuve de l'innovation : les pouvoirs publics face au developpement des monnaies virtuelles », coll. Les rapports du Sénat, juill. 2014

Tracfin, Rapport « L'encadrement des monnaies virtuelles », Recommandations visant à prévenir leurs usages a des fins frauduleuses ou de blanchiment, Groupe de travail « monnaies virtuelles », juin 2014

Tracfin, Rapport annuel d'activité 2011, 22 août 2012

Tracfin, Tendances et analyse des risques de blanchiment de capitaux et de financement du terrorisme 2017-2018, nov. 2018

Tracfin, Tendances et analyse des risques de blanchiment de capitaux et de financement du terrorisme 2018-2019, dec. 2019

World Economic Forum, Insight Report, Central Bank Digital Currency Policy-Maker Toolkit, Centre for the Fourth Industrial Revolution, janv. 2020

Jurisprudences

- Nationales

T. com. Nanterre, 26 février 2020, n°2018F00466, BitSpread c/ Paymium : com. G. Marraud des Grottes, RLDI n°168, p.49-51 ; com. L. Costes, RLDI n°168, p.40 ; com. M. Julienne, JCP E n°19, p.41-44 ; N. Mathey, LEDB avr. 2020, p.1

TGI Paris, Référés, 20 juin 2017, n°17/55291

TGI de Grasse, Commission d'indemnisation des victimes d'infractions, 26 septembre 2016, n°15/02876

CA Paris, 1, 1, 26 août 2011, n°1115269
T. com. Créteil, 31 août 2011, n°2011R00323, SAS Macaraja c. Credit
TC Créteil, 2ème ch., 6 déc. 2011, n°2011F00771
CA Paris, 26 septembre 2013, n°12/00161 : JurisData n°2013-024887 ; RDBF 2014, comm. 3, obs. F.-J. Crédot et T. Samin ; JCP E 2014, 1091, note Th. Bonneau

- Européenne

CJUE 22 octobre 2015, aff. C-264/14 Skatteverket c. David Hedqvist : note J. Huet, RDC 2017, n°113, p.54 ; note R. Vabres RISF 2016 n°1, p.170 ; adde : Th. Bonneau, « Analyse critique de la contribution de la CJUE à l'ascension juridique du bitcoin », *in* Liber amicorum Blanche Sousi, L'Europe bancaire, financière et monétaire, Rev. Banque 2016

- Etrangère

Hangzhou Internet Court, Province of Zhejiang People's Republic of China, Case No. 055078 (2018) Zhe 0192 No. 81 Huatai Yimei/Daotong, June 27, 2018

Thèses et mémoire

Azzi T., *Recherche sur la loi applicable aux droits voisins du droit d'auteur en droit international privé*, thèse ss. dir. H. Gaudemet-Tallon, Paris 2, LGDJ, 2005

Bergeaud A., *Le droit à la preuve*, thèse ss. dir. J.-C. Saint-Pau, Bordeaux, LGDJ, 2010

Bergson E., *Essai sur les données immédiates de la conscience*, thèse, Félix Alcan, coll. Bibliothèque de philosophie contemporaine, 1889

Boursier M.-E., *Le principe de loyauté en droit processuel*, thèse ss. dir. S. Guinchard, Paris 2, Dalloz coll. Nouvelle Bibliothèque des thèses, 2013

Caire A.-B., *Relecture du droit des présomptions à la lumière du droit européen des droits de l'homme*, Pedone, coll. publications de l'Institut International des Droits de l'Homme, thèse ss. dir. J.-P. Marguénaud, 2012

Catala P., *La nature juridique du paiement*, thèse, Paris, 1961

Chambost A.-S., *Proudhon et la norme, pensée juridique d'un anarchiste*, thèse, Lyon 3, Pur, 2004

Clément Fontaine M., *Les œuvres libres*, thèse ss dir. M. Vivant, Montpellier, 2006

Cocural M., *Étude théorique et jurisprudentielle des conventions des parties en matière de preuve, en droit civil français*, thèse Toulouse, 1933

Dalbignat-Deharo G., *Vérité scientifique et vérité judiciaire en droit privé*, thèse ss. dir. L. Cadiet, Paris 1, LGDJ, Bibliothèque de l'institut André Tunc, 2002

Dauriac I., *La signature*, thèse ss. dir. M. Gobert, Paris 2, 1997

Demarchi J.-R., *La preuve scientifique et le procès pénal*, thèse ss. dir. C. Ambroise-Castérot, Nice, 2010

Fongaro E., *La loi applicable à la preuve en droit international privé*, LGDJ, thèse ss. dir. B. Beignier, 2004

Foulquier C., *La preuve et la justice administrative française*, thèse ss. dir. Jean-Arnaud Mazères, Toulouse 1, 2009

Khalil L. J., Signature électronique : Le cadre juridique d'une Autorité de Certification, thèse ss. dir. X. Linant de Bellefonds, UPEC, 2002

Lagarde X., *Réflexion critique sur le droit de la preuve*, thèse ss. dir. J. Ghestin, Paris 1, LGDJ, coll. Bibliothèque de droit privé, Tome 239, 1994, n°160, p.272

Le Balle R., *Des conventions sur les procédés de preuve en droit civil*, thèse Paris, 1923

Legeais R., *Les règles de preuve en droit civil. Permanences et transformations*, thèse ss. dir . R. Savatier, Poitier, LGDJ, 1955

Mazeaud H., *La conception jurisprudentielle du commencement de preuve par écrit de l'article 1347 du Code civil*, thèse, Lyon, 1921

Merkle R. C., *Secrecy, authentication, and public-key systems*, these, Université de Stanford, 1979

Normand J., *Le juge et le litige*, thèse, Paris, coll. Bibliothèque de droit privé, 1965

Prybis-Gavalda N., *L'obligation de donner*, thèse ss. dir. M. Cabrillac, Montpellier, 1997

Sescioréano G.-M., *Des conventions sur la preuve de la libération du débiteur*, thèse, Paris, 1920

Teissier A., *Le secret professionnel du banquier*, thèse, Aix-en-provence, 1998

Wintgen R., *Étude critique de la notion d'opposabilité. Les effets du contrat à l'égard des tiers en droit français et allemand*, thèse ss. dir. J. Ghestin, Paris 1, 2002, LGDJ, coll. Bibliothèque de droit privé, 2004

Zhang C., *Faut-il réguler la blockchain ?*, mémoire ss. dir. P. Sirinelli, Paris, 2017

Zimmer S., *Mécanismes cryptographiques pour la génération de clefs et l'authentification*, thèse ss. dir. D. Pointcheval, École polytechnique, 2008

Colloques / évenements

Colloque « *Blockchains* et Crypto-monnaies : hors-la-loi ? », intervention table ronde n°2 « *blockchain* et droit : responsabilité, preuve et données personnelles », Université de Nanterre, 23 mars 2018

Colloque « La circulation de l'information dans la *blockchain* : enjeux pour le droit international privé », organisé par l'Association « Lex », intervention J.-S. Bergé, 28 fév. 2019

Colloque « La déontologie des magistrats de l'ordre judiciaire : la déclaration d'intérêt », Allocution d'ouverture de J.-M. Marin, 30 juin 2017

Conférence « Computational law and *blockchain* festival (CL+B Fest) », organisé par Stanford CodeX *Blockchain* Group, modération de l'atelier convention de preuve, 2 Mars 2019

Conférence « Computational law and *blockchain* festival (CL+B Fest) », organisé par Stanford CodeX *Blockchain* Group, intervention « preuve et *blockchain* », 16 Mars 2018

Conférence « Les mardis de l'espace des sciences », organisée avec l'Université de Rennes 2-CREA, intervention de J.-P.Delayahe « Les mathématiques et la cryptographie réinventent la monnaie : le bitcoin », 14 oct. 2014

Conférence, *Blockchain* Protocol Analysis and Security Engineering 2018, intervention de P.Wuille « Schnorr signatures for Bitcoin: challenges and opportunities », Université de Stanford, 24-26 janv. 2018

Conférence Paris P2P Festival, intervention de A. Takkal Bataille, J. Favier, « Bitcoin, clé privée et clé de voûte du P2P », 9 janv. 2020

Conférence Scaling Bitcoin, Synthèse partie 2 : scalabilité, Université de Stanford, 4 et 5 nov. 2017

Conférence Scaling Bitcoin, Université de Stanford, 15 janv. 2018

Conférence Scaling Bitcoin, Université Keio de Tokyo, 6-7 oct. 2018

Conférences Woman in *blockchain*, « La recherche académique dans l'écosystème *Blockchain* : champ d'action et perspectives », organisation et modération, 8 janv. 2019

Cour de cassation, Colloque « L'expertise : entre neutralité et partis-pris », 16 mars 2018

Cour de cassation, Cycle de conférences « Entre mystère et fantasme : quel avenir pour les *blockchains* ? », ss. dir. scientifique de M. Mekki, N. Blanc, B. Haftel

European Commission, EU Blockchain observatory and Forum, atelier « digital assets », le 24 mai 2019

OEB, conférence « Patenting blockchain », 4 dec. 2018

Séminaire de « Cryptofinance » organisé par R. Pérez-Marco et C. Grunspan, intervention de Y. Seurin « Les signatures de Schnorr et de leurs applications dans Bitcoin », 14 mars 2018

Sémainaire de la « Cryptofinance » organisé par Pérez-Marco et C. Grunspan, intervention de G. Fuchsbauer « *Strong anonymity in cryptocurrencies* », le 8 juin 2017

Séminaire IRT SystemX, D. Augot, fonction de hachage et blockchain, 22 nov. 2017

Table ronde « L'officier public ministériel est-il soluble dans la blockchain ? », organisée par Le Club du Droit & le Conseil supérieur du Notariat, le 14 mai 2019

Workshop Blockchain, organisé par la Coalition of Automated Legal Applications (Coala), P. De Filippi, European University Institute, Robert Schuman Centre for Advanced Studies and the Law Department, Florence, 30 nov. 2017 et 1er dec. 2017

Mooc

Campbell R. Harvey, Cryptotransactions, Duke University Courses, janv. 2019

Bonneau J., Lecture 5 – Bitcoin Mining, Princeton's Bitcoin Mooc, Princeton University

Delahaye J.-P., Du bitcoin à la *blockchain* n°1, Mooc sur l'Informatique et la Création Numérique, Inria Learning Lab, mai 2017

Felten E., Lecture 1 – Introduction to crypto and cryptocurrencies, Pinceton's Bitcoin Mooc, Princeton University

Narayanan A., Lecture 6 – Bitcoin and anonimity, Princeton's Bitcoin Mooc, Princeton University

Interventions scientifiques

Consultation pour la rédaction de l'amendement n°1317 sur la « preuve *blockchain* » au projet de loi sur la croissance et la transformation des sociétés n°1088 dit « PACTE »

Membre du jury du LAB de l'Ecole du Barreau de Paris (EFB), ateliers *blockchain*

Sites Internet

https://bitcoin.fr

https://bitcoin.org

https://bitconseil.fr

https://bitnodes.earn.com

https://*blockchain*france.net

https://blockstream.com

http://cjc.ny.gov/

https://culturemath.ens.fr

https://cyber.stanford.edu

https://eth.wiki/en/white-Paper

https://Ethereum.org

http://evidence.netcourt.gov.cn

https://gsell.tech

https://hbr.org

https://lejournal.cnrs.fr

https://libra.org

https://nakamotoinstitute.org

https://opensource.org/licenses/MIT

https://proofofexistence.com

https://stanford-jblp.pubpub.org/

https://theodi.org

https://www.afnor.org/

http://www.apache.org

http://www.assemblee-nationale.fr

https://www.cencenelec.eu

https://www.cnil.fr

https://www.coinhouse.com

https://www.college-de-france.fr

https://www.conseil-superieur-magistrature.fr

https://www.consilium.europa.eu

https://www.courdecassation.fr

https://www.cours-appel.justice.fr

https://www.economist.com

http://www.enm.justice.fr

ttps://www.entreprises.gouv.fr

https://www.espace-sciences.org

https://www.Ethereum-france.com

https://www.europol.europa.eu

https://www.gnu.org

https://www.goquorum.com

http://www.hashcash.org

https://www.hyperledger.org

https://www.irs.gov

https://www.iso.org

https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance

https://www.mekki.fr/publications/articles

https://www.nextinpact.com

https://www.numerama.com

http://www.oecd.org

https://www.parity.io

https://www.r3.com

http://www.scilogs.fr

https://www.ssi.gouv.fr

https://www.strategie.gouv.fr

INDEX

(Les references renvoient aux pages)

A

B

C

D

E

F

H

J

L

M

O

P

R

S

T

U

V

Z

TABLE DES MATIERES

Le droit de la preuve à l'aune de la *blockchain*

Les preuves *blockchains*, preuves cryptographiques et distribuées d'un nouveau genre, émergent dans le paysage du droit de la preuve. Si le droit commun a la faculté de faire correspondre ses règles aux procédés complexes et iconoclastes des preuves *blockchains* et que le droit spécial les traite partiellement pour certains titres financiers, des frictions et des incomplétudes subsistent. Afin de résoudre ces difficultés, révéler la vérité cryptographique fournie par ces preuves et offrir plus de sécurité dans leur usage, un socle de grands principes internationaux relatifs aux preuves *blockchains* et des mécanismes de *soft law* seraient bienvenus. Dans le même temps, l'appréhension juridictionnelle de ce nouvel arsenal probatoire est prudente et des attentes importantes sont portées quant au travail des auxiliaires de justice. Cette appréhension complexe est traduite par une adhésion et une reconnaissance lentes de ces preuves par les juges. Des propositions de renforcement de l'office et de l'indépendance des juges sont donc des pistes à examiner.

Mots clés : droit de la preuve, preuves *blockchains*, pair-à-pair, distribué, open source, vérité cryptographique, signature *blockchain*, horodatage *blockchain*, empreinte *blockchain*, juridictions, auxiliaires de justice

---

Law of evidence in light of blockchain

A new kind of cryptographic and distributed evidences is emerging within the framework of the law of evidence: blockchain evidences. The rules derived from ordinary law may easily apply to the complex and iconoclastic mechanisms of blockchain evidences. More than that, specific statutes already expressly take into account and recognize blockchain evidences, specifically regarding certain financial securities. However, sticking points and incompleteness remain. In order to reveal the cryptographic truth provided by these evidences, to offer more security while using them, and to serve the courts usefully, the development and implementation of major international principles relating to blockchain evidences, and soft law mechanisms, would allow this new kind of evidences to expand. At the same time, the jurisdictional approach to these evidences is cautious and there are high expectations on the work of court officers. The technical complexity of these evidences may explain why the judges are struggling to recognize and accept them. Therefore, courts' jurisdiction and independence should be strengthened: proposals on this topic need to be discussed.

Keywords: law of evidence, blockchain evidences, peer-to-peer, distributed, open source, cryptographic truth, blockchain signature, blockchain timestamp, blockchain fingerprint, courts, court officers

Unité de recherche/Research unit : Centre d'études et de recherches administratives, politiques et sociales (CERAPS), UMR 8026-CNRS, 1 Place Déliot, 59000 Lille, https://ceraps.univ-lille.fr/

Ecole doctorale/Doctoral school : Ecole doctorale des sciences juridiques, politiques et de gestion n°74, 1 place Déliot, 59000 Lille, http://edoctorale74.univ-lille2.fr/

Université/University : Université de Lille, 42 rue Paul Duez, 59000 Lille, https://www.univ-lille.fr/