Reliable Platform Using Distributed Ledger Technology For IoT-based Industrial Environment

Houssein Hellani

THESE de Doctorat

Pour obtenir le grade de Docteur délivré par :

Université De Pau Et Des Pays De L'Adour

Spécialité: Informatique

Présentée et soutenue publiquement par :

Houssein HELLANI

Date: 13 July 2022

Reliable Platform Using Distributed Ledger Technology For IoT-based industrial Environment

Membre du Jury :

Guido PERBOLI Professeur, ÉCOLE POLYTECHNIQUE DE TURIN (ITALIE)	**Rapporteur**
Raoudha BEN DJEMAA Maître de Conférences, HDR, UNIVERSITÉ DE SOUSSE (TUNISIE)	**Rapporteur**
Khalil DRIRA Directeur de Recherche CNRS, Laboratoire d'Analyse et d'Architecture des Systèmes	**Examinateur**
Marco AIELLO Professeur, UNIVERSITÉ DE STUTTGART (ALLEMAGNE)	**Examinateur**
Nawal GUERMOUCHE Maître de Conférences, INST. NATIONAL DES SCIENCES APPLIQUÉES DE TOULOUSE	**Examinateur**
Ernesto EXPOSITO Professeur des Universités, UNIVERSITÉ DE PAU ET DES PAYS DE L'ADOUR	**Directeur de thèse**
Layth SLIMAN Maître de Conférences, HDR, ECOLE FRANCAISE D'ELECTRONIQUE ET D'INFORMATIQUE	**Co-directeur de thèse**

Acknowledgements

Throughout the writing of this dissertation, I have received a great deal of support and assistance. In the first place, my thanks go to God for supporting me all the time, giving me the strength and courage to accomplish this work, and leading me to success.

I would like to thank my supervisor, Professor Ernesto Exposito, whose expertise was invaluable in formulating the research questions and methodology. Your insightful feedback pushed me to sharpen my thinking and brought my work to a higher level.

I am extremely grateful to my supervisor at EFREI university, Professor Layth Sliman, for inspiring my interest in developing innovative technologies. You provided me -all the time- with fruitful and broad advice together with the right tools to choose the right direction and complete my dissertation successfully.

I would particularly like to single out my tutor Professor Abed Ellatif Samhat. I want to thank you for your patient support and all of the opportunities I was given to further my research.

In addition, I would like to thank my family for their continued support and love. You are always there for me. Finally, I could not have completed this dissertation without the support of my friends, who provided stimulating discussions and a happy time, indirectly contributing to the progress of my research.

Abstract

Boosted by modern technologies such as the Internet of Things (IoT), artificial intelligence (AI), Cloud, and so on, an innovative shift in economic models towards collaborative and dynamically constructed productions processes is being shaped worldwide, including in the context of supply chains. Nonetheless, current systems are incapable of managing/analyzing the massive amounts of incoming data as proposed in centralized situations. Consequently, the current network infrastructure cannot fully harness the Internet of Things' potential, resulting in data loss. Besides, the proliferation of IoT devices in the market increases the need for platforms that support data transparency to enforce full trust in information sharing and enable collaboration among the various partners. Existing supply chains have several drawbacks as a result of independent partners' lack of cooperation and mistrust. Blockchain, the distributed ledger technology (DLT), is a promising solution for the new technological business challenges. Based on a cryptographically decentralized platform, it ensures business applications' productivity enhancement and the removal of many limitations such as a lack of trust and data transparency. However, with the massive influx of IoT data, Blockchain faces numerous major challenges that prevent it from integrating into the supply chain. Directed ayclic graph (DAG) DLT, as an alternative to Blockchain, can address all of the drawbacks of Blockchain. Still, it has additional constraints such as smart contract limitations and a lack of task allocation mechanism. To that end, the purpose of this thesis is to define a new supply chain framework that considers the proliferation of IoT and the needs of new collaboration models through the integration of DLT technologies. We propose combining Blockchain and DAG into a single platform to respond to new supply chain requirements while bridging the gaps caused by these DLTs' drawbacks. Furthermore, we propose a distributed algorithm that runs on the DAG side to reallocate the numerous tasks among the various IoT devices, resulting in a high-performing system. Moreover, the DLT transparency feature shows unease with data privacy and supply chain control. Therefore, we investigate and analyse the DLT transparency impacts by shedding light on the existing supply chain projects. The study comes up with several mechanisms that could be used to achieve the supply chain goal and conclude that our DLT proposal has the suitable infrastructure for the required enhancements.

Table of contents

List of figures

List of tables

Chapter 1

Introduction

Today's modern business models have paved the way in production and successfully made progress using technological advances [1] such as the internet of things (IoT), cloud computing, artificial intelligence (AI), etc. Applying these technologies in a critical business system like the industrial supply chain is vital to overall improvements and human business advancements. As a result, depending on these current sophisticated technologies enhances output, lowers costs, collects vast amounts of data, and promotes product variety and innovation throughout the supply chain's geographic locations. Distinctly, IoT technology is involved in all business sectors and has a substantial influence on the advancement of corporate output. It converts the physical world into a massive information system by empowering any "Thing" to connect and communicate. The proliferation of these devices transforms human life and contributes to vast economic benefits. IoT technology can deliver the collected records from all the networks to improve productivity and traceability of the supply chain. Hence, recently, the IoT has become an increasingly indispensable partner in the supply chain processes [2, 3].

Although IoT technology ameliorates the production progress of any supply chain, helping the fabrication part and providing high control, it charges servers and peripheral devices with high data volume [4]. According to the Cisco report, [5], the increasing number and diversity of IoT devices will increase supply chain complexities [6–8]. Unfortunately, the present network infrastructure cannot fully harness the Internet of Things' potential, resulting in some data loss. Current systems cannot manage/analyze vast incoming data as envisioned under centralized settings [9]. As a result, further data charges will encircle the supply chain where the exchange of this data leads, on the one hand, to problems with data consistency and platform scalability. On the other hand, intermittent data affects collaboration, which is the engine of a successful supply chain. Hence, this data structure undermines partner and consumer trust.

In fact, effective collaboration among the different stakeholders requires a supply chain

with a high degree of transparency [10]. Data transparency enables the different participants in the supply chain to have complete visibility on data, services, and products being introduced and exchanged. Furthermore, it enriches the clients with more detailed information regarding the goods, including quality of service, manufacturing source, safety, conformity documents, etc. One of the solution to respond to the business requirements is to use cloud based applications. However, the cloud does not address the IoT impairment and does not promote trust and collaboration among stakeholders, as required by the supply chain.

A recent platform called distributed ledger technology (DLT) is introduced to decentralize applications and remove third-party services. Blockchain [11] is the first DLT platform that underlies the first cryptocurrency known as "Bitcoin." Rapidly, the Blockchain is developed to underly different dApps (decentralized applications) to replace the traditional centralized systems. Blockchain becomes of great importance as it turns into a center of interest in many business sectors [12] since it mitigates the issue of the massive IoT data. It assures to business applications the productivity enhancement and the overcoming of many limitations such as lack of trust and data transparency, based on great added values of Blockchain platform features [13]. The main characteristics of Blockchain that benefit the supply chain are:

1. Decentralized technology: Blockchain is a distributed ledger among its nodes. Thereby, no governing authority or single party takes charge of the process.
2. Consensus-based: the consensus manages the exchanged messages and decisions of every single transaction to provide network consistency and maintain the whole system.
3. Immutability: once a transaction is recorded in the ledger, there is no way to alter or remove it.
4. Secure: the Blockchain data is cryptographically hashed, which prohibits frauds and hides the original nature of the data in the network.
5. Transparent Ledger: Every transaction in the ledger is time-stamped and accessible by all the participants' nodes, which facilitates traceability.
6. Automation: The smart contact introduced in Blockhain enables the participants to create and deploy particular transactions to be executed under specific conditions.

These features are considered attractive to businesses because they respond to market expectations and their technical requests. Data records immutability encourages companies to store vital information on the Blockchain platform, such as essential documents, cryptocurrencies, contracts, or other valuable digital assets. The data transparency feature of

Blockchain becomes the spotlight of many trading companies to enforce trust among supply chain partners and their end-users/clients. Moreover, in a trading environment, Blockchain aids the participants, including the clients, in tracking their goods/services using their private keys. So, the decentralized system provides people with control and clear view over their assets.

1.1 Thesis Objective

The main goal of this thesis is to define a new supply chain framework that takes into account the proliferation of IoT as well as the requirements of the new collaboration models via the integration of DLT technologies. Hence, the key sub-objectives are:

- **Objective 1:** Humiliate all the obstacles of the Blockchain that hinder the integration of the supply chain. This is done through a profound study showing the benefit of using Blockchain to address the supply chain challenges giving attention to IoT and data transparency in the first place.
- **Objective 2:** Investigate the different DLT solutions, including the interoperable DLT homogenous/heterogeneous platforms that can overcome the existing Blockchain-based supply chains limitations, and best fit the business requirements.
- **Objective 3:** Analyse the overall outcome data, including existing DLTs and DLT-based supply chains. Thereafter, set the ideal requirements/characteristics of the typical platform as a preliminary step toward planning and proposing the appropriate platform solution.

Moreover, the integration of the IoT-based supply chain with Blockchain becomes of great importance for overall improvements in general and for transparency purposes in particular. However, the use of Blockchain in current supply chain systems encounters several technical limitations, as detailed in the problem statement section.

1.2 Problem Statement

Although the integration of both Blockchain and IoT technologies brings many benefits to the supply chain, it has some limitations [14]. Blockchains, in general, are computationally expensive and involve high bandwidth overhead and delays, which are unsuitable for most

IoT devices [15]. Each participant node has to store the whole ledger in order to validate the transactions. Most IoT devices have no storage capability, and they are distributed in different geolocations with inadequate network coverage. Besides, the Blockchain structure that opens one block at a time and the minimal block capacity hinder the accomplishment of processing millions of transactions in a real-time fashion. The scalability is mainly affected by the linear block structure and consensus algorithms. Additionally, the proliferation of IoT devices in the market requires an advanced Blockchain system to tackle the current performance and ledger volume issues.

These limitations are considered as an obstruction of Blockchain utilization in IoT-based industrial context [16]. Currently, the researchers direct their focus towards facilitating the Blockchain integration within the industry through the fourth upcoming version. Most of the researches work either on storage optimizing or Blockchain redesigning. The latter focuses on improving the consensus algorithm, which is the core engine of the Blockchain. A typical consensus algorithm increases the speed of the Transactions' validation and speeds up their storage in the current open block. Indeed, such storage and computing resolutions partially improve the Blockchain performance. In fact, they do not solve the drawbacks permanently due to the extremely high number of incoming transactions which leads to a decrease in performance and an increase in latency and size.

Fortunately, another DLT based on the DAG (Directed Acyclic Graph) is introduced to tackle the Blockchain drawbacks [17] . The DAG technology is found to treat IoT's scalability issue, enable micropayments, reduce ledger size, and resist quantum computing algorithms. Contrarily to Blockchain, the DAG's performance increases when the number of transactions is abundant. It consists of transactions only, where neither block nor chain exists. The DAG-based architecture enables processing large transactions simultaneously, which nominates it as a scalable DLT system [18]. However, DAG technology experiences some limitations as it does not perfectly applies smart contract [19] the same way Blockchain does. Also, it requires attaining certain transaction numbers to be secure and fully decentralized. Besides, we observe another limitation to DAG that hinders the overall system's performance. The IoT devices are distinguished by their resource capacities, and thereby the weak nodes cannot directly participate in the DLT network. Instead, those weak nodes seek help from the other highly resourced nodes to issue their transactions. Currently, no efficient algorithm organizes the huge weak nodes' requests. Hence, to largely allocate the full nodes' resources, an efficient mechanism within the DAG platform must replace the existing manual one. To this end, we conclude that no one DLT is considered a typical solution for the supply chain if

used solely. To resume, below are the main drawbacks of the current DLT solutions for the IoT-based supply chains:

- Current supply chain systems lack trust, transparency, and efficient collaboration
- Blockchain has many drawbacks that hinder its integration with the supply chain:
  - Block structure
  - Mining and competition
  - High transaction fees
  - Scalability issue
  - Uncontrolled data transparency
- The existing Blockchain-based solutions do not solve all the above highlighted aspects
- DAG, the alternative to Blockchain, has other kind of drawbacks:
  - Smart contract limitation
  - Manual resource allocation

1.3 Research Proposal

To respond to the aforementioned supply chain challenges and limitations during its integration with Blockchain, we have developed a research methodology illustrating the thesis structure, as depicted in figure 1.1. The suggested solution is a set of the following actions:

- State of the art sets a profound revision of the related works on the existing supply chains and the Blockchain-based supply chains. The studies indicate that Blockchain features represent the best solutions for the supply chain but it is not ready for this mission as it has crucial technical limitations.
- We focus on the Blockchain limitations and show how they can be solved. The study demonstrates that the issue lies at the core of the Blockchain, despite improvements on several layers. we focus our research on a sophisticated alternative Blockchain platform that offers equivalent Blockchain added values. As a result, the study concludes that the alternative DLT meets the requirements better, although it has another type of constraint.

- We discovered that the technical details of two heterogeneous DLTs are complimentary in terms of features and downsides after analyzing their technical details. We then identified the need to provide a solution for a typical DLT platform for an IoT-based environment by combining these two DLTs in a single platform with a suitable architecture to eliminate their constraints. The suggested platform is used for the first portion of the thesis research project.
- In a second stage of our study, we aim to improve the DAG mechanism by resolving dispersed IoT tasks across nodes and providing load balancing. In this way, we enhance the maximum proliferation of IoT in the platform.
- In the third stage, we study the new data transparency feature that DLT brings to the supply chain in a collaborative environment in order to ensure confidentiality of operations and control access to sensitive data.

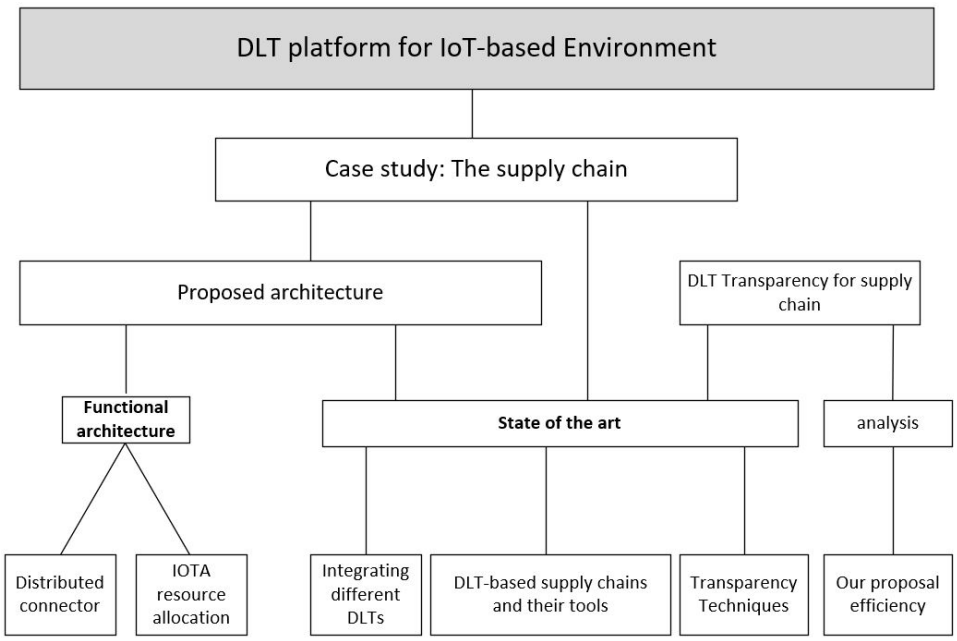


Fig. 1.1 Thesis structure

1.4 Thesis Contributions and Organization

This thesis consists of developing a typical DLT platform for IoT-based collaborative environment while ensuring scalability, privacy and high transparency. In this context, we mainly focus on supply chain system as a case study.

The contributions of this thesis are illustrated in figure 1.1 and given as follows:

1. We have conducted a thorough study to show necessity of Blockchain in the supply chain and highlight the Blockchain challenges. The study is done on three levels: DLT, supply chain, and DLT interconnection. On the DLT level, we discussed Blockchain and DAG technologies, as well as the differences between their ledgers structures. On the supply chain level, we reviewed existing Blockchain-based supply chain projects, illustrated/investigated their contributions and limitations, and demonstrated their comprehensive technical sides. On the DLT interconnection level, we evaluated and classified the various DLT interoperability types and proposed a new heterogeneous type that fulfills our DLT interconnection idea.

2. New DLT platform suitable for IoT-based system: We proposed a DLT platform to tackle the issues behind the massive IoT devices in a supply chain system. The proposed platform is a combination of Blockchain with DAG, in which the latter represents the front-end application, where Blockchain represents the back-end platform and a connector part intermediates both DLT technologies.

3. Distributed connector: To provide the connectivity between the different parties of the platform we built a distributed connector software running on several DAG nodes. The connector's role is to translate the transactions types from Tangle into Blockchain and vice versa. The connector implementation is based on the zeroMQ (zero message queuing) and Ethereum web3 protocols.

4. DAG resource allocation scheme: We introduced an efficient mechanism to distribute the tasks fairly among full nodes and hence achieve load balancing. To do so, we considered the task allocation between the nodes by introducing an enhanced resource allocation scheme based on the weight least connection algorithm (WLC).

5. Investigation of DLT transparency for the supply chain: We elaborated a state of art on DLT transparency for the supply chain. We highlighted the supply chain transparency requirements and challenges. We showed how different projects and applications tackled data transparency issues by involving the Blockchain in their core platform in different manners. We concluded that further enhancements are needed to set a

balance between data transparency and process opacity required by different partners to assure the confidentiality of their processes and to control access to sensitive data. In addition, our proposed architecture has the suitable infrastructure for the required enhancements.

The rest of this thesis is organized as follows:

- Chapter 2:
  This chapter provides an overview of Blockchain and DAG DLTs and describes interested interconnected DLTs. The technical details provided represent a precursor to the presentation of our proposal, which is based on these technologies.

- Chapter 3:
  In this chapter, we present the different projects and applications tackled the adoption of DLT-based supply chain. These projects show significant contributions in developing the DLT system to facilitate its integration, and solve its scalability issue.

- Chapter 4:
  In this chapter, we propose a new decentralized architecture in which Blockchain and DAG are combined to increase the IoT functionality and enhance storage while keeping a high level of reliability, data accessibility, integrity, and security. We also highlight connector's role, architecture and implementation.

- Chapter 5:
  In this chapter, we propose a resource allocation scheme to fairly redistribute the decentralized computing loads between the DAG full nodes. The target is to balance the computing tasks among all full nodes. This can be achieved by the collaboration between the nodes to maintain the efficient system performance.

- Chapter 6:
  Since transparency is essential for a successful supply chain, we specify this chapter to highlight the DLT-based supply chain that enhances transparency. We survey the existing DLT-based supply chain projects leveling data transparency and we investigate the techniques utilized in the data transparency enhancement process including our proposed architecture. We Then shed light on the importance of transparency and borders between transparency and opacity through access control to successfully integrate Blockchain into a supply chain.

- Chapter 7:
  Conclusion and future works are presented in this chapter.

Chapter 2

State of the art on DLT

2.1 Introduction

Supply chain system refers to the entire process to produce and distribute a specific product including every stage from the supply of materials and the manufacture of the goods to their distribution to the consumer. Innovative technologies will enable the supply chain systems to perform their tasks rapidly and efficiently. IoT and DLT are interesting recent technologies that may help in improving the collaborative supply chain systems. In fact, in an overly simplistic way, IoT devices can serve as data collectors and transmitters, and DLT can act as a decentralized database. Nevertheless, these technologies bring many challenges to the overall system. This chapter mainly deals with Blockchain and DAG distributed ledger technologies. It provides a comprehensive technical introduction to both technologies included in our research. Thereafter, it discusses the interested interconnected DLTs and their adopted approaches. Furthermore, we introduce DLT-based supply chains and the challenges they face and define the requirements of a typical supply chain DLT platform.

2.2 Background: Overview on Blockchain

Blockchain is a distributed ledger that records all the transactions that have occurred among the participants of its network [13]. It is a peer-to-peer (P2P) Network with data storage composed of a sequence of interconnected "blocks," such as every block contains a set of encrypted and mutually hashed data. Therefore, the majority of the participants should validate the transactions to be involved in the ledger. The Blockchain runs upon four main layers that determine the data flow within a fully decentralized P2P system, as illustrated in figure 2.1. It is composed of connected nodes that might be end-users represented

by wallet applications running Blockchain-compatible software. It could be any device running software for mining purposes that help reach an agreement known by a consensus mechanism. Blocks are "chained" and secured by this consensus mechanism based on asymmetric cryptography and a cryptographic hash function. The Blockchain contains the timestamp of the chained blocks maintained by every participating node. Consequently, the historical transactions stored on Blockchain cannot be deleted or altered without invalidating the whole chain of hashed data [20].

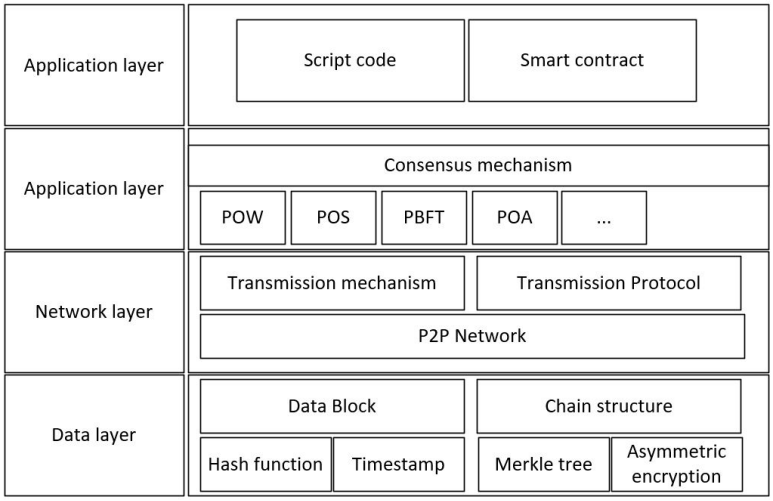


Fig. 2.1 Basic framework of Blockchain

Figure 2.2 depicts the Blockchain data structure that consists of an infinite chain of blocks started with the main block known as 'Genesis.' All the blocks consist of a header and a body. The latter contains the validated transactions, where the header contains various fields responsible for maintaining the chain. The header fields are mainly composed of block version, the hash of previous block header, timestamp, and Merkle tree hash representing the hash value of all the transactions in the block.

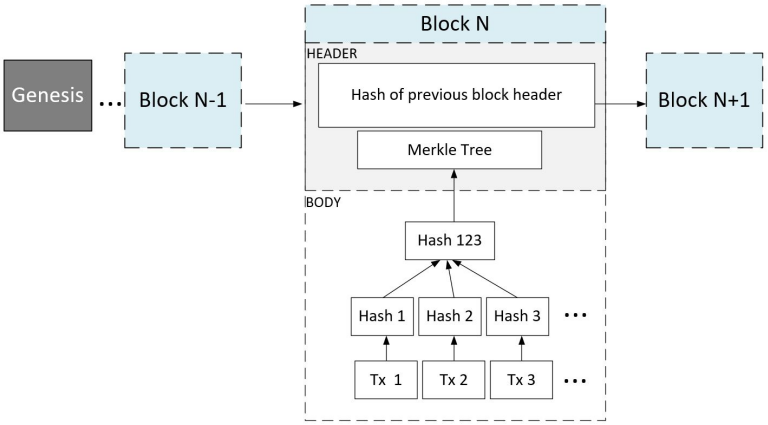


Fig. 2.2 Blockchain Structure

Blockchain technology is based on a cryptographic concept called a Merkle tree (AKA a binary hash tree). Merkle tree enables a binary tree data structure to generate a set of single-use signatures related to a single public key. Thus, a Merkle tree is a binary tree with an associated value for each node where each one is the hash of its children [10]. These data structures are useful for Blockchain technology in order to use transactions' hash inside the blocks. As a result, it allows a Blockchain part verification without downloading the whole of it. Figure 2.3 shows a simplified Merkle tree linked to a given block where T presents a transaction and H presents a hash. The block of all transactions hash is obtained by hashing each transaction, grouping them two-by-two and hashing the concatenation, then this action is repeated until we obtain only one hash representing the final hash of the block. If there is an odd number of transactions, one of them is doubled, and its hash is concatenated to itself.

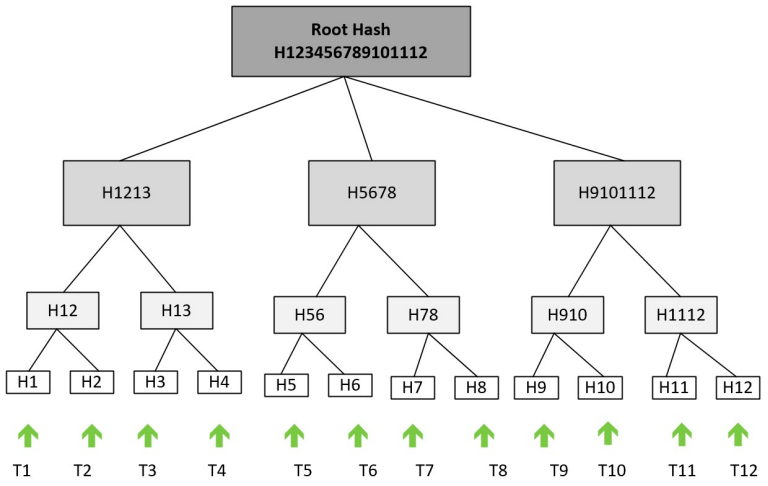


Fig. 2.3 Merkle tree structure

			READ	WRITE	COMMIT	EXAMPLE
BLOCKCHAIN TYPES	Open	Public Permission less	Open to anyone	Anyone	Anyone	Bitcoin, Ethereum
		Public permissionned	Open to anyone	Authorized participants	All or subset of authorized participants	Supply chain platforms viewable by public
	Closed	Consortium	Restricted to an authorized set of participants	Authorized participants	All or subset of authorized participants	Multiple banks or chain of restaurants operating a shared ledger
		Private permissioned	Fully private or restricted to a limited set of authorized nodes	Network operator only	Network operator only	Enterprise ledger shared among head office and branches

Table 2.1 Blockchain types

Mainly, there are four types of Blockchain [21] as shown in table 2.1 : Public Blockchain (permissionless) is available for anyone, such as bitcoin. Public Blockchain (permissioned) is open to anyone for data reading but restricted for data input, consortium Blockchain is a network of predefined organizations, and private Blockchain (permissioned) is limited to one enterprise.

2.2.1 Consensus mechanism

Contrarily to the centralized systems where trusted central authority maintains and controls the database, Blockchains are decentralized without any single authority. Furthermore, the nodes participating to a Blockchain are often non-trusted and/or anonymous. Hence, it is required a secure and fault-tolerant mechanism that allows authenticating transactions and maintaining a unique and shared view of the database among all the participants. In Blockchain terms, this mechanism is called "consensus." A consensus mechanism is used in a Blockchain to achieve the agreement on the Blockchain's state periodically. It is governed by a set of rules that regulate the contributions of the different nodes in order to maintain the Blockchain' state.

The consensus protocol is the essential component of Blockchain that generates and links the blocks to each other. It validates transactions within a pure P2P environment without relying on any trusted third party. Reaching consensus among non-trusted nodes is the core idea of decentralization. The Proof of Work (PoW) [11] is the first introduced consensus mechanism used in the Bitcoin system, which uses a mathematical riddle added to block hash. Only nodes with certain computation capability (or other selected criteria) can find the block validation hash in a reasonable lapse of time. The node that first resolves the riddle is

qualified for block validation and is rewarded specifically (paid in bitcoin). However, this whole mining mechanism needs high energy consumption and a longer processing time.

Proof of Stake (PoS) [22] is an alternative consensus algorithm with less energy and time consumption. PoS employs the stake of each node and a lucky factor to decide the block appending one. Using stake as proof has the advantage that the one who owns much stake would be more trustful. PoW and PoS consensus algorithms are the most popular ones used in research and applications. Besides these two well-known consensus algorithms, many proposed algorithms have considerable influence on the performance and security of the Blockchain. Proof of Capacity (PoC) [23], proof of authority (PoA) [24], and Practical Byzantine Fault Tolerance (PBFT) [25] are yet other exciting algorithm that are used nowadays on a large scale. The PoC mechanism is based on the storage capacity of the nodes. In this algorithm, the more storage space a node has, the more permissions are granted to add a new block. In the PoA consensus algorithm, a set of nodes are selected for the Blockchain management process. The nodes should prove their authority to generate a new block. In general, such an algorithm is used in a private Blockchain and proves high performance compared to other Blockchain types. PBFT algorithm guarantees network safety even when some nodes are faulty or malicious, as long as a minimum percentage of nodes are connected, behaving honestly, and working properly.

2.2.2 Smart contract

In the global market, companies use a massive of manual documentation to organize their relationships and execute their deals. The challenges of such complex processes urge the automated execution of the actual contract for improving business process execution. To tackle this issue, the concept of "Smart Contract" was introduced. This term was initially proposed in the early 90s for e-commerce applications [26]. Recently, it has been widely used in DLT and, in particular, Blockchain technologies [27].

A smart contract is a computer program intended to enforce a deal between two or more parties and guarantee its execution. In Blockchain, a smart contract is a computer program stored in the ledger and executed by some participant nodes. In this context, the Smart contract presents the relations, conditions, and rules that organize the business relationship. According to [28], a smart contract is an automatable and enforceable agreement executed on a computer and may require human input and control. A smart contract has a legal significance and a legal effect [29]. However, the recognition of the legal status of smart contracts currently represents a considerable debate. A smart contract can automatically implement

the content of a separate agreement, expressed in natural language. In this case, the smart contract may provide evidence for the agreement's existence and content between the parties [29]. Otherwise, when no other existing documents record the agreement, the smart contract itself embodies the binding expression of that agreement [29]. Smart Contracts are often written using dedicated languages. They are then compiled into bytecode and embedded in self-contained and self-enforced virtual machines or containers deployed in any node in the Blockchain. Blockchain-based smart contracts languages have been developed using general-purpose programming languages to fit the specific context of distributed transactions execution. For instance, we can mention Solidity [30], LLL (Low-Level Lisp) [31] and Serpent [32].

Solidity is an object-oriented static-typing language based on JavaScript to write smart-contracts for several blockchains like Ethereum [33], Tendermint [34], Zeppelin [35] and Counterparty [36]. A smart contract written using Solidity is compiled and embedded in an Ethereum Virtual Machine EVM. LLL language is similar to the assembler that came to add a low-level layer before the EVM. The language adopts the syntax of Lisp. It is used when there is a need to have direct access to memory and storage. This can be explained by the need for optimization or resolution of a particular problem that is, by nature, low-level. The Serpent is a contract writing language close to Python. It is designed to encompass the benefits of Python in its simplicity, minimalism, and dynamic typing. The Serpent code is first compiled into LLL and then bytecoded into the EVM when building the executable.

2.3 Background: Overview on DAG Technology

DAG is another form of DLT composed of individual transactions linked to multiple other transactions that do entirely away with blocks. Two different DAG-based DLTs were introduced recently: IOTA and Hashgraph. The latter is primarily designed as private DLT, and it does not fit with the primary goal requirement of our research. Hence, the remaining study highlights the IOTA, a public DLT that fits with the massive IoT data of the supply chain.

2.3.1 IOTA Infrastructure

The IOTA Foundation has developed the Tangle as an alternative to the Blockchain to tackle most of the current Blockchain drawbacks [17]. IOTA conception has two main motives: i. the necessity of a scalable ledger because of the massive transactions sent by large IoT

devices and ii. the micro-payments of these devices. IOTA is based on DAG [37], where the transaction is the only IOTA element. Precisely, neither a block nor a chain is available. DAG is a mathematical graph approach, which consists of an edge and a vertex. The edge is a unidirectional vector between two vertices with no loop back to the initial vertex.

As shown in Figure 2.4, a transaction represents the vertex of DAG, which is charged by the validation of two transactions as a condition to be issued. Thus, to issue a transaction, the intended node should establish two direct connections to two different transactions. Connecting these transactions in this binary form and attaching the upcoming transactions to the network determine the shape of the Tangle, as shown on the right side of Figure 2.4. The genesis is the first transaction of the Tangle where tokens are created.

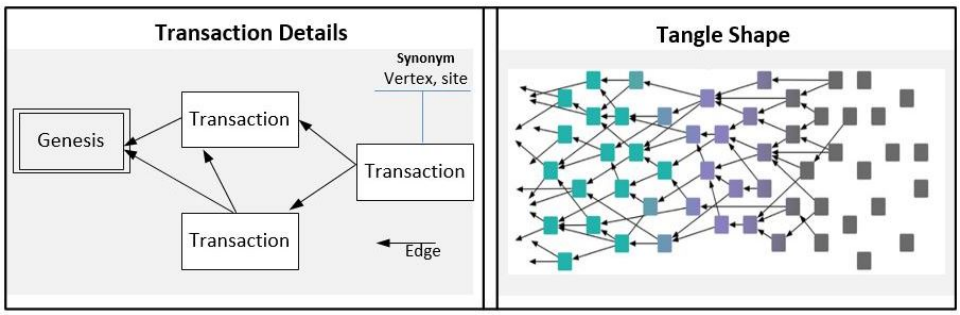


Fig. 2.4 IOTA DAG Structure.

Physically, each participating node communicates with its neighbor nodes to replicate their data, where all the nodes share the same ledger. The new transaction, which is recently attached to the Tangle and is not validated yet by any node, is called "tip," and is highly recommended to be selected by other nodes. A node that aims to issue a transaction selects two transactions from its up-to-date ledger to be validated; thereby, it will approve or decline them based on the ledger content. The lazy node is defined as the node that aims to pick approved transactions rather than tips. Selecting transactions, which are already validated, will leave behind many tips orphaned and impact the overall system performance. Therefore, it is recommended to eliminate the lazy nodes in the first step, or encourage the nodes to select tips rather than non-tips transactions.

2.3.1.1 Coordinator

The Tangle's security is primarily based on the high frequency of transactions that allow a considerable amount of nodes to participate in the transaction validation. The Tangle turns to be more secure when more transactions are issued. However, the current Tangle network's size is not large enough to achieve robust protection against several attacks where

double-spending is possible. Thus a third party is required to be installed temporarily for security purposes. Accordingly, the coordinator [37] is the temporarily trusted third party implemented to check the Tangle health periodically. It is a centralized application operated by the IOTA foundation to protect the Tangle from different kinds of attacks and double-check the validation of the transactions. The coordinator issues a milestone transaction every two minutes to validate the transactions. All the approved transactions have immediate confirmation confidence of 100% where the second transaction of a double-spending will not be accepted if any. Each transaction attached to the Tangle has its parameter values [37] that the coordinator uses to determine its path, and thereby, the honest transactions have a higher probability of being validated. In contrast, the lazy nodes which do not validate the new transactions (named tips) are punished.

2.3.1.2 IOTA Address

Each node's user has their wallet composed of a "seed" address that generates an unlimited number of public or private addresses. The newly generated addresses are retrieved from the combination of a seed plus address indexes. The address index is a positive integer starting from "0". Consequently, the "seed" is a random combination of 81 characters (letters A-Z) and the number nine that represents the secret account key, which should not be disclosed by anyone except the wallet owner. When a user publishes a transaction to the network, transaction will be signed based on Winternitz-One-Time-Signature-Scheme [38], and a part of their private key address is disclosed to the public.

2.3.1.3 Creation Transaction Mechanism

For a successful transaction issuing, a node is responsible for applying three steps sequentially: creating a bundle, selecting and validating two tips, and performing PoW:

- Create a bundle: Whenever a node wants to add a transaction to the network, it should create a bundle of transactions called sub-transactions. A normal transaction is a bundle of four sub-transactions that are indexed from 0 to 3. Index 0 is the recipient's address "output" of the external wallet with the amount to be sent. Index 1 is the sum of all the amounts inside the sender wallet called "inputs" and has half of the sender's signature. Index 2 represents the second half of the sender's signature. Index 3 is the remainder "output" that must return to the sender's wallet, which is the output minus the input. Accordingly, successful bundle results in an equal number of transactions in both output and input. The bundle is atomic so that either all its transactions are accepted or none of them.

- Select tips: Before attaching a transaction (bundle of transactions) to the Tangle, the node should select the two newest tips and approve them.

  Building a robust "select tip algorithm" is mandatory in a DAG-based decentralized environment. The motivations behind designing such an algorithm are based on pushing nodes to select the unapproved transactions (tips) and checking the conflict of transactions, double spending, and falsifying. There are three main algorithms that the coordinator can use to trigger the node to select tips [39]: unweighted, random walk, weighted random walk, and Markov Chain Monte Carlo (MCMC).

- Local Proof of work (PoW): Contrarily to the Blockchain PoW consensus, the IOTA PoW is done locally by the imitator node without interchanging the result with the other nodes. Thus, this PoW type does not share mathematical puzzle and avoid the competition among the nodes. Performing local PoW is the node's last task before issuing its transaction. Once the bundle is created, signed, and tips are attached to the bundle, the node performs PoW for each transaction of the bundle. The PoW is a sophisticated mathematical approach represented by the node's computational effort to achieve a predefined minimum weight magnitude (MWM) of the hash function Curl [38]. An MWM is the number of zeros included in a nonce to be accepted. During the execution of PoW, a nonce is found by combining a specific counter with transaction data that fit with the MWM. The PoW process is hard to achieve, but it is easy to verify the answer. Thus, the PoW validation will be the node task that signalizes this tip, and so on. Once PoW is performed, the bundle is attached to the Tangle as a new tip and broadcasted to the whole network to be validated by some node(s) later.

2.3.2 IOTA Updates

From the very beginning, the IOTA foundation recognizes the necessity of eliminating the coordinator to be a fully decentralized system once the network becomes big enough. The coordinator plays significant roles in security and achieving consensus, so the core network will witness major enhancements over Tangle components to shut it down. Thereby, they are working on fixing several drawbacks in the next release by introducing "the Coordicide" [40]. The coordicide includes the below new features that reshape the next IOTA structure:

- Autopeering: Currently, the process that allows nodes to join the network is applied manually, but it probably subjects the nodes to various attacks, such as the eclipse attack. Where the adversary can control the entire neighbor's node, the autopeering mechanism is required to facilitate the neighboring operations and hinder attacker

activities from targeting specific nodes. Autopeering consists of "peer discovery" and "neighbor selection" mechanisms. Peer discovery uses the authentication ping-pong protocol that allows every node to impart or perceive other network participants.

- Voting and Consensus: Tangle can comprise conflicting transactions due to the network propagation delay. Thus, it is required to reach a consensus on those conflicting transactions, which are currently applied by the tip selection algorithm. However, this algorithm is considered slow in solving the conflict since it uses random walking bias via honest nodes that leave conflicting branches behind. In addition, the transactions that select the wrong branch will be orphaned and reattached to a large number of transactions of the proper branch. Therefore, a consensus mechanism called "Shimmer" [40] is introduced in the new release of IOTA. Hence, nodes query other nodes about their current opinion of the ledger and adjust their opinion based on the proportion of other opinions. Two voting mechanisms, fast probabilistic consensus (FPC) [41] and cellular automata (CA) [42] are used to allow nodes communicate and decide on transactions status. There is a possibility of requiring a combination of both mechanisms to add flexibility to the voting process.

- Adaptive PoW: IOTA proposed this new algorithm [40] to allow devices with low computing resources to be involved in the attaching transactions' process to the Tangle. Additionally, it seeks to limit the devices with high resources from attaching an infinite number of transactions. IOTA defines new parameters on each node. The basic difficulty represents the threshold difficulty level that fits with any small device capacity. The adaptive rate is calculated based on mana owned by the node [40] and the number of transactions issued by this node within a time w. Each node's new difficulty is equal to the basic difficulty plus the adaptive rate multiplied by the number of issued transactions within a time interval w. Thus, the more a node issues transactions, the more the difficulty increases, and the allowed number of transactions is adjusted. On the other side, this algorithm empowers the low-resource devices to issue transactions with a minimal degree of difficulty;

- Tip selection: Represents a crucial part of the IOTA network that pushes nodes to verify the Tangle transactions. Currently, the biased random walk used by the coordinator has computational drawbacks, as it adds complexity over the orphaned transactions and obligates nodes to reattach them later on. The new consensus mechanism is independent of the tip selection algorithms (TSA), so the current TSA algorithms can be enhanced to select faster tips and incentivize non-lazy nodes. Furthermore, the limitation behind the biased random walk behavior is improved by pushing the node to

select from non-lazy nodes only while lazy nodes still have a chance to be promoted and approved if their issuer intends to. There is no direct intervention in the selection process, and at the same time, the selection becomes faster;

- Global node identities: in the new coordicide architecture, each node in the network has its identity that must be well protected. The identity is based on a new common public-key cryptography created by the IOTA foundation to sign transactions and link it to the issuing node in a tamper-proof way. Additionally, the issuing node adds its public key to every signed transaction. On the other side, introducing identities leads to a Sybil attack [43]. By introducing "mana", this kind of attack is mitigated. "Mana" is a reputation value that is equivalent to the total funds transferred within the transaction. In that way, the more mana, the more contributions in the network and vice versa.

2.4 State of the art: Interconnected DLT

After presenting the main features of Blockchain and IOTA, we consider the works related to the DLTs' integration topic in this section. While some forms of interaction and communication are possible today, the interoperability between different DLT technologies is still under investigation.

2.4.1 DLT's Interoperability

There are many Blockchain types, all of which have different characteristics such as the transactions' forms, crypto algorithms, and consensus algorithms [44]. The problem is further increased by different networks and organizations running completely different DLT technology versions and governance rules. It resulted in unconnected platforms and siloed, which affected the organizations from reaching their full potential and achieving their goals. Different interoperability solutions are introduced to connect various ledgers and mitigate the gap behind the decentralization concept. As the disparate DLT types and directions, their interconnections are also disparate with different aims and architectures. We distinguish between two main DLT interoperability types: homogenous and heterogeneous, as illustrated in figure 2.5. In the homogenous type, the DLTs are either Blockchain or DAG platforms. The interconnected DLTs belong to different architectures such as Blockchain, off-chain, or DAG in the heterogenous type. Below are the most exciting interoperability solutions:

- Sidechain [45] is a homogenous solution innovated in 2014 for Blockchains' interoperability and easiness of asset transfer between different cryptocurrencies. It is

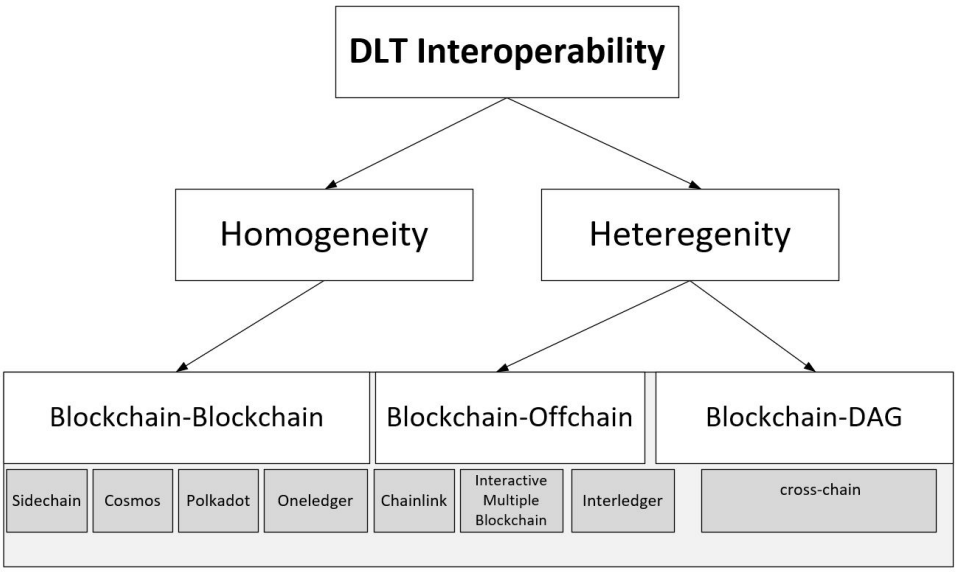


Fig. 2.5 Interoperability DLT Structure

represented by a second Blockchain connected to the main one through two-way pegged. It is not designed to make different Blockchains communicate with each other.

- Cosmos [46] is an interoperability solution for Blockchains that aims to link them to each other at a large scale. The Cosmos platform relies heavily on smart contracts, where its architecture is based on the 'hub-and-spoke' system. A series of 'spoke' chains connect to the hub central through inter-blockchain communication. They build IBC (Inter Blockchain Communication) protocol to communicate between the hub and the other chains linked to the network.

- Interledger [47] is an open-source protocol developed by the W3C Interledger Community Group. It is designed to be working within an open network to facilitate interconnection between different parties. Its core protocol ILP, (InterLedger Protocol), inspired from the internet protocol (IP), is somehow similar to the internet concept. Connectors of interledger work as internet routers where ILP protocol turns all transactions into the same ILP packet size. The main goal of interledger is to remove the barriers between Cryptocurrencies and allow payments throughout a predefined network set of connectors. A connector is a participant that has an account on the two different ledgers.

- Interactive Multiple Blockchain [48] is another proposal to tackle heterogeneous Blockchain integration based on a network of multiple Blockchains called router

Blockchain. Any node that joins the network becomes the router of this specific blockchain system. Routers share a dynamic routing table that is updated whenever a node leaves or enters the network. Since different Blockchains have different transaction formats, a unified cross-chain transaction is introduced for all systems. Two functions are used to fulfill the conversion process, pack and unpack. A transaction generated by blockchain A will be packed by its router and forwarded to Blockchain B. To this end, B's router will unpack the transaction, and thereby,it will be either accepted or denied based on the validation result. The router node transmits transactions according to the routing table written in the router Blockchain.

- Polkadot [49] is a Blockchain network that aims to solve blockchain extendibility and scalability. It is composed of a relay chain and parachains, where each parachain represents an independent blockchain. The relay chain is the connector that links these parachains and streams the message between them. With Polkadot, a parachain like "Ethereum" can apply its smart contract to other ones through the relay chain connector.

- Oneledger [50] is a heterogeneous connector that aims to connect centralized and decentralized applications and remove barriers between these two worlds. It is a gateway for organizations to their decentralized applications composed of API, protocol, and sidechains. Oneledger is called the Blockchain of Blockchains, and it provides communication between many independent Blockchains. The consensus is built upon three stages to enable effective integration with these different blockchain products: business initialization, channel consensus, and public chain consensus. Technically, it consists of a business center, consensus protocol, identity management system, intelligence engine, and blockchains with sidechains attached directly to their core networks.

- Chainlink [51] is an interoperability solution for heterogeneous DLT. It facilitates communications between disparate Blockchain platforms. The resources suppose off-chain data to enable smart contracts and outputs like established payment systems. This solution is vital for Blockchains that do not have to interact with other Blockchain protocols but require external inputs and outputs.

In addition to the above frameworks, the integration of Blockchain and DAG is not well investigated. W. Jiang et al. [52] propose a cross-chain interactive decentralized IoT data access model that integrates Blockchain consortium and IOTA to address the IoT scalability and usability. Their provided solution is a combination of Blockchain, tangle, IPFS storage, and notary nodes. IoT devices mainly work on tangle or sub-tangle platforms; however, IoT

devices can work on any Blockchain platform such as Ethereum, Hyperledger, and FISCO BCOS. IoT devices are grouped into sidechains, where each one represents an independent network. Blockchain acts as a controller with a primary role to connect multiple sidechains through notaries. The latter is a group of nodes that resides between Blockchain and the sidechain, acts as a gateway for transaction flows between Blockchains. The notary network confirms each cross-chain transaction by the voting mechanism, and the transaction is approved when the signatures of more than 2/3 notaries in the network are collected. IoT data is stored in IPFS storage, while the Blockchain stores only the hash of these IPFS files. They make use of BigChainDB to address the authentication drawback of IPFS. In comparison to single Blockchain utilization,this solution provides scalability for IoT devices. and offers an explicit integration between the DLTs mentioned above to enable inter-communication. Such explicit integration is considered as a limitation for the case where users are from the Tangle side only.

To overcome the limitations of the above solutions that tend to interconnect DLTs, we propose in chapter 4 an efficient solution where the inclusion of tangle-based applications is implicitly done with a backend Blockchain storage. Besides, while the existing solutions use IPFS based on the participants' devices, our proposal provides Blockchain as a service running on stable cloud nodes providing a robust and secure environment.

2.5 Background DLT-based Supply Chain

The Supply Chain field greatly influences the whole production ecosystem. The global target is to create a valuable supply chain platform while synchronizing business needs with new technologies such as DLT and IoT. To achieve this target, the management of key relationships and processes must integrate the whole chain seamlessly. In the following subsection, we present the current challenges related to supply chain, IoT, and DLT. We then summarize the DLT requirements for a typical supply chain platform in the next subsection.

2.5.1 Supply Chain Challenges

Globalization led supply chains to span the globe, integrating stakeholders from different companies, cultures, habits, and values. Putting aside the many benefits this change has brought, the supply chain is now encountered by a set of new challenges, such as the lack of standardization between entities, limited visibility over the whole supply chain, and the ever-increasing demand for transparency by the last consumers. In fact, in a collaborative

supply chain, participating stakeholders might be subjected and/or accustomed to different ways of collecting, storing, and exchanging data (in some cases, complex physical documents are still being used [53]). This procedure leads to different data types, latency, and data unreliability throughout the chain. Consequently, many inadequate decisions may be made, bringing down all the advantages of collaboration.

To improve the supply chain in collaborative environment, it is necessary to accurately collect relevant data, securely store them, and then provide transparent access to the intended information in a tamper-resilient manner. In other words, we need an efficient platform that can provide products' end-to-end traceability so that stakeholders get the necessary information about the products component's provenance, distributors, certificates, storage, and manufacturing conditions at the right time. In this context, IoT and Blockchain are used to improve the supply chain systems.

2.5.1.1 IoT-based supply chain challenges

The enormous variations in the supply chain increases the demands on implementing IoT technology within the supply chain. Due to the current supply chain infrastructure, which constitutes multi-centralized independent platforms, the supply chains are surcharged with high loads, leading to information loss [9]. These systems, such as Walmart and Cisco [54], depend profoundly on standalone, often different, and centralized platforms [55]. The group of databases involved in the production are autonomous, heterogeneous, and distributed [56]. Therefore, the inflexibility in interchanging data among these databases is referred to as the hard-coded nature of different data form standards. The collaboration would be limited due to the organizations' desire to use their platforms and control their data and different protocols and workarounds are used to enable interoperability to a particular supply chain. XML, ebXMB, and UDDI are some workarounds used to facilitate interoperability, but they are ineffective in heterogeneous databases due to different standards of databases. File transfer that uses fix format such as XQuery is the only protocol used to interchange data between organizations [56]. The uncontrolled informational data of the centralized systems causes outsize counterfeit, huge information loss, and bad business reputation.

Besides, data traffic is the primary concern referring to the distributed nature of the IoT-based partners. In other words, these IoT devices collect enormous data which the centralized stakeholders cannot fully manage. A product that passes across several geographical areas includes many critical documents such as invoices, ISO certificates, letters, proofs, customs, etc., requiring different levels of communications between partners. A study displayed that two hundred connections are needed to realize a single product delivery [57]. On a large scale,

traditional systems suffer from high traffic connections. Unfortunately, the current solutions do not guarantee safety, integrity, and on-time delivery of goods/documents, which leads to data loss and confusion. Furthermore, the current systems are vulnerable to exploitation and attack on a large scale due to their widespread and lack of control [55]. The characteristics of IoT devices and their challenges in the supply chain are listed in the below subsection.

2.5.1.1.1 IoT characteristics and challenges

The widespread of IoT adoption is triggering profound changes in global manufacturing and supply chains [58]. IoT technology has the potential to affect every piece of daily human life. The following characterizes the IoT:

- Low-cost and high-performance: IoT devices are heterogeneous in nature with different hardware platforms and capacities. Most of them are sensors of small size and limited computing resources, storage, and communication. These devices are classically low in cost and can be extensively positioned on large scales to collect temperature, pressure, humidity, and medical/chemistry parameters.

- Massive nodes and enormous collected data: The number of IoT devices participating in the different areas is continuously increasing, and it is expected to increase up to 140.94 billion by the year 2030 billion [59]. Besides, the massive presence, IoT gathers significant numeric data volume instantly and with highly accurate information.

- Decentralization: due to their heterogeneity and their wide geographical distribution, IoT devices can belong to different systems and applications. The IoT devices run in a decentralized manner to avoid processing data at the same time. Decentralized clustering algorithms in wireless sensor networks (WSN), for example, contribute to IoT's capacity and scalability [60].

Although IoT technology facilitates the production progress by helping the fabrication part and providing high control, it charges peripheral devices and servers with high data load [4]. The current network infrastructure fails to employ the IoT's full potential and manage the enormous received data within such centralized situations [9]. In that way, considerable IoT power is dismissed. Unfortunately, centralized solutions fail to manage and control the enormous incoming data as they were designed for [9]. Nowadays, there are no reliable frameworks or infrastructures intended to connect the massive heterogeneous and disparate IoT devices and their connected services, not to mention data analysis and aggregation [61]. The current standalone supply chain systems ineffectively contend

to provide some of the requirements in the means of trusted third parties and workarounds [9].

2.5.1.2 Blockchain challenges in the supply chain

Blockchain has another kind of shortcomings as it does not cover all the supply chain requirements. The Blockchain-based supply chain systems encounter new significant issues due to the decentralized nature and the structure of each Blockchain. The scalability is the primary concern of Blockchain applications, and it is referred to the delay in responding to the numerous requirements caused by the decentralized P2P system structure. The instability of the IoT' networks integrated with supply chain and the low throughput multiply the scalability issue. Blockchain transaction relies on different factors. Reaching consensus among non-trusted nodes is the core idea of decentralization. The consensus protocol is the essential component of Blockchain that generates and links the blocks to each other and validates transactions within a pure P2P environment without relying on any trusted third party. Despite its precise and vital role in protecting the businesses among non-trusted nodes, the consensus protocol is the major Blockchain component that directly impacts scalability. Furthermore, Blockchain decelerates the application by its design and restrains the transaction with internal cryptographic rules that reduce the transaction propagation speed to an unaccepted rate. In the previous sections, we distinguished between the different consensus algorithms with reference to their performance and scalability. The second factor of scalability is the single shared ledger -the Blockchain engine- that contains the blocks, where each block is a set of validated transactions [13]. The block creation and transaction validation processes consume time and limit/control the propagation of the overall operations to get in the ledger. These processes hinder the system performance. The ledger size, the numbers of validator nodes, and the network status of nodes all over the supply chain also directly impact the processing time and performance.

With decentralization, participants are involved in rigorous computing tasks to maintain the distributed ledger. Power resources and CPU capacity are the main challenges of IoT devices. Such devices struggle to save energy by sleep mode [62] in idle time, for example. In this manner, the mentioned devices cannot contribute to computing P2P missions the same way as a dedicated server-miner. Consensus algorithms, such as POW and the cryptographic activities (encrypt, decrypt, hash, etc..), are not applied on most IoT devices [63] that are running on economic power [64], especially in a supply chain that contains millions of resource-limited peripheral devices. Thus, the transaction cost is relatively increased. IoT devices are installed for particular tasks and distributed at a large scale to gather data accurately. The ledger size, which is being stored on every node of the network, increases

with time. Thereby, they are very limited in storage capacity [65][66]. Most devices are sensors and detectors; thus, finding an IoT node with accepted memory storage is rare. Hence, reliance on these devices to store the distributed ledger is a considerable challenge that affects the whole system. Furthermore, every transaction is stored permanently on the Blockchain ledger, while storing low-value information is futile. The inability to compact or reduce the ledger's undesired data augments the challenges.

Network infrastructure is likewise a primary factor for a successful Blockchain. All nodes involved in the DLT system should be continuously connected and synchronized to maintain the P2P network. However, high network requirement is inconvenient with IoT's nature. Mainly, most of the supply chains distribute their IoT devices in different geolocations. Providing good throughput is costly and unstable, which poses security risks and/or data instability. Conjointly, transaction fees are still a significant drawback in Blockchain resulting in transaction delays in the process [67].

2.5.2 Supply chain requirements

In this subsection, we set the typical DLT-based supply chain requirements to clarify and facilitate the future proposal options. The leading technologies that compose the modern supply chain applications are DLT (mainly Blockchain) and IoT systems. DLT, IoT, and supply chain platforms altogether compose the robust body of the future supply chain. Thus, considering the combination of these factors [9] while investigating supply chain shortcomings is a must. As seen in the previous section, traditional systems encounter many issues and require profound alignment to cope with business expansion. We have also seen that Blockchain is not free of limitations and drawbacks, where regular supply chain integrated with IoT and Blockchain contains drawbacks and limitations [9][63]. In short, it is like a compatibility matter between the regular supply chain and IoT from one side and between the supply chain and Blockchain from the other side. Hereafter we investigate the relations between supply chain, IoT, and DLT that determine the strength of the modern supply chain. We then list the requirements for the typical platform system and the strategy of the upcoming works, where scalability, traceability/transparency, and overall visibility are the core benefits of a proposed system. We raise the flag of the typical supply chain so that decentralization is the crucial answer [68][69], taking into account the diversity of the IoT devices to exempt the weak devices from being charged with heavy tasks. This study is conducted to obtain the maximum benefit and advantages from the current DLT and IoT technologies without paying high workload taxes from the peripheral device's resources. The Blockchain requirements for any supply chain system are decentralization, traceability, the immutability of the ledger, fault tolerance, and data security. Besides, smart contract

technology running on top of the Blockchain platform introduces process automation and improves the integration of the IoT systems [55]. Table 2.2 groups the best practices of computing, storage, and transaction fees related to the above Blockchain problems. The table points out the typical values of the three drawbacks of Blockchain under the typical Blockchain conditions. Each table entry determines the perfect situation, which may be out of reach in many cases. However, these inputs assist in constructing the next faultless platform and are almost free of limitations. Computing is the primary factor in a DLT P2P system to validate transactions, achieve consensus, and build blocks securely. The P2P system should consider the computing resources of devices not to consume more than a predetermined margin of a participant node resources. Fulfilling the computing tasks requires nodes to be online and synchronized continuously, which is not well-conditioned for most IoT devices in terms of power, network, and device health status.

Besides, the supply chain system is already designed to achieve large complex tasks, so the consensus algorithm and its mining process associated with the DLT system should not affect the production progress. Eliminating high computing is possible, but it supposes conditions and major changes such as diving into permissioned DLT or using specific consensus algorithms such as POA. Storage is another major factor in a successful DLT system. As a P2P system, the ledger is stored basically on peripheral devices that surcharge them by the ever-increasing size. The best practice in a supply chain system is to exempt participants from being charged with high load.

BLOCKCHAIN REQUIREMENTS		
Computing	Storage	Feasible Transaction
Not rely on IoT devices	Extendable size	Consider micropayments
Avoid continuous	Not rely on IoT device disks	Feasible transaction fees
synchronizations	Accessible anywhere	Not limited to some currencies
No high power consumption	High throughput	Consider IoT device status
No high network consumption	Secure (data encrypted)	
Light mining system		
Light & secure consensus protocol		

Table 2.2 Ideal Blockchain requirements for supply chain

The alternative storage solution should provide extendable storage to avoid the disk space problems and be located outside the participants' devices (on the cloud, for example) so that the IoT devices can access the data securely and with an acceptable throughput. When it comes to transaction costs, it is highly recommended to consider the micropayment transaction fees. In other terms, the recommended fees system should be very low, feasible for different payment types and currencies. Also, consider the peripheral devices that are working

offline or using internet service intermittently to provide the ability to issue offline payments and join the ledger after being online. Minimizing the impacts of computing, storage, and transaction fees is an uneasy mission, and it is based on each use case's requirements and capabilities in managing its parameters. In short, the terms mentioned earlier should be managed so that each case's primary goal is achieved with no negative impacts on the platform. Ideally, the IoT technology should attain all the Blockchain advantages without being charged with computing, storage, and network replication tasks. Currently, this milestone is not well-achieved with the current Blockchain systems.

2.6 Conclusion

This chapter paved the way for a better understanding of the various DLT technologies, which are essential for this research. It helps with the comprehension portion of the thesis's first objective. We began by providing the necessary technical background for Blockchain and DAG technologies, and then we highlighted the various existing frameworks aimed at different interconnecting DLTs. We also investigated the possibility of connecting Blockchain and DAG systems, as in [52], and discovered that the proposed interconnection is limited and insufficient for the case where users are only from the DAG side. To progress further in the DLT-based supply chain while ultimately achieving part of the second thesis' objective, this chapter introduced also the DLT for the supply chain, their challenges, and the DLT requirements to acquire a typical platform. In the next chapter, we will investigate the most critical DLT-based supply chains and their tools and architectures.

Chapter 3

DLT-based Supply Chain in the literature

In the previous chapter, we achieved the majority of the thesis first objective and part of the second one by presenting a detailed overview of the two different DLT types and covering the state of the art of the integration/interoperability of the DLTs platforms. Also, we highlighted the existing supply chain challenges and depicted the DLT requirements for supply chain. In this chapter, we continue in achieving the second thesis objective by listing the existing DLT-based supply chain projects and investigating the well-known tools involved in the supply chain projects. Besides, we investigate other projects that are external to the supply chain environment and also address the Blockchain drawbacks. The analyses of the tools/mechanisms mixed up with these projects lead us to propose a completely new DLT platform suitable for the supply chain.

In the literature, few surveys and studies highlight the integration of Blockchain with the supply chain environment. Table 3.1 displays the current surveys that tackle the Blockchain-based supply chain entirely or partially and provide a clear perception/understanding of the Blockchain and supply chain challenges and their impacts on different case studies.

Surveys	Roles
[70, 71]	Reviews industrial applications across different domains.
[72, 73]	Surveys the enabling and constraining roles of the technology from a business/ management-oriented perspective.
[74, 75]	Organizes the theoretical implications of adopting Blockchain in supply chains.
[76]	Analyzes the impact of Blockchain on different supply chain flows through case studies.
[77]	Offers a systematic mapping study focusing on the research aspect of Blockchains, recognize challenges that remain unsolved.
[78]	Conducts a brief literature review to introduce the Blockchain technology and utilizations.
[79]	Adopts Blockchain in several organizations and host in their work summary statistics useful in benchmarking the current practice.
[80]	Evaluates the applicability of Blockchains in the supply chain domain.
[56]	Categorizes the different scalability solutions into different layers, including on-chain and off-chain, and compares their impacts.

Table 3.1 Existing surveys on Blockchain-based supply chain

However, these surveys do not consider the alternative DLT solutions that could enhance the supply chain and cover the typical supply chain requirements within the decentralized platforms. In addition to the above surveys, many projects run on the new supply chain DLT-based concept to somehow introduce many tools in their proposals. We will present these tools during the next section to be enrolled in the design of future proposals, and we focus on the exciting projects and their tools.

3.1 Existing DLT-Based Supply Chain Solutions

The DLT integration with the productions and their different partners aims to renovate the global supply chain with the help of smart contracts, other Blockchain features, and IoT technology. Many DLT-based projects aim to provide scalability and reduce the time and cost by investigating new platforms based on DLT. Many challenges encounter these projects, including the type of supply chain business, the main goals of the new platform, and the DLT challenges mentioned above. Ucl CBT report [81] mentions around a hundred projects integrated with DLT and IoT and characterized them upon four natures: healthcare,

grocery, fashion, and supply chain. Most of these projects are based on the Ethereum public Blockchain and API interfaces but have no detailed technical references or clear publishments. This section aims to present a considerable number of studies and projects that invest in the DLT for the supply chain and display their technical part if any. We First shed light on the five projects with valuable contributions in this field. Then we list the remaining projects in subsection 3.1.2.6 .

3.1.1 Existing Tools to Achieve the Typical Supply Chain Platform

Before introducing the existing solutions, we list the important tools that are somehow involved in enhancing the DLT platform. The proposals of the developed DLT-based supply chain include some tools and solutions. We investigate these projects and retrieve the existing tools that could be used to fulfill the scalability requirements related to the supply chain progress. It is meaningful to filter them out to design and figure out the future supply chain platform. It is worth noting that no one tool alone helps to achieve the ideal supply chain platform. Instead, a combination of many solutions has an advantage in this situation.

Tools	**Data Size**		**Tx Speed**		**Tx Cost**	
	Tx Rate	Ledger Size	Consensus Algorithm	Block Structure	Tx Fees	Computing
Off-Chain	✓	✓	x	x	x	x
Sharding	x	✓	x	x	x	x
BaaS	✓	✓	x	x	x	✓
Consortium/ Private	x	x	✓	x	✓	✓
Modify BC Core	x	x	✓	✓	x	x
Editable BC	x	✓	x	x	x	x
Alter DLT system	x	x	✓	✓	✓	✓
Involvement of IoT Device	x	✓	x	x	x	✓

Table 3.2 Tools' impacts on Blockchain Scalability

The displayed tools are listed to address the most significant Blockchain problems, where each one treats a single problem. Furthermore, each mechanism has its advantages and drawbacks; thereby, the ideal proposed solution afterward should reap only the features as maximum as possible. Table 3.2 depicts the tools' impacts on the three scalability metrics: data size, transaction speed, and transaction cost. Below are the most valuable tools:

1. Off-Chain Solution:
   Although Blockchain is an immutable, secure, trusted, and linked-time solution for

any application,it ends up putting a huge data on its board. Off-chain comes as an exit to benefit from the Blockchain features while the data are processed and stored outside the Blockchain ledger [68]. In this case, Blockchain is responsible for monitoring the overall transaction processes by storing hashed transaction values inside its ledger [69]. Besides, smart contracts can be implemented inside the Blockchain for off-chain services. By doing so, the Blockchain will not be overloaded, and at the same time, data are processed outside the block policies. Thereby, this solution provides scalability and data reliability for the off-chain applications while maintaining the decentralization concept. Off-chain can be decentralized but not a DLT-based platform that can be integrated with other DLT platforms; the case of [82].

2. Sharding Blockchain:
   The increase in participants that share a single Blockchain ledger causes the unreliable distribution of blocks among vast nodes affects scalability. The sharding technique is a solution that aims to divide blocks between nodes [83][84]. In other words, nodes will be grouped into shards (limit number of nodes), and each shard contains a different part of the ledger. The transaction process, including validation and reaching consensus, and storage location, is limited to the intended shard only. Using this technique in a massive Blockchain environment achieves scalability [85] and prevents high latency [86] following block distribution across all nodes.

3. Blockchain as a Service (BaaS):
   Cloud services are adopted to facilitate the IoT functions, storage, and data processing [87], and fog computing technology helps distribute IoT services at a massive scale [88]. However, cryptographic algorithms are not enough to secure such a great workload regarding security and transparency. In addition, with the absence of transparency, data could be corrupted, doubled, or altered due to data spread in different geolocations and distribution on billions of devices. Accordingly, running Blockchain on top of cloud services and edge computing peripherals solves the security and privacy issues throughout the immutable, transparent, and reliable ledger. Besides,the cloud plays the role of the big shared extendable storage of the Blockchain instead of relying on the users' devices [89][69]. The successful implementation of edge computing servers [88] for a supply chain empowers the IoT devices to exchange data quickly and with minimum latency.

4. Private/Hybrid Blockchain:
   A hybrid Blockchain is a particular Blockchain that lies between private and public Blockchains. It is also called the public-private Blockchain. It is mainly used to restrict

the information's visibility in the network. The hybrid Blockchain is represented by partial integration of Blockchain in the workload while keeping a considerable part outside the Blockchain access and control. This type of Blockchain integration is welcomed by systems that do not fully support DLT or insist on keeping part of their application(s) under their centralized control. Multi-chain, such as Cosmos [90], lightning networks, and payment channels use hybrid models. Furthermore, private [91] or consortium Blockchains are closed of permissioned systems where peers deal with transactions upon predefined rules, and the transaction validators are limited to preselected authorized users. The permissioned Blockchain is attractive in terms of performance and scalability since the validators are limited in numbers and device types. With permissioned Blockchain, there is no need for complicated algorithm protocols such as POW or POS. Instead, POA or any other light protocol will be useful and secure in this case.

5. Editable Blockchain:
   The well-known immutability and irreversibility features of Blockchain are a two-edged sword. Although these features provide the supply chain with many benefits, they bring some drawbacks. Blockchain suffers from the inability to cope with the high incoming information of the vast IoT environment because of the components that compose its structure. The data recorded in a ledger is permanent, negatively reflecting on the ledger size and pushing all nodes to store the negligible data forever. The feasibility of having an editable Blockchain [92] is not available yet, as it still requires more research. Editing or removing a block(s) due to mistakes, typos, attack impacts, temporary records, or negligible data without breaking the chain enhance Blockchain adoption and scalability. Authors of [92][93] propose a redactable Blockchain using the Chameleon hash function, which helps to reduce the data size, especially for unimportant data like those related to food after being consumed. This bold move toward editable Blockchain is critical and requires strict governance rules to avoid exploitation and fraud facilities.

6. Blockchain core improvement:
   The P2P Blockchain system encumbers IoT devices with computing tasks and high storage demand [94]. In the cryptocurrency field, there are several full nodes prepared with high capacities for the purpose of mining and validation, which is not the case with the massive supply chain IoT devices. Thus, it is required to adapt the main characteristics of Blockchain to boost the association of IoT devices with their circumstances. Minimizing the block size, adjusting the consensus algorithms, and reducing

block creation time, are the most changing and adjusting Blockchain areas to fit IoT requirements.

7. Non-Blockchain DLT Platform:
   The success of Blockchain encourages researches in this domain. A directed acyclic graph (DAG) [95] technology DLT-based named IOTA [40] is found to tackle IoT devices' scalability and transaction fees where transactions are treated simultaneously. IOTA (or Tangle) is similar to Blockchain in terms of decentralization features, but it differs in structure and behavior. It neither has block, chain, nor transaction fees. The transaction is the only unit in the scene where the node is responsible for validating two previous transactions to get into the Tangle. Running a DAG-based application on IoT devices will overcome the Blockchain shortcomings, but we cannot rely on DAG technology alone (at least for the time being) in managing the whole system. Another DLT system is the Autonomous Decentralized P2P Telemetry (ADEPT) [96], provided by Samsung and IBM. ADEPT categorizes the IoT devices into three types: weak to strong, including light peer, standard peer, and exchange peer. A peer list that is shared among devices permits each device to define its level. The use of lightweight network protocols for IoT devices helps in achieving streaming communication. Also, Hashgraph [97] is a new DLT type, asynchronous Byzantine Fault Tolerance (aBZT) consensus algorithm based on a virtual voting algorithm and the gossip protocol to achieve consensus quickly, fairly, efficiently, and securely.

8. Involvement of IoT Device
   IoT device has two main functions: It captures the data and delivers it to its endpoints. Thus, IoT has two main challenges, the storage and the security of these data. Also, the integration with DLT, end device generates transactions of raw sensory data, verifies transactions, and even mines blocks. It is worth working on improving the IoT manufacturers to be suitable with Blockchain requirements. IOTA [40] categorizes the IoT nodes upon their capacities [98, 99], so there are the full and light nodes. However, the light node still needs to validate transactions to satisfy the system requirements. It is also quite important to mention the necessity of the "IoT for Blockchain" concept. In other terms, to improve the IoT end devices as maximum as possible to fit with DLT requirements in terms of CPU, disks, network, and power. In that way, some of the projects listed in the next section have contributions to the IoT hardware improvements.

Tools / projet	Sharding	Off-Chain	Cloud-Based	Blockchain Core Improvement	IoT Involvement
Waltonchain [100]	Not applied	Subchains are working as off-chain of the main parentchain	Not applied	Consensus POST (POS+POW+ POL)	RFID enhancements
Origintrail [82]	Not applied	ODN: Decentralized system composed of 4 node types	Blockchain layer can be the cloud service	Not applied	Not applied
Vechain [101]	Reed-Solomon(RS) algorithm	No applied	Vechainthor is BaaS for the supply chain projects	New fields to transaction format to mitigate a bundle of issues Added new payment method “multi transaction payment"	Upgrade traditional IoT equipment on the chip layer
Ambrosus [102]	Not applied	IPFS(storage)	Not applied	Custom Ethereum blockchain Introduce smart contract requirement /measurement	Introduce new effective sensors to trace internal and external data
Modum [103]	Not applied	Not applied	Not applied	Not applied	Introduce “modum temperature logger” shipment

Table 3.3 Existing tools for supply chain

3.1.2 DLT-based Supply Chain projects

This section highlights five DLT-based supply chain projects with good contributions and optimizes parts of the supply chain components. The five DLT-based supply chain projects are involved in the evolution of the modern supply chain integrated with IoT technology. Each project includes a short description and a figure inspired by its whitepaper. Moreover, this study highlights the tools used in each project, the problems encountered, and how far they are practically distinctive from the typical supply chain. Table 3.3 resumes the essential tools of these projects and their different techniques.

3.1.2.1 WaltonChain

WaltonChain [100] is a particular Blockchain designed for the supply chain to track the RFID-based transactions by multi partners. As illustrated in figure 3.1, it is composed of parent chain and sub-chains with cryptocurrency named WTC running and mined on the parent chain. A sub-chain is working separately after being created and registered inside

the parent chain. The parent ledger contains only detailed information related to the sub-chains. Each sub-chain has its ledger and can be created and registered any time under the parent chain network. Parent chain consensus is a combination of POW, POS, and POL. Besides, its block creation time is 60 seconds. Its ledger size is not affected by the number of sub-chains since the parent chain runs independently of sub-chains. Thus, the parent chain is considered scalable and secure. In addition, the smart contract is the foundation of waltonchain that builds and maintains the underlying logic platform. The waltonchain block contains up to 255 transaction records. It is made up of Block's depth and timestamp, block identity, block account ID and public key, the identity of the previous block and the hash value, the total number of tokens of the transactions contained in the block and byte fee, the transaction information contained in the block, Block payload length and payload hash value, The generated signature of the block, Accumulated coinage difficulty of the block. An updated version of POS called proof of stake trust (POST) is used to achieve the consensus of the waltonchain parent blockchain. With the assistance of RFID, Blockchain involved the reputation of nodes to track their behavior and select the honest nodes as coinage nodes. The POST mechanism strengthens the security of the Blockchain. The subchains are free to choose either POS or POST or any other consensus algorithm that fits their application requirements.

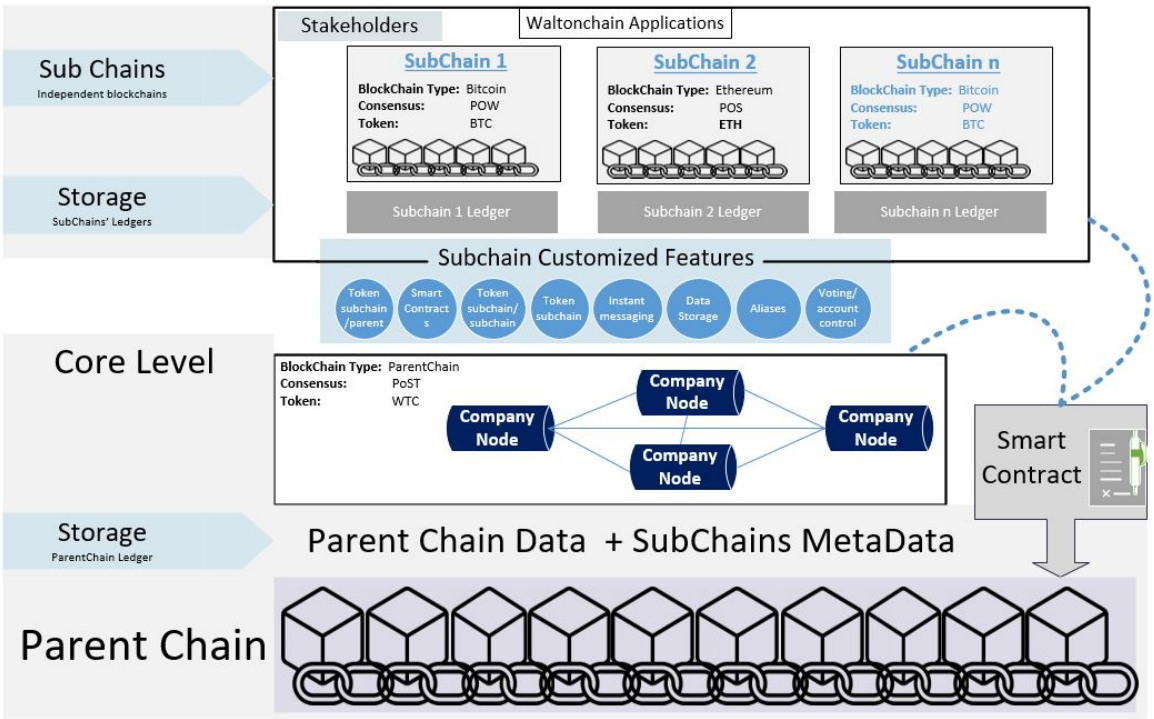


Fig. 3.1 WaltonChain Architecture

To create a subchain, the creator consumes WTC on the parent chain, so basic information regarding the new subchain is registered in the current parent block. The creation of a new subchain can be customized based on its nature and conditions. Subchain features mainly include WTC token, subchain token, cross subchain token transactions, smart contract, account control, data storage, etc.

Waltonchain considers the IoT side tool by developing the RFID chips to integrate Blockchain better while tagging assets. However, this development is limited to IoT functionality, and it does not tackle the IoT weaknesses mentioned above (computing resources and storage). The block creation time is about one minute, which will inhibit the scalability of the vast IoT involved within the system. The POST consensus algorithm is the waltonchain invented tool to be used within their parentchain platform. The interaction between stakeholders is hard and complicated because subchains have a wide variety of consensus to select. This design does not take into consideration scalability and real-time performance as well as the storage ledger size, network, and computing resources concerns.

3.1.2.2 OriginTrail

OriginTrail [82] is a supply chain solution that integrates different partner applications, off-chain networks, and Blockchain. It makes use of different nodes, as shown in figure 3.2. Some nodes, which are not DLT-based, implement off-chain within the decentralized environment. Some other nodes are involved in the Blockchain platform. The off-chain network is known by ODN (OriginTrail Decentralized Network), which is composed of data and network layers. The architecture is thus the stakeholders' applications, the non-blockchain decentralized ODN, and the Blockchain platform. Using a Blockchain platform stores the data fingerprint, ensuring integrity and transparency of records and providing an immutable supply chain system. OriginTrail protocol uses the consensus check mechanism to validate data provided by different stakeholders. The consensus check mechanism consists of three steps: Step1: approve the stakeholder by the previous one. Step 2: verify the matching stakeholders. Step 3: verify the matching transactional data and timestamps. OriginalTrail uses the zero-knowledge mechanism to prove private information without revealing them. Four node types are involved in the OriginTrail ODN structures distinguished by their roles: Data provider (DP): represented by the stakeholders, organizations, or consumers with data input to be shared with the supply chain. Data Creator (DC): it is the entry node toward the OriginTrail network. DC nodes receive the data from its provider and link it with data holder nodes. The DC controls and maintains the data process until it is executed. In addition, it checks the availability of the data during service time.

Data Holder (DH): DH nodes store the data provided by DC for a specific time and

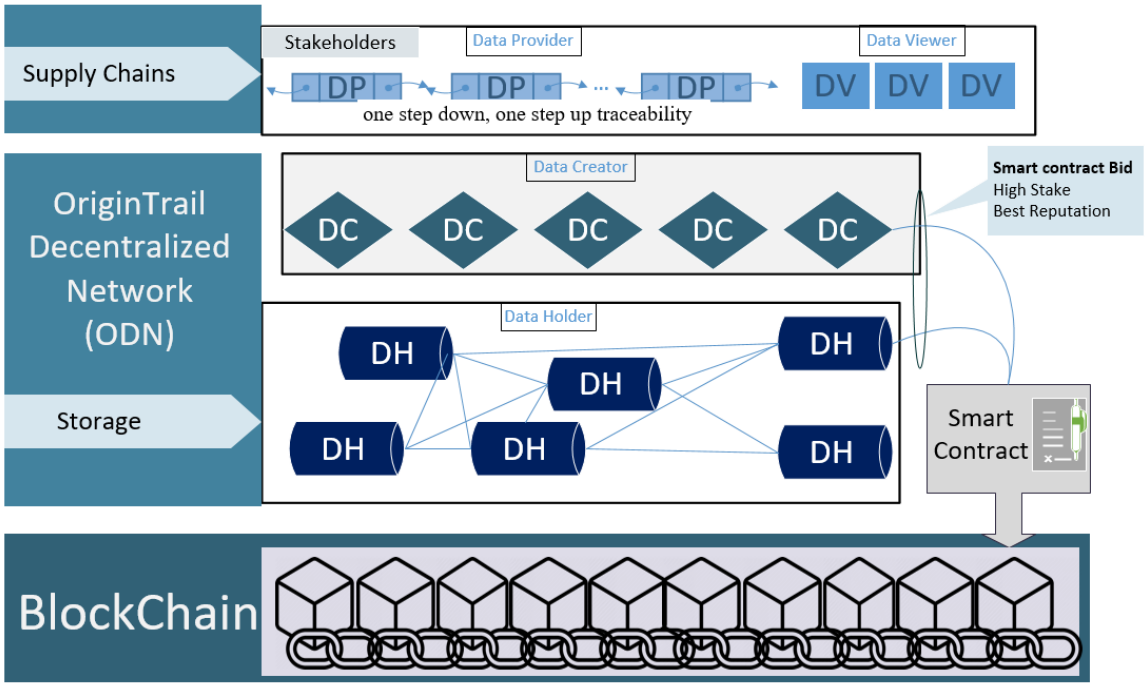


Fig. 3.2 OriginTrail architecture

ensure the data will not be altered. DH nodes are highly available to overcome bandwidth bottlenecks and the single point of failure. DH nodes share the data that is received from DCs in order to reply to some interested parties. DH nodes are compensated by the token" TRAC" for their efforts. A DC is dealing with DH through a smart contract that determines a set of conditions written by DC in addition to the minimum amount of stakes the DH should have. The amount of stakes owned by DHs guarantees its honesty in the execution of the required service. In addition to the stake, the reputation of DH and other factors are taken into consideration during the selection phase by DC. Data viewer (DV): DV is the entity that requests the data from other nodes with the ability to verify the integrity of the data by running the litigation procedure against the provided data. The nodes request their services by forming a bid between them (requesters) and the executors (other nodes). Therefore, DCs broadcast their offers to the network that is received by the interested DH nodes. The offer contains the requested services in addition to the criteria of the DH nodes. These criteria are the number of stakes, service price per data unit, the time elapsed to execute the service, and the candidate nodes' reputation. DC selects the storage node (DH) based on its hash value, where the closest hash value is preferable. This selection is automatically made to avoid the DC-specific selection of DH node(s). Off-chain is the most prominent invented tool of OriginTrail that is represented by the ODN network. The decentralized ODN nodes

employ the Blockchain platform to ensure their immutability and data integrity. In this context, Blockchain can be a cloud-based platform that facilitates communication between the different nodes of ODN. The none DLT-based solution provides scalability for the system as it discharges nodes from the computing and power consumption tasks. However, the system is exposed to a vulnerability attack if Blockchain and ODN are disconnected or being forcibly isolated.

3.1.2.3 Vechain

Vechain [101] is a supply chain solution composed of vechain supply chain projects and vechainthor blockchain-based platform as shown in Figure 3.3. Vechainthor is an enhanced version of Blockchain. It is forked and improved based on the Ethereum codebase. Below are the enhancements:

1. transaction format includes three new fields: ID, DependsOn, Blockref, and Expiration;
2. Each transaction has its own ID; thereby, the application deals with a single transaction instead of a transaction bundle of transactions;
3. Blockref delivers additional information about the previous, current, and next block. Also, it gives info about transaction creation time. It will be helpful for financial purposes in case of acceptance delay, for example;
4. Expiration is added to the transaction to avoid stacking for a long time. In addition, a transaction can do additional POW to speed up the validation time (it can consume more to track miners' attention, but the extra pow will compensate its loss);
5. Multi-task transaction: a transaction is composed of many small transactions to address the complex business payments.

Vechain uses Proof of Authority "POA" as a consensus algorithm that considers both stake and reputation. The maximum transaction speed announced is 10k transaction per second. As future work, they are looking for involving side chains to enhance the scalability of the vechain system. Vechainthor introduces the new multilayer payment model to ensure the token stability price. Two tokens are utilized to fulfill the transaction process: VET and VTHO. VET is the main token or" smart money" that represents the amounts been held by users. VET generates VTHO to cover the cost of smart contracts and transaction payments. Using this payment method will stabilize the cost of the token. Vechain uses Reed-Solomon (RS) algorithm to shard objects into many parts, and then it reliably reconstructs the data from the remaining drives. Thus, Vechain reduces the size of the data significantly. Besides,

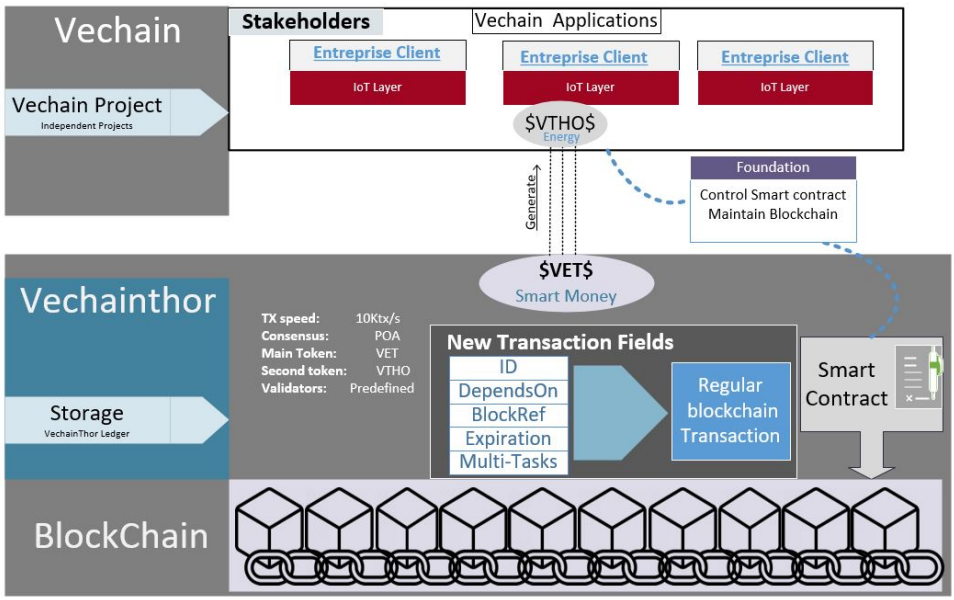


Fig. 3.3 Vechain architecture

Vechain considers IoT diversity and categorizes them upon their resources and functionalities to best employ their capabilities with Blockchain. Vechain connects the technologies RFID, QR codes, NFC, and bar codes to Blockchain to tag the items by a universally readable identity. This allows tracing the origin of items and prevents counterfeiting since Blockchain records cannot be alternated or duplicated. Altering block structure and sharding are the main tools used by Vechain to enhance the Blockchain platform. It also considers the IoT side and categorizes them based on their capabilities. POA consensus algorithm used in Vechain is more diacritical than POW and POS in terms of the validation process, and it does not require computing efforts. However, in a vast supply chain system, the validators become an easy target for adversaries. On the other side, the way the validators are identified renders the platform from being entirely decentralized. In an extensive supply chain project where IoT devices spread in many areas, Vechain does not provide a real solution to protect such weak devices from being surcharged by computing tasks.

3.1.2.4 Ambrosus

Ambrosus [102] project is to track products throughout their circulation in the market. It is a supply chain, Blockchain-based, dedicated mainly to protect and control pharmaceutical products and food values. This solution is principally composed of a customized version of Ethereum-Blockchain integrated with a data storage solution named interplanetary file system "IPFS" as illustrated in figure 3.4. To avoid the high cost of running the transactions

on the main Ethereum platform, Ambrosus develops its independent customized version of Ethereum. Besides, Ambrosus does not rely on Ethereum storage to store the supply chain data as it is limited in capacity. It makes use of IPFS as the main storage for their large transactions to provide scalability and high throughput for the clients. Ambrosus takes advantage of the Merkle tree hash cryptography in their transactional processes. With this tree algorithm, users can quickly find their data and filter out the wrong inputs.

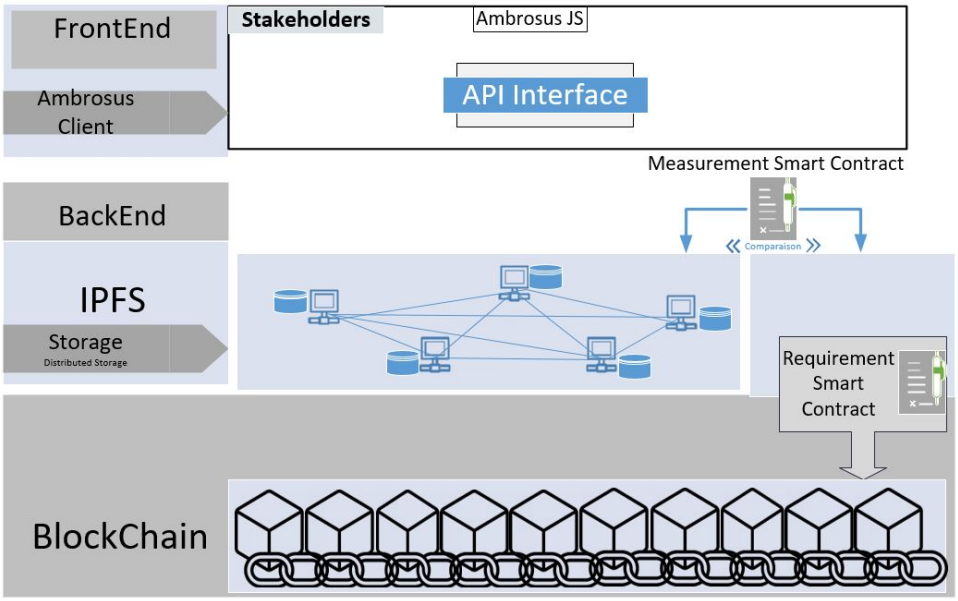


Fig. 3.4 Ambrosus architecture

Two types of smart contracts are introduced: the requirement smart contract to describe quality standards to be directly compared to items inside the Measurements Smart Contract. The measurement smart contract holds the list of the Merkle tree root hash, ambrosus-certified devices, and the collected attributes throughout the supply chain to note the variation of compositions' quality, if any. The Merkle tree data is uploaded periodically to the main Ethereum network to reduce network problems and improve scalability. The main structure of the Ambrosus network consists of three main layers: layer 1 contains the Ethereum blockchain and the IPFS storage. Layer 2 represents the supply chains and smart contracts, offline verification, and off-chain operations. Layer 3 represents the application and the Ambrosus javascript protocol. Ambrosus uses IoT hardware and sensors to tag products, thereby it tracks goods through the supply chain and ensures the full integrity. In addition to the environmental detectors such as temperature, humidity, Ambrosus has an advanced sensitive sensor. Several types of sensors or Biosensors have been developed to detect and analyze particular cases related to food and medicaments. For example, they can detect pH levels, allergens, DNA, and other types of physical properties. Ambrosus considers the IoT

side by introducing new high-level detector sensors. Besides, it is a customized blockchain that supports off-chain integration. The main ledger stores the Merkle tree roots to ensure that the data cannot be changed once written into a contract. Moreover, the idea behind the Requirements Smart Contract sounds goods, as it determines if a product continuously meets standards defined by intended participants in the Ambrosus network. This is to control the IoT detectors to get accurate results. On the other side, the structure of the nodes that form the customized Blockchain and the consensus algorithm used or the block creation time are questionable. Furthermore, the IPFS storage solution of Ambrosus is not a DLT-based system. It relies on participants' capacities to store the data, including IoT devices. Ambrosus does not respond to computing and storage concerns to enhance IoT integration with the supply chain.

3.1.2.5 Modum

Modum [103] is a supply chain for monitoring solutions that control the distribution of immense volumes of sensitive goods, especially pharmaceutical ones. It comprises the Ethereum blockchain network, the API applications, and a specific sensor called modum temperature logger. Modum architecture constitutes of frontend and backend phases, as illustrated in figure 3.5. The backend comprises an Ethereum network, smart contracts, and a specific server connected directly to external users. The frontend comprises sensors and mobile applications connected to the HTTPS server in the backend via REST API and JSON. The SensorTag (Logger) is the top added value that is used to measure the environmental conditions of the shipments. Each logger owns a unique MAC address represented in QR code and each shipment has its unique QR named "track and trace." Both QR codes will be scanned by the user's mobile applications and sent to the server. In case the server is not available, data will be stored on the logger's internal memory. Once received the combination QR codes, the server broadcasts the smart contract, then store the ID of the smart contract on the sensor. Then the client scans the "track and trace" code and requests the temperature measurements from the sensor via BLE "Bluetooth Low Energy." The smart contract obtains the data for verification purposes and sends back a report to the mobile client. It certifies data authenticity at every change of ownership. The evaluation results are immutably stored in a Blockchain as of proof-of-existence. In this way, opening the package to verify the content become useless.

The "modum temperature logger" sensor is used to precisely track the temperature of drugs periodically alongside the supply chain. Logger uses the NFC plate to connect with the shipment ID, where each one has a unique smart contract. By using NFC, the Logger alerts the team in case of problems during transport. Furthermore, they can add other sensors

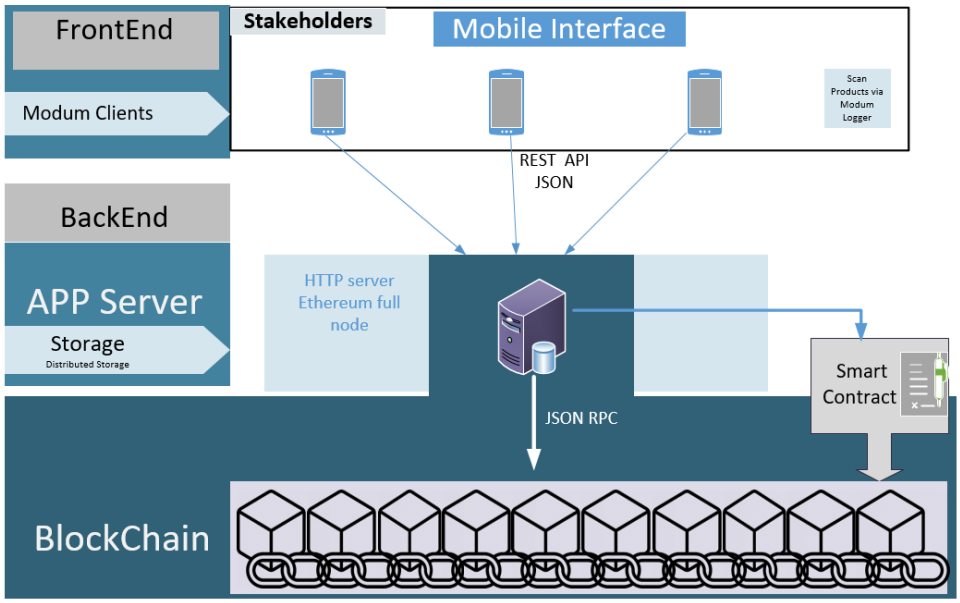


Fig. 3.5 Modum architecture

related to different monitoring tasks like motion detection for fragile goods, such as evolving their platform to fit different products and partners. Modum considers the IoT side "tool" by introducing a new sensor involved directly in the tracking process. It uses the public Ethereum for data verification with a specific HTTP server as a full Ethereum node that stores smart contracts and data users. However, this server is considered a single point of failure since it is not decentralized. Furthermore, scalability is not considered. It relies on Ethereum efficacity; thereby, improvements over computing and storage are not targeted by this project.

3.1.2.6 Additional DLT-based supply chain

Beside the aformentionned five projects, there are a considerable amount of projects that tackcle the DLT integration with the supply chain. In this subsection, we resume the maximum number of projects that interact with DLT and IoT technologies:

- Shipchain [104] is a fully integrated system of the entire supply chain that is specialized in tracking the shipments from the moment of leaving the factory to the final receiver customer's. Shipchain is running on Ethereum public blockchain using mainly smart contract techniques and side-chain. All the Records are stored on the Ethereum database, while side chain data are stored and validated on the organizations' network

for cost-saving purposes. Thereby, the data is located either on Ethereum public ledger or in the side chain ledgers where no intermediary is engaged. Moreover, shipchain contains a web platform that enables shippers to connect directly to carriers without passing by the traditional brokerage models.

- Devery [105] is an open-source protocol based on the Blockchain Ethereum network for verification services. This protocol is used to build applications for verification purposes where sellers can allocate unique signatures to their products. The signatures are stored on the Ethereum ledger and used in verifying a product throughout the application queries. Devery protocol consists of three data structures that interact with Ethereum through DeveryRegistery.sol and DeveryTrust.sol smart contracts. The three data structures are StructApp, unique identifier, and account. StructBrand is used to register a brand public key alongside the unique identifier of an application and store the brand information. Struct Product contains the app account, brand account, and product information. The hash of the product information determines the individual identifier for each product stored on the Blockchain and allows lookup via the check (address item) method. Devery uses the EVE token (Entry Verification Engine) for payments and charges. The consumers of the application service must pay the application host for the product verification service using' Bokky's Token Teleportation Service' (BTTS), which permits consumers to not interact directly with EVE or gas tokens.

- Cargox [106] is a decentralized solution that tackles the bill of lading documents implemented on the Ethereum Blockchain. Cargox is specialized in supply chain logistic trading worldwide. Users communicate via the API interface of the Cargox DApp and create their smart bill of lading. It has payment flexibility, so users can either consume cargo token "CXO" directly or utilize the USD/CXO conversion mechanism.

- CargoCoin [107] is a decentralized supply chain platform based on the Ethereum network that aims to encapsulate all cargoes, transport them into a unique platform, and then link them to the intended traders. To achieve this objective, both the services' platform and the smart contracts are utilized within the Blockchain. The platform allows for a range of communication channels between stakeholders involved in the supply chain progression, providing a method of sending/receiving, approving, rejecting or signing documentation.

- Bext360 [108] platform uses the blockchain system to track agriculture products throughout each step in the supply chain. Bext360 provides product traceability and

management of payments and smart contracts. It is based on a RESTful API that allows wholesalers and retailers to insert the technology into their own websites, point-of-sale systems, or supply chain management tools.

- Tael (WaBI) [109] is a decentralized application that creates a secure link between partners. It is an independent blockchain installed on user mobile to validate their product through a mobile application. WaBI includes a mining process that incentivizes the users. The incentive process is done throughout the scanning process, where users perform proof of purchase for each scan. The name of Wabi refers to the Walimai organization and supports the "Walimai label," which is applied at a designated 'point of origin' along with the supply chain system. The registered products of the "Walimai system" consume WaBI tokens for their protection.

- TE-FOOD [110] is represented by one ecosystem that involves all partners of the food fabrication (Farmer, producer, transporter, and consumer) corresponding to successful farm-to-table food traceability. TE-FOOD fights against Food frauds and mistrustful supply chains. It introduces a utility token called TFD, blockchain protocol, smart contracts, and 1D/2D and RFID tools for identification purposes. Two types of Blockchain are involved in the progress: the public Ethereum blockchain used for the payment process with TFD token and a second private Blockchain used to store the transactional data. Therefore, supply chain organizations have two types of wallets: Ethereum network wallet, which can be used directly or through the TE-FOOD mobile application, and Transaction wallet on the private network, which the TE-FOOD mobile application can use.

- FarmaTrust [111] provides a solid cloud-based platform that aims to track pharmaceutical products via a supply chain that relies on digital systems to the physical pharmaceuticals. FarmaTrust is based on the Ethereum public Blockchain with a POA consensus algorithm to enhance the scalability. The API and blockchain layers are separated, and the database layer is based on MongoDB and Cassandra.

- BlockGrain [112] is a decentralized platform using Ethereum Blockchain for the agriculture supply chain. BlockGrain is structured into three main layers: public Blockchain, Private Blockchain, and applications. The main data, smart contracts, and transaction Agri tokens are located on the public Blockchain, while buyers utilize the private Blockchain to reduce the costs of both transactions and waiting time associated with a public blockchain. The Blockchains are managed through the applications Layer of the BlockGrain Platform.

- ZERO defects [113] is a DAG-based platform in order to track supply chain products. It is announced through a collaboration between Pickert (ISO certified company) and the IOTA Foundation. Each product is identified using its serial number, and all the data is safe, immutably stored, and accessible in the IOTA Tangle.
- Blockverify [114] is an anti-counterfeit Blockchain-based solution for luxury supply chain items. Blockverify constitutes the combination of Bitcoin and a permissioned Blockchain to store public and private information within the public and private ledgers successively. Each product tracked by Blockverify has a unique special tag along the supply chain, where the customer itself determines the transparency level.
- Chronicled [115] integrates smart tags and the Chronicled application to track the physical products and link them to the Blockchain using "identity inlays and tamper-evident cryptographic seals." The Smart Tag is a cryptographically secured chip containing details about the physical good linked with a private key.
- Everledger [116, 117] is specialized in protecting the integrity of diamond products using two Blockchain platforms. It uses the private Blockchain 'Hyperledger' and Ethereum public Blockchain to ensure the transaction history's immutability rather than scale up the system.

3.2 Discussion on DLT integration with the supply chain

Previously, we have mentioned various solutions targeting the IoT-based supply chain improvement integrated with Blockchain that enriches the system with trust, complete visibility, and traceability. Blockchain limitations are manifest to all of these projects, although their technologies and requirements vary markedly. These projects associate the Blockchain within their platforms to overwhelm the downsides and add value to the current DLT systems. In this section, we present a deep analysis of the current Blockchain limitations in the supply chain. Such limitations include high computing, storage size, and massive IoT data. We discuss the related challenges with reference to the on-chain and off-chain solutions, as shown in figure 3.6. Table 3.4 depicts the approaches' taxonomy to solve the DLT-based supply chain's challenges using tools based on the on-chain, off-chain, and application layers.

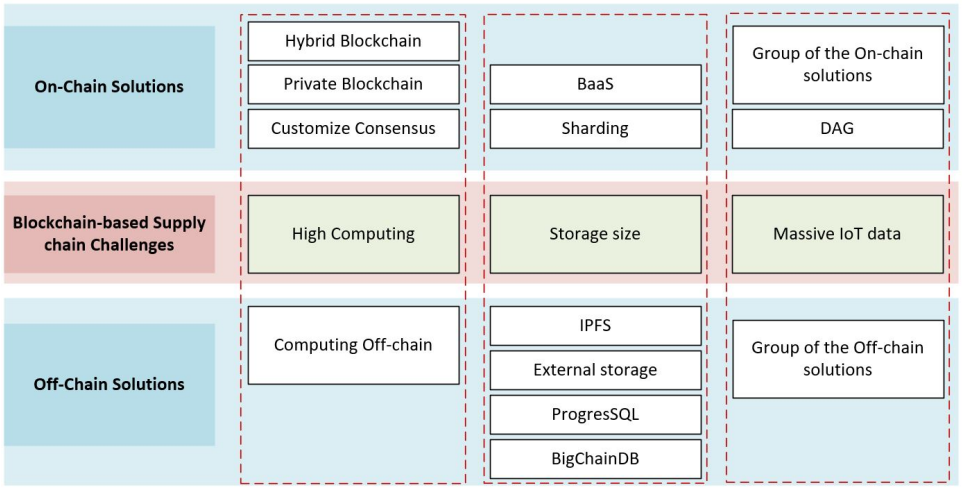


Fig. 3.6 On-chain/Off-chain solutions for the supply chain challenges

Layers	**Tool mechanism**		**Supply chain Projects**
On-chain	Modify Consensus algorithm		Waltonchain [100]
	Sharding technology		Vechain [101] (Reed-Solomon algorithm), ProductChain [118]
	Move to DAG platform		ZERO Defects [113], TradeMarkea [119]
	Cloud-based		FarmTrust [111]
	Transaction format		Vechain [101]
	IoT enhancement		WaltonChain [100], Ambrosus [102], Modum [103]
	Private/Consortium Blockchain		ProductChain [118]
	Multiple System	Side-chain	Waltonchain [100]
		Hybrid Blockchain	Modum [103]
		Multiple Blockchain Public/Private	WaltonChain [100], BlockGrain [112], Blockverify [114], Everledger [117]
Off-chain	IPFS		Ambrosus [102]
	ODN		OriginTrail [82]
	External Storage		ProductChain [118]
	PostgreSQL		Modum [103]
	BigChainDB		Feng [120]
Application	Web interface		Devery [121], Bext360 [122], Modum [103]

Table 3.4 Taxonomy of the supply chain DLT tools.

The on-chain solutions enhance the Blockchain components while all the transaction data stream on the P2P decentralized system. They are mainly focusing on enhancing the computing side to provide Blockchain scalability. The off-chain solutions focus on offloading part of the workload outside the Blockchain platform using centralized or decentralized systems. In a supply chain, the off-chain tool is proposed primarily within the DLT-based supply chain to reduce Blockchain's storage and speed up the transaction process.

3.2.1 Computing Challenges

The computing, which has the highest impact on the supply chain scalability, is concerned directly with the consensus algorithm type utilized in a Blockchain. In fact, there are many proposed consensus algorithms [123] within the on-chain solutions to enhance Blockchain performance. Tools such as private and hybrid Blockchain overcome the scalability issue by reducing the number of validated nodes. Ambrosus, for example, used these tools and introduced apollo Nodes with the relevant authority in its network to validate the transactions. Vechain utilizes the POA consensus algorithm to improve data circulation with around a 10k transaction rate per second. However, the private and hybrid Blockchains are not suitable platforms for the global supply chain. Another customized consensus algorithm called POST is a combination of different algorithms (POW, POS, POL) introduced by Waltonchain. POST is appropriate in a supply chain with one central Blockchain where its role is limited to Blockchains' management purpose. It is not designed to deal with huge transaction loads as its block confirmation time is about one minute, hindering IoT devices' proliferation. Besides, running part of the computing load on off-chain relieves the Blockchain process and enhances the overall performance.

3.2.2 Storage limitations

The on-chain ledger size is considered the significant challenge of any supply chain where most devices cannot hold such large data volume according to their limited resources. The ledger's data size should be considerably controlled from exceeding the limited size. The listed projects earnestly consider controlling the ledger's data size and propose several solutions to manage this concern.The below subsections discuss the available solutions.

3.2.2.1 Sharding as a solution for the ledger size

Sharding is one of the proposed solutions to manage the ledger size. In the literature, there are many sharding proposals (table 3.5). In the supply chain environment, the Vechain project

uses the sharding technique to distribute the ledger volume to many locations using the RS algorithm. Nevertheless, Sharing does not permanently solve the storage problem because all data is still stored on the Blockchain. It only distributes data to different places, further complicating the supply chain at a large scale.

3.2.2.2 BaaS as a solution for the ledger size

One of the on-chain solutions for scalability and ledger volume is to run a Blockchain in the cloud or use the Blockchain as a service "BaaS." The participants and the peripheral devices will be out of the computing and data storing tasks as both storage ledger, and computing charges will be offloaded on the cloud. Thus, when Blockchain runs on a Cloud, there is no need to utilize the peripheral device capacity, and there is no need to be fully synchronized. In addition, the edge computing facility over the cloud service enforces scalability, streamlines the data, and empowers IoT devices to exchange their information with low latency. The cloud computing solution behind BaaS facilitates access to a global shared pool of configurable computing resources such as storage services and applications [4]. The stakeholder's cooperation issue is a significant concern in which cloud computing can be considered the important solution [124]. The IoT applications mainly reside in cloud storage and are accessed remotely via mobile application-based running on smartphones or any other devices [125]. Thereby, the cloud improves real-time applications, saves time and cost, and enhances machine-to-machine (M2M) interactions.

3.2.2.3 Off-chain solutions to reduce ledger volume

Many solutions have been proposed to solve the Blockchain-based supply chain projects. Ambrosus project uses the well-know IPFS (Interplanetary File System) decentralized storage system to offload the massive data outside the Blockchain so that the cost and the ledger size are reduced. Nevertheless, IPFS is not secure since the IPFS files are accessible to anyone in the network. Also, IPFS is inflexible with corresponding data. Another distributed scenario introduced by OriginTrail called ODN which creates an independent decentralized platform to decentralize the transaction processes outside the Blockchain ledger. At the same time, ODN is managed by Blockchain smart contracts to ensure controlling the whole system's integrity. In this regard, all ODN nodes are controlled by Blockchain while offloading a large amount of data outside the DLT ledger. Besides, many other off-chain solutions could be tested within the supply chain.

3.2.2.4 IOTA snapshot as a solution to reduce ledger volume

IOTA introduced a local snapshot mechanism to reduce the size of the ledger on the node level. Local snapshot prunes old transactions from node' disk regularly, and the resulting balances are consolidated into a new genesis state. This state allows for the nodes to start over with an empty database. At the same time, nodes with good resources defined as Permanodes are excluded from the snapshot process, so they store the whole ledger volume. This mechanism is attractive for the IoT-based supply chain, where the devices' capacities are generally deficient.

3.2.2.5 Editable Blockchain as a future solution

Although cloud is considered a suitable place for large ledger size, some data are meaninglessly stored, such as records related to food after consumption. Wherefore, they must be removed. The editing block of a Blockchain ledger breaks the immutability rule of the new decentralization. Nevertheless, Editing blocks is necessary in many cases. Using Chameleon Hash Function [92] could help compress the ledger, but it is still not applied, neither as a pilot nor in production supply chain projects. Suppose the Blockchain becomes editable in the future without risking the integrity of the data. In that case, it will ease off the supply chain from a large amount of undesired/old data, thereby compressing the ledger size as either on-cloud or on local nodes.

3.2.3 IoT limitations

The integration of Blockchain with the IoT technologies brings many added values for the IoT systems. Blockchain helps address some of the IoT drawbacks as it provides a shared distributed database and adds another security layer to prevent many kinds of attacks. However, massive amounts of data produced from large IoT devices can bottleneck an IoT system, resulting in poor quality of service (QoS) [126]. The main challenges of integrating IoT systems on the Blockchain are:

- Computing resources: The high computational power required to run Blockchain algorithms has slowed down the advancement of these technology-based applications on resource-constrained devices [127].
- Real-time data and throughput issue: Blockchain throughput is limited due to its cryptographic security protocol and consensus mechanisms. In time, the IoT devices

continuously stream data, resulting in high concurrency [128]. Therefore, the real challenge is to increase Blockchain's throughput to meet the need for frequent transactions in IoT systems.

- Handling massive data size: Participants in the Blockchain network should maintain a local copy of the whole ledger in order to validate each block. Although this mechanism improves efficiency, solves the bottleneck problem, and removes the need for trusted third parties, the management of IoT data on the Blockchain puts a burden on the IoT devices' storage space.

3.2.4 Existing solutions outside the supply chain

Besides the improvements/proposals of the above Blockchain-based supply chain projects, several solutions outside the supply chain environment can help achieve scalability if applied to the supply chain. These solutions can be widely used within the public Blockchain, which is the most preferable for the supply chain. In addition, these solutions are categorized into on-chain and off-chain solutions. Table 3.5, which is inspired from [56], presents the available scalability involved within different approaches. Based on their testing, they have a significant effect on Blockchain performance. The size of the block is one of the major factors since it is related to the number of transactions in a block. The larger the size of the block, the more transactions it receives, leading to high throughput. However, increasing the block size leads to slow propagation and forks in the network. Another solution is represented by involving different sharding technologies to mitigate the ledger volume. Therefore, different sharding technology [129, 56] are surveyed based on the various consensus algorithms.

Layers	Blockchain solutions	Project	Role and Benefits	Limitations
On-Chain	Block size modification	Litecoin [130]	Handle large Tx number	Many orphaned blocks
			The time block is 2.5 second	
			Throughput is 56 TPS	
		SegWit (Segregated Witness) [131]	Remove part of the Transactions	Complexity in the management of the blocks
			Divide the block into two: base block and extended block	
		Bitcoin Cash [132]	Increase the block to 32 MB	Large block brings back the centralization
		Jidar [133]	The node stores the Txs needed only	Not all the data are located on the node disk
			keeps Merkle tree image of the whole block	
	Sharding Based on PoW and PBFT	Elastico [83]	Designed for public blockchains	Security challenge
			Tolerate one-fourth fraction of byzantine faults	Throughput 40 TPS
		Omniledger [134]	Use bias resistant randomness protocol	Resilient only 25% to Byzantine faults
		Rapid Chain [86]	Kademlia routing algorithm	Tolerate up to 33% of malicious/faulty
			Throughput 7380 TPS	Partitioning attack
		Ostraka [135]	Shards are the nodes themselves	Smart contract limitation
			Multiple inter/intra shard communication techniques are used to increase the bandwidth	
			Throughput 400 kTPS	
	Sharding Based on PoS and PBFT	Zilliqa [136]	Execute parallel Txs	Susceptible to single shard takeover attacks
			Throughput is 2828 TPS	
		Harmony [137]	Supports state sharding	Throughput 500 TPS
		Ethereum Sharding 2.0 [138]	Executed in three phases: Beacon Chain, Shard Chain, and State Execution.	N/A
	Sharding Based on Consensus	Monoxide [**?**]	Linear scaling using asynchronous consensus zones	Asynchronous system hinders the overall data replication
			Independent zones, and each one is responsible for its data	Mining and transaction confirmation are limited to each zone
		Logos [139]	Use Axios delegated PBFT consensus algorithm	Throughput 2500 TPS
	DAG (alternate DLT platform)	NXT [140], Nano [141] Bytball [142], Inclusive [143], SPECTRE [144], PHANTOM [145], Conflux [146],Dagcoin [147]	Enable low-cost micropayments and High throughput	Need high traffic for its functioning
				Accumulation of unconfirmed Txs
				Smart contract challenges
Off-Chain	Computation	Truebit [148]	Outsource the computations to a verified third-party	Add complexity to the implementation
			Third-party called 'solver' is based on smart contract	
			Challenger is another third party to verify the work done by a solver.	
		Arbitrum [149]	Performs the verification of smart contract off-chain	
			Reducing Ethereum Gas Costs and Increasing Throughput	
	Cross-chain	Polkadot [49]	Network of many independent Blockchains	
		Cosmos [90]	Provide interoperability between different Blockchains	
			Achieve high scalability	

Table 3.5 Scalability solutions outside the supply chain

3.3 Conclusion of the analysis

This section briefs the analyses above and highlights the key components of the proposal in the next chapter. Table 3.6 depicts the tools solution for the Blockchain challenges in terms of the DLT requirements for the supply chain. Minimum computing and storage and feasible transaction requirements face many limitations of Blockchain structure, and in return, they have various tools to overcome these challenges. Based on the above study, many scenarios could be applied to reach a typical supply chain environment by combining different tools listed in Table 3.2. Some of these tools like sharding, off-chain tools, IoT involvement, and private/hybrid Blockchains serve particular supply chain cases. Other tools can commonly be used with different supply chains like BaaS, Editable Blockchain, and Blockchain core improvement. It is noteworthy that all supply chain projects focus on enhancing the Blockchain using the above tools while ignoring any alternative DLT platform presented as an "alter DLT system" tool.

Supply chain requirements	**Blockchain challenges**	**Tools**
Minimal Computing	Low Scalability Consensus mechanism Block structure IoT integration	Off-Chain BaaS Modify BC core Consortium/private BC Alter DLT system
Minimal Storage	Large ledger size IoT resource capacity	Sharding BaaS Off-Chain Editable BC
Feasible Transaction	High transaction fees	Consortium/private BC Alter DLT system

Table 3.6 Tools classification to address challenges and requirements

While many improvements over Blockchain are under development, testing, or creation, it is worth highlighting the alternative DLT DAG-based platform shown in Table 3.5. DAG

system, especially IOTA is designed to tackle many Blockchain drawbacks. Contrarily to Blockchain, IOTA fits all the supply chain requirements. It has no scalability problem and can involve a huge amount of participants in its network, including the IoT devices. Besides, IOTA reduces the ledger size using the snapshot technique, reduces the transaction fees to a negligible value, and introduces the ability to work offline features. Thus, we dig the IOTA DLT platform in our proposal that targets the typical supply chain. Nevertheless, the DAG-based projects are very few compared to the Blockchain-based ones. They are constrained by many drawbacks, like the need for a centralized coordinator (to be removed when the network becomes large enough) and the smart contract challenges. These limitations are not included in Blockchain. From an analysis point of view, amalgamating these two heterogeneous DLTs into one platform helps to attain more significant advantages [69] and advance the IoT integration within the decentralized supply chain.

3.4 Conclusion

This chapter overviews the existing DLT-based supply chain projects and details their technical side and their main contribution to enhancing the Blockchain platform, as mentioned in the thesis' second objective. The analysis depicts considerable efforts to address the Blockchain drawbacks and reveals different innovative tools used for this purpose. Nonetheless, Blockchain is not yet ready to fully meet typical supply chain requirements and replace centralized and traditional supply chains. We broaden the analysis to include other DLT projects that could somehow benefit the supply chain. The investigation findings lead to considering DAG-Based IOTA, the alternative of Blockchain, as the suitable DLT platform for the supply chain. IOTA can overcome the drawbacks of Blockchain while meeting the needs of the entire supply chain. However, IOTA has additional drawbacks that Blockchain does not have. In the following chapter, we will use "alter Blockchain system" and "BaaS" tools in our proposal to combine Blockchain and IOTA into a single platform suitable for the supply chain.

Chapter 4

DAG with Blockchain Architecture

4.1 Introduction

Based on the analysis and the state of the art of Blockchain and DAG efficiency in the supply chain, we suggest combining both DLT platforms into one end-to-end platform, fulfilling the central part of the thesis's third objective. The proposed platform comprises the DAG-based IOTA, which represents the front-end application, Blockchain represents the backend platform, and a connector part intermediates both DLT technologies. The proposed platform brings many benefits to the supply chain instead of using only one of the DLTs mentioned early. The decentralized applications (Dapps) run over the IOTA platform to achieve scalability so that the massive IoT integration becomes supportable. The incoming traffic is duplicated on the Blockchain backend side to be stored permanently on its ledger. Also, the proposed architecture allows the nodes to work offline and run the smart contracts on the Blockchain platform towards IoT nodes. These features advance decentralized systems, especially in complex IoT environments such as supply chains. Furthermore, this architecture eliminates the need to keep IoT nodes online since the data is always up and running on the backend. The following subsection details the motivations behind the new platform. Besides, the chapter includes experiments that validate the integration of Blockchain and DAG in the first stage and the smart contract feasibility in the second stage.

4.1.1 Proposal motivation

In addition to the aforementioned supply chain limitations and requirements, the following features and drawbacks of the two heterogeneous decentralized systems represent the technical motivations for our new platform proposal.

4.1.1.1 Blockchain Drawbacks

- IoT device capabilities: Blockchain relies mainly on their participants' resources to achieve the decentralized goal. Most IoT devices are constrained by their limited computing and storage resources, which hinder their integration with the Blockchain system.
- Block structure: All the transactional data that come at a specific time should be stored in the last open block. This block is available for a determined time, and then another block should close it and replace it, and so on. This block serialization process is incompatible with billions of integrated devices, leading to a performance issue with the vast IoT data.
- Mining and competition: Blockchain is based on reaching consensus among its active nodes, resulting in competition in the network. Many alternative consensus algorithms succeeded in reducing mining and the utilized powers. However, the way the Blockchain reaches the consensus requires inter-communications between the nodes, which is unsuitable for billions of IoT devices.
- High Transaction fees of Blockchain: The block structure, the mining process, the competition, and the transaction/block incentives elevate the cost per transaction. On the other side, the IoT devices' functionalities produce huge micropayments while interacting, leading to significant constraints with Blockchain utilization.

4.1.1.2 IOTA Features

- DAG structure: the DAG platform can process multiple transactions simultaneously. This parallel data processing fits with the vast IoT environment, so DAG can treat these incoming data without the need to put them in a specific block. This feature nominates IOTA as a scalable DLT for IoT-based systems.
- Iota low transaction fees: contrarily to Blockchain structure, the participants' nodes in IOTA perform local POW without competing with any other nodes. Thus, there is no mining or competition among participants. Such a method decreases the transaction cost to a nominal price and encourages proliferation of micropayment transactions.
- Ability to work offline: IOTA, which does not rely too much on timestamp transaction and block creation time, allows the node to create their transactions offline and register them when they come back online. Working offline is a good feature suitable for IoT devices such as sensors and data collectors with a bad or non-stable connection.

4.1.1.3 IOTA Drawbacks

- DAG-based smart contract issue: the DAG structure in nature encounters problems while applying smart contract. IOTA struggles nowadays to achieve smart contract the same way the Blockchain does. Still, many constraints in this subject. Such critical drawback prevent the IoT-based environment from applying IOTA for their underly platform.
- DAG security concern: IOTA platform should reach a considerable network size to be secure enough. It relies on third-party software to cover the security weakness until it becomes big enough. In an IoT-based business system, the security concern should be considered within a fully decentralized platform from the beginning, when the platform enters the service.

4.2 Proposal: DAG with Blockchain for supply chain

We propose a new decentralized architecture to achieve storage independence, enhance scalability, and provide data sustainability and availability at a time. The system is composed of the Blockchain platform, the tangle-based platform, and the independent connectors that separate the two platforms, as shown in Figure 4.1.

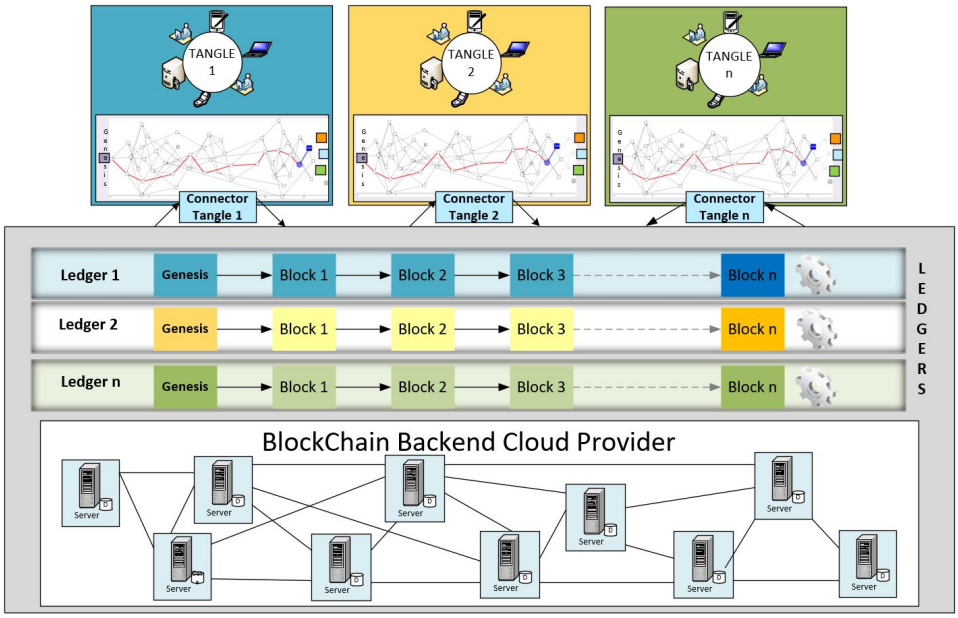


Fig. 4.1 Proposal structure

The Blockchain platform is installed in the backend, representing the permanent ledger and data storage. The backend can be deployed in the cloud to provide better connectivity to the frontend IOTA applications. The Blockchain creates multiple ledgers where each one is referred to a supply chain application. Ledgers in our backend platform play the role of data storage and backup in the first stage. In the second stage, ledgers have several functions regarding security, privacy, and smart contract.

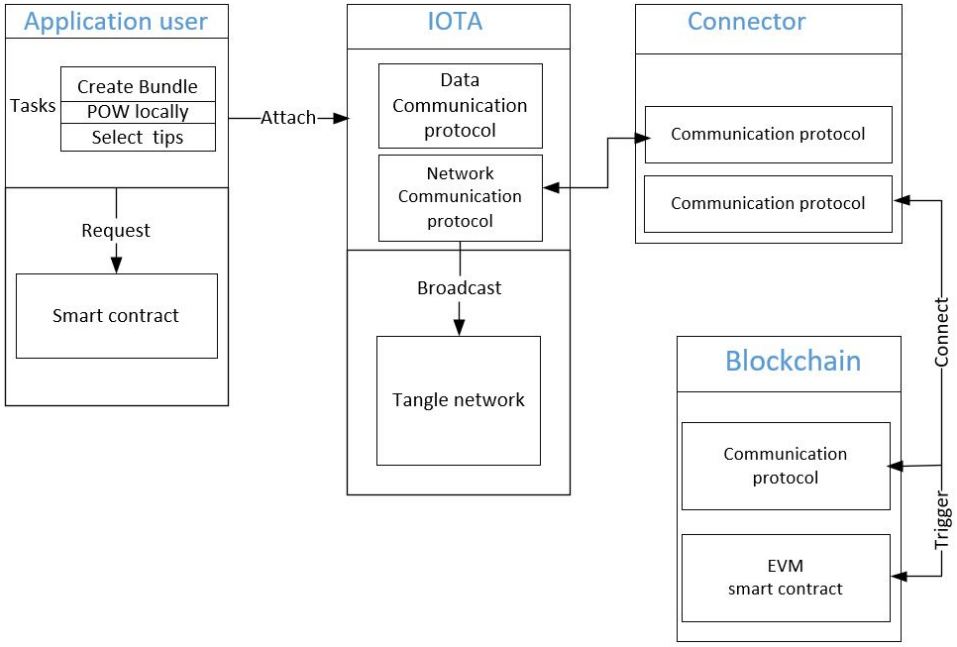


Fig. 4.2 Functional architecture

The second main platform is composed of several independent tangle-based applications distributed along with the IOTA applications. Each application has its own tangle-based ledger. The connector can communicate with two ledgers and passes the IOTA transactions towards Blockchain ledger, the permanent destination of the data. From a high-level view, we propose combining two heterogenic DLT types and integrating each other implicitly to provide a single end-to-end solution. Figure 4.2 represents the functional architecture of the proposal where users will generally be dealing with one DLT platform, while the second platform will be embedded within the provided solution via a distributed connector.

Figures 4.3 and 4.4 detail the proposal mechanism of how a Tangle-based node issues a transaction. In the Blockchainless Tangle, the node should prepare its transaction inside a new bundle (data, recipient address, transactions details, etc.), sign it, select/validate two previous transactions and perform POW locally. Thereafter, the nodes attaches the new bundle of transactions to the Tangle to be broadcasted to the remaining nodes. The bundle

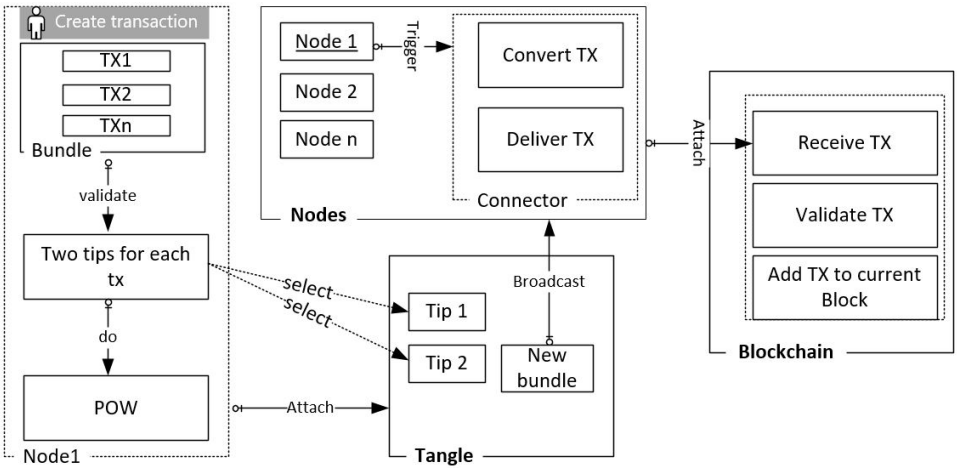


Fig. 4.3 Detailed Proposal mechanism of issuing transactions

is still invalidated until some node selects and validates it. A connector that placed next to IOTA node receives the new bundle to converts it into Blockchain form and deliver it to the Blockchain nodes. Once received, the transaction is subjected to further verification by these nodes and stored permanently in the Blockchain ledger. In the below three subsections, we present the three proposal components.

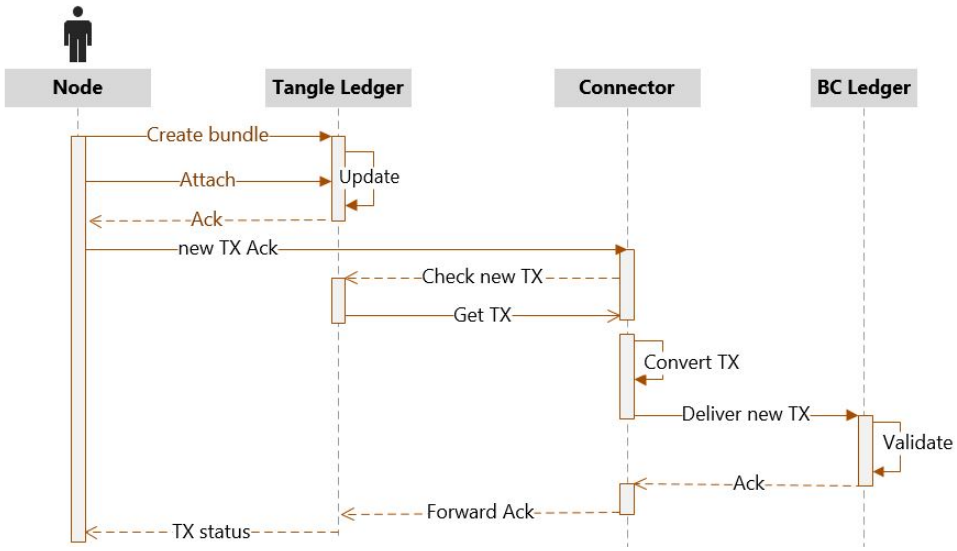


Fig. 4.4 Sequence diagram of the proposal

4.2.1 FrontEnd: Tangle-Based Application

The Tangle approach improves the IoT devices' affinity with the decentralization concept. It empowers nodes to save energy since they are not involved in creating blocks and mining. Furthermore, the Tangle considers the various type of IoT devices and categorizes them into full and light nodes. Thereby, the light node with limited resource can be directly connected to a full node to perform its computing tasks. Besides, Tangle empowers the IoT devices to work offline in case of emergency and network disconnection; therefore, the issued transactions must be attached to the Tangle, later on, to be validated by the peers. Allowing nodes to issue offline transactions is quite necessary for IoT society since most of these devices span many geolocations with unstable network connectivity. These new DLT features motivate IoT technology proliferation and reduce faulty incidents during issuing transactions in a massive supply chain environment. It is worth mentioning that the supply chain partners have options to build their applications on top of private or public Tangle DLT systems. Subsequently, all partners' data are stored in one Blockchain ledger and treated as one supply chain database.

4.2.2 BackEnd: Blockchain Platform

Blockchain is employed in the backend of our architecture to store the incoming IoT data permanently. It is a managed Blockchain platform allowing the clients to build their apps and services effortlessly with built-in connection systems and maintenance support. Our architecture clients use Blockchain ledger to store their incoming data from the Tangle-based applications. Usually, the structure of a BaaS allows clients to benefit from the DLT services without being involved in the Blockchain tasks like storage, computing, mining, etc. Thereby, a participant in a Tangle application is not engaged directly in the Blockchain platform. The Blockchain nodes are independent of Tangle nodes and the number of IoT devices participating in a Tangle-based application. The number of arrival transactions is the most crucial parameter that should be considered in such combination. Consequently, the best practice is to run the BaaS in the cloud with edge computing availability to facilitate the connectivity between Tangle nodes and Blockchain [88] and to avoid latency during transaction propagation. Many Blockchain providers nowadays provide BaaS, such as Microsoft Azure, IBM, Hyperledger Fabric, and others. Mainly, they are running on the cloud to provide both public and consortium Blockchain services. Accordingly, the application owner must subscribe to one of these providers to bind its Tangle-based application with the Blockchain system. Based on our experiment results, it is worth mentioning that any type of Blockchain can be integrated with a Tangle-based application.

4.2.3 Connector

With the aim of binding Tangle and Blockchain DLT systems into one platform, a decentralized middleware connector is developed and installed on each Tangle node. The connector's role is to translate the transactions types from Tangle into Blockchain and vice versa. The connector is a separate decentralized application triggered each time a node wishes to attach transaction on the Tangle. Once the transaction is attached to the Tangle, the node's connector deals with it to be transferred to the Blockchain side and get into the Blockchain ledger.

Generally, the software connector is the first-class element of the software architecture [150], defined by interactions between different components' systems. The interacted component services are categorized under communication, coordination, conversion, and facilities. Each category includes many connector types: procedure call, event, data access, linkage, stream, arbitrator, adapter, and distributor. Connectors, in general, have different roles: middleware, interaction modeling, architectural styles, and distributed systems. In a heterogeneous system, the connector tends to be the adapter type, as it supports interaction between different components that are not designed for interoperation. It involves interaction protocols to match the different parties and mitigate the gap between the different communication channels. The process is done through conversion tasks to synchronize the parties.

Concerning the connector types listed above, our proposed connector is classified under adapter type that relies on the conversion process to convert Tangle-based transactions to be readable by the Blockchain platform. The connector is oriented to implicitly bridge Tangle and Blockchain. It is logically situated between Tangle and Blockchain ledgers. Physically, it can either reside on Blockchain or Tangle nodes. Also, it can be installed on independent nodes and behaves as distributed connector system. The records of a given Tangle-based application are propagated and replicated to a Blockchain ledger. In other words, each record will be stored twice within the two different DLT ledgers. Transactions validated by Tangle nodes and recorded within the Tangle ledger are immediately forwarded to the nearest connector. The received transaction will be submitted to exact format change to fit with Blockchain architecture.

4.3 Architecture of the connector

There are two main ways to construct the connector: we either agree on a uniform transaction format [48] to be used by both DLTs or build a separate connector that plays the role of translator between DLTs. However, using a uniform transaction format adds many constraints

to the system. Due to various application data types, one transaction form will not fit all DLT requirements involved at any given time. Therefore, we adopt translating transactions option, and we use the IOTA javascript package named "@iota/transaction-converter" to achieve the translation. This package represents the methods used for calculating transaction hashes and converting transaction objects to transaction trytes and vice versa. The Tangle-based transactions are subjected to the IOTA function "asTransactionObject" to translate them to "object type" that Blockchain is readable. In the opposite sense, "asTransactionTrytes" function is employed to translate object transactions of Blockchain directed to the Tangle.

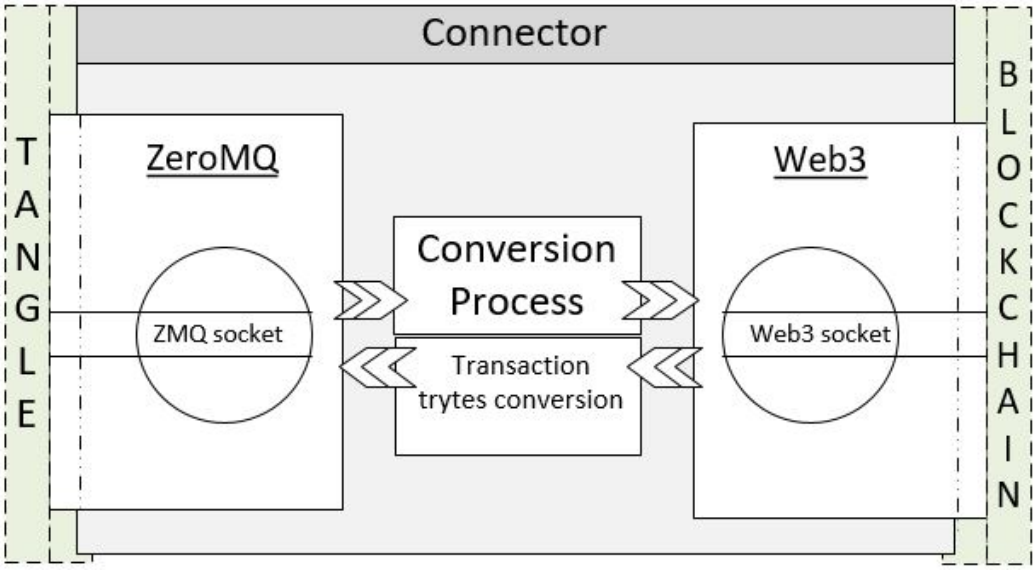


Fig. 4.5 Connector's Architecture

The proposed connector comprises two types of communication channels, zeroMQ (zero message queuing) and Ethereum web3, as illustrated in figure 4.5. Unlike the communication protocols such as TCP, UDP, and Websocket, the message queuing approach provides processing data in a queue, either in FIFO (first in first out) or according to a priority policy. The main idea is that the data is added to a queue system and executed whenever the caller is ready. ZeroMQ has crucial roles in large-scale distributed systems and enables asynchronous communication [151]. Compared to the single-threaded and multi-threaded queue approaches, ZeroMQ can handle the largest number of users, provides immunity against distributed denial of service attack (DDoS), and is scalable [151]. Additionally, it enables working offline with the guarantee that no single record will be lost. This feature enforces the built-in working offline of a DAG-based environment and adds more reliability and flexibility to the system.

Besides, the Blockchain transactions exploit the ZeroMQ feature of being able to work offline. For example, in a non-stable IoT system, a disconnected node that has triggered a smart contract payment in Blockchain can resume its task when it goes back online without losing the initiated transaction.

On the other side, Web3 is a set of communication protocols that allows Blockchain to distribute peer-to-peer transactions without intermediaries. It can interact with Ethereum nodes through HTTP or IPC connections. Using the web3 JavaScript libraries, the connector can interact with smart contracts and retrieve many information such as user accounts, send transactions, and more.

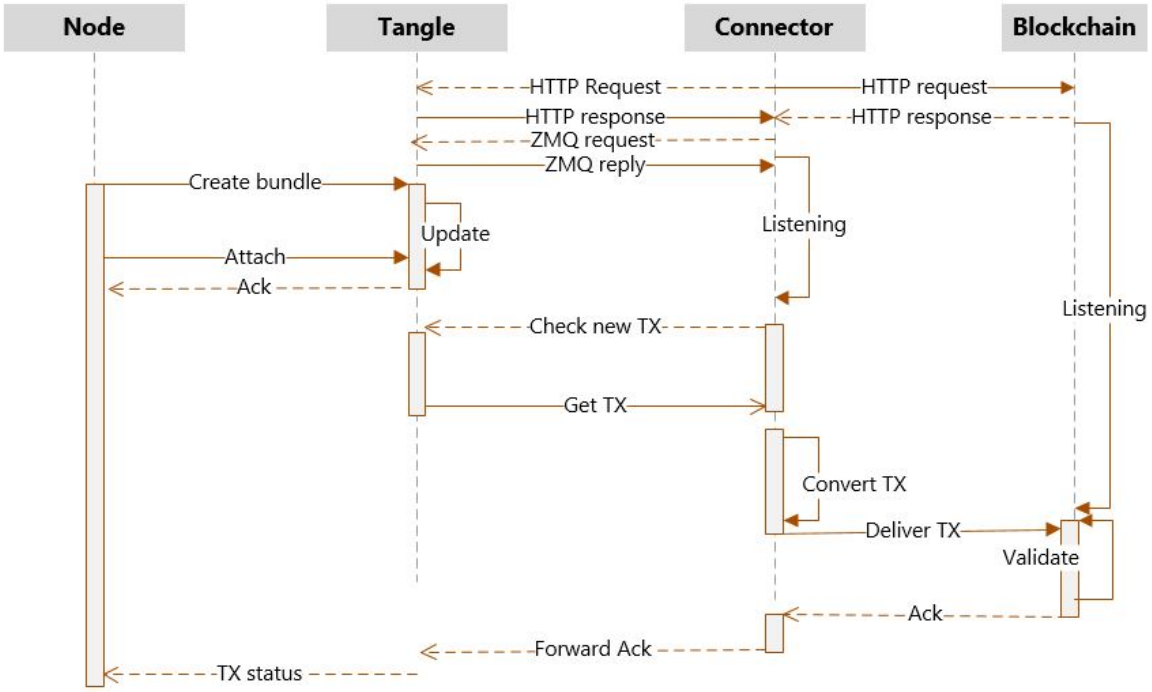


Fig. 4.6 Proposed sequence diagram

Figure 4.6 details the mechanism of issuing transactions by the Tangle-based node and mirroring them to the Blockchain ledger. The connector establishes its HTTP connections with both DLTs' nodes at the initial stage. It then establishes a TCP connection with the Tangle nodes for the ZMQ protocol. These connections put the connector in listening mode for both DLTs. The IOTA full node prepares its bundle of transactions (signature, validates two previous transactions, and POW locally) and attaches it to the Tangle. The connector receives the new transaction through the ZMQ protocol and immediately converts it into Blockchain format. Blockchain nodes listening to the web3 connector interface receive the new transaction to validate and store it in the last block.

The designed connector's primary role is to unify Blockchain and Tangle into one platform suitable for large environments. In addition, it could be used in open collaboration among different DLTs to achieve interoperability. For example, a Dapp Ethereum can communicate with one of the Tangle applications through its connectors. The guest Blockchain benefits from mirroring their transactions with the Tangle application to the main Blockchain. Achieving this kind of interoperability requires adding new connection parameters for the guest DLT similar to the existing ones.

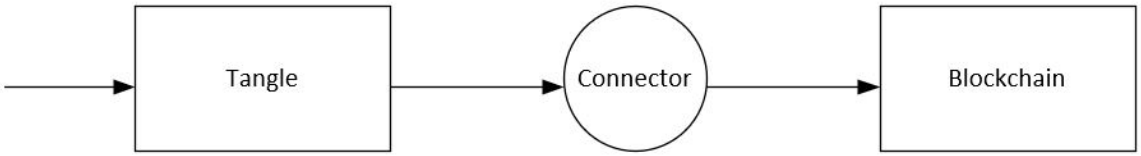
Each Tangle application has its group of connectors, which are independent of the other applications. Connectors are distributed on several nodes alongside the Tangle nodes areas. The connectors can run on top of a private Tangle ledger to guarantee its security and transaction propagation speed.

4.4 Enable Smart Contract

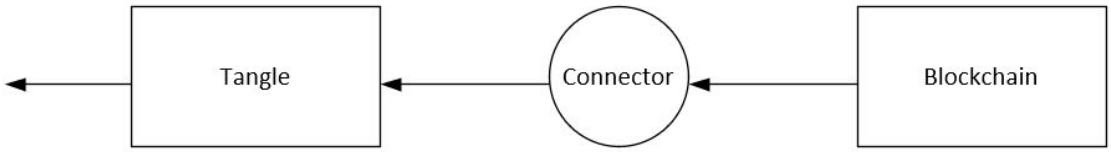
The smart contract is an executable program that should be deployed on the Blockchain level and running on top of its platform. Generally, a Blockchain-based node triggers the deployed smart contract directly on the Blockchain to fulfill its intended objectives and conditions. The smart contracts are broadcasted similar to regular transactions, validated by the participant nodes, and stored on the Blockchain ledger. In our proposal, since IOTA has limitations with smart contracts, they should be deployed and stored on the Blockchain and executed on the Tangle. There are two main challenges in this implementation.

The first challenge is that our connector streams the transactions from IOTA towards Blockchain only, as illustrated in figure 4.7 . The second challenge is the Tangle-based nodes have no direct connectivity to the Blockchain. Thus, it is required to upgrade the connector to be running on the opposite side, from Blockchain toward IOTA, and translate the smart contract transactions into tryte format.

We go with two main approaches to run the smart contract on The Blockchain while the IOTA nodes request it. The first approach represents most of the nodes located behind the Tangle without access to the Blockchain. We create an API function parallel to the connector includes the smart contract code. As illustrated in figure 4.8, the normal node calls the API to trigger the smart contract to be executed on the Blockchain. The API then translates the smart contract result into tryte format and sends it back to the Tangle then to the initiator node. At this point, the Tangle re-sends the smart contract result to the Blockchain for permanent registration.



(a) Normal direction



(b) Smart contract direction

Fig. 4.7 Normal direction versus smart contract direction: the two different directions of *a* and *b* illustrates the next challenge of running smart contract in our proposal, which requires additional developments in order to reply to the smart contract requirements.

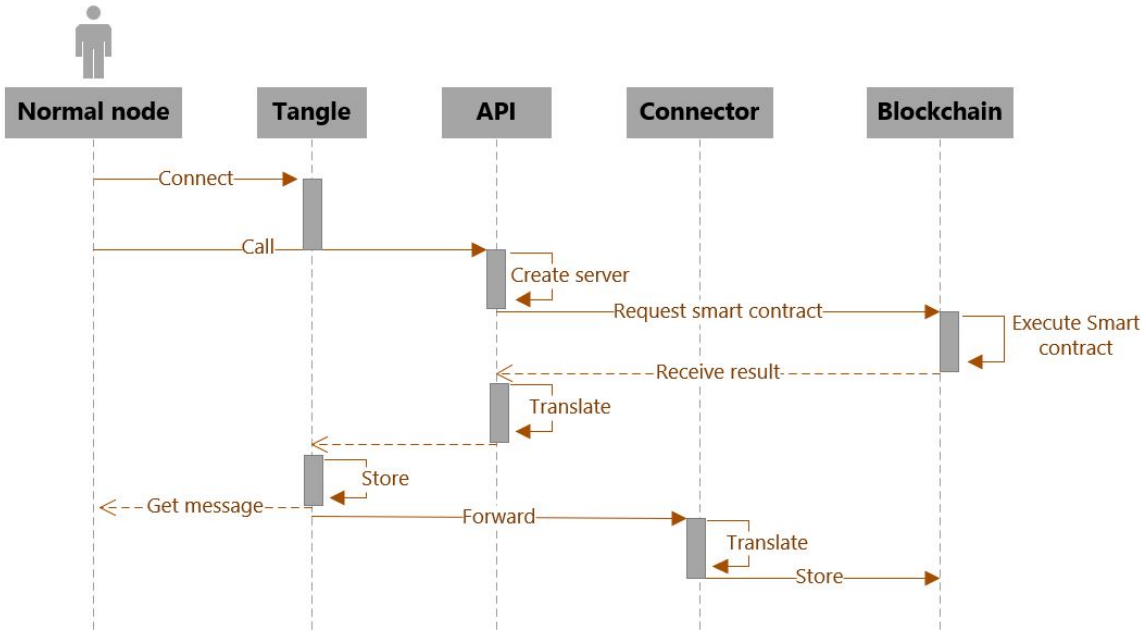


Fig. 4.8 Normal node calls for smart contract

In the second approach, we assume the presence of a supernode that has direct connectivity to the Blockchain and is located on the same level as the connector, as illustrated in figure 4.9. In this case, the node triggers the smart contract directly on the Blockchain and forwards the result back to the Tangle. The smart contract transaction will be stored on the Tangle

after being transformed to tryte format via the superuser. The connector will then receive it and register it in the Blockchain ledger.

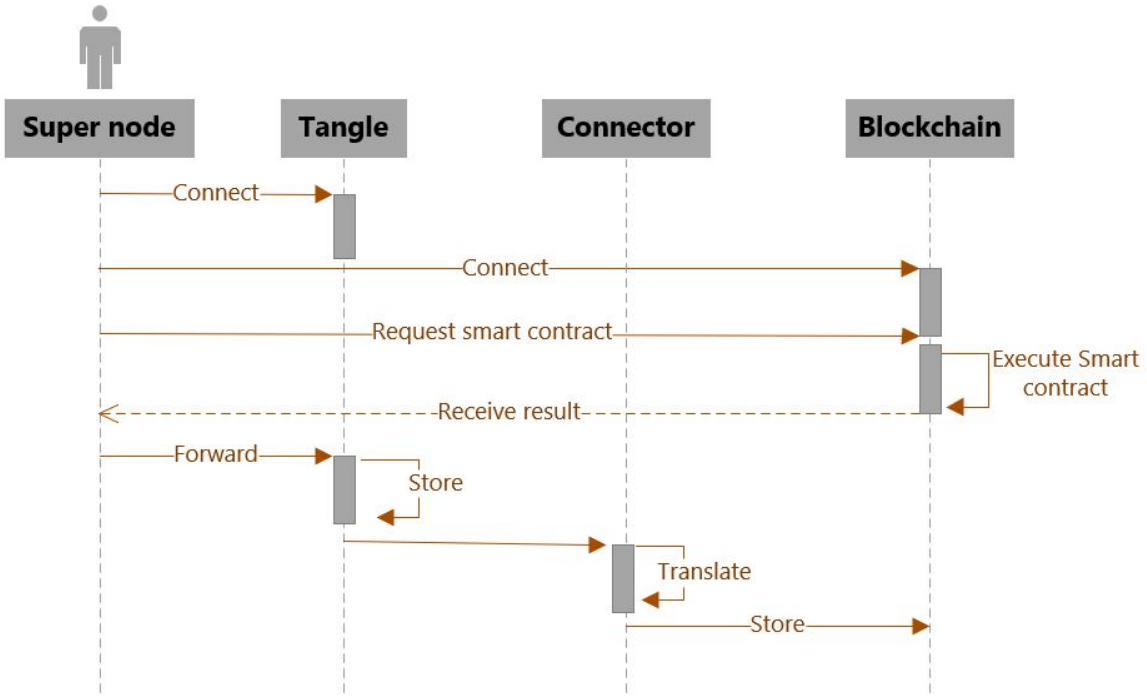


Fig. 4.9 Super node calls for smart contract

4.4.1 End to end Smart Contract

In the first phase of our architecture, we verified the feasibility of connecting the two intended heterogenous DLTs, Blockchain and DAG. Nevertheless, the proposed connector, in its current situation is not ready to manage the whole data flow in a supply chain, especially when it comes to smart contract utilization. Moreover, the distribution of the connector nodes along the DAG network requires involving the connector in parsing transactions to add more reliability to the proposed platform. Thus, we adapt the connector to rely mainly on the smart contract in sending and receiving transactions.

In this subsection, we continue to promote smart contract working better in the DAG-Blockchain environment through engaging the DAG-based client and the intermediate connector at the core of smart contract initiation. This is a new approach with the objective to avoid using the API call and enable the end-to-end smart contract from the IOTA client to Blockchain through the connector directly. This is done by upgrading the connector to have three new main functions. First, it can send the data flow on the inverse side from Blockchain toward DAG. The second connector function is represented by its ability to parse

the DAG request types and distinguish between the different smart contract functions and forward the exact requests to the Blockchain. The third function is to monitor and explore the executed smart contract results before sending them to the initiator node. Figure 4.10 represents a sequence diagram of a DAG node that triggers a smart contract. It prepares the request in a bundle and attaches it to the tangle. The tangle receives the request as a normal transaction in the tryte format. The connector detects the new transactions and pulls them immediately. Once detected, the connector investigates the data type and in this case, it infers the smart contract transaction and relays it to the intended function, and sends the update request to the Blockchain. The latter triggers the smart contract in question and executes the required functions and the results are registered within the Blockchain ledger. At this stage, the connector monitors the smart contract results and translates them into DAG format, and sends them back to be registered in the tangle. Lastly, the initiator node receives the result.

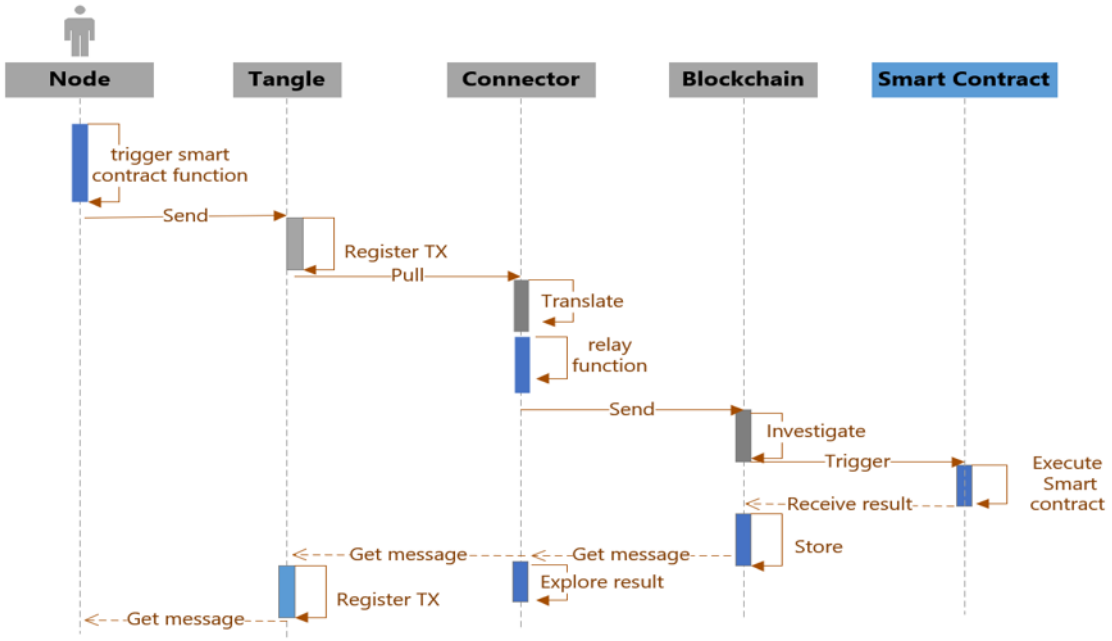


Fig. 4.10 Updated connector: end to end smart contract

4.5 Proposal benefits

Involving IOTA in the frontend applications ensures the system's high scalability and nominal transaction fees features. Besides, the benefits of integrating Blockchain and IOTA are remarkable:

- Involve the maximum number of IoT devices directly into the decentralization plat-

forms with minimum computing and data storing tasks. Also, the number of Tangle nodes is independent of Blockchain nodes.

- Data are recorded on two ledgers. IOTA ledger or the Tangle conserves recent records and snapshots (delete the old ones), while the Blockchain ledger stores the entire records.
- Data storage becomes of no concern regarding availability and physical location since it is doubled and distributed throughout the Blockchain ledger.
- Participants are not relying hardly on each other to execute queries since they have two different data sources, which adds flexibility to the Tangle nodes.
- The disconnected IoT nodes can work offline, initiate transactions and be broadcasted whenever they go back online.
- The smart contract will run on the IOTA environment while initiated and stored on the Blockchain.

4.6 Experiments: DLTs combination

As illustrated in the figure 4.11, we deployed three virtual machines to simulate the connector and test its functionality among DLTs. On the Linux-based VM1, two private IOTA instances were installed and configured to share the same Tangle ledger. Each IOTA instance runs through a configuration file (*.ini*) that includes a UDP port for Tangle inter-communication, zmq port, and other parameters related to the Tangle structure. The Ethereum Geth node is installed on VM3. The Genesis and all the Blockchain transactions are stored locally on the VM3 disk. On VM2, the connector is installed as a javascript program that includes all required IOTA, ZMQ, and web3 libraries. We create a NodeJS-based application to generate random values towards Tangle 2. Both Tangle 1 and 2 replicate data instantly after being verified and attached to the ledger. The connector is linked to Tangle 1 through HTTP to provide connectivity and through TCP to listen to the data traffic by ZMQ port. On the other side, it is connected to the Geth node through HTTP.

The connector code includes the below different javascript libraries that allow connecting both DLTs:

```
const sender=require('dgram');
const Iota = require('@iota/core');
```

```
const Extract = require('@iota/extract-json');
let zmq = require('zeromq');
let sock = zmq.socket('sub');
const txconverter= require('@iota/transaction-converter');
const converter=require('@iota/converter');
const fs =require('fs');
var Web3 = require('web3');
var Promise = require('promise');
```

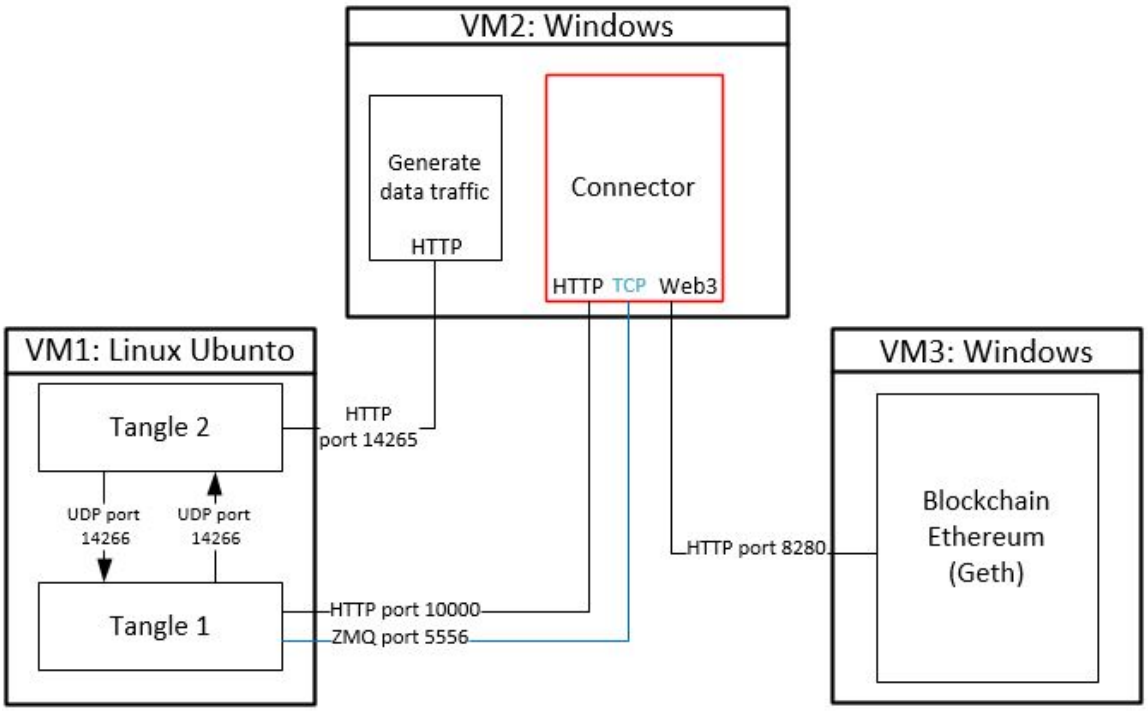


Fig. 4.11 Implementation bloc scheme

below is the function used to mirror the transaction in the Blockchain:

```
const txobj = txconverter.asTransactionObject(data[]);
const writtable_data=JSON.stringify(txobj,null,4);
```

The results of different tests show the flexibility to merge both DLTs using ZMQ protocol that enriches the new platform with reliability and enforces the offline working feature.

4.6.1 Smart Contract Implementation

The test environment is composed of the Ethereum Remix web with its plugin named Remixd and the Ethereum wallet called Mist, as shown in the figure 4.12. Remix web is used to develop the smart contract code and interact with the Blockchain. It can work with Web3 objects and can send directly to the "Mist" application. Remix web is typically the best-used application for testing contracts [152]. The Remix would be replaced by a standard EVM (Ethereum Virtual Machine) in a real environment. In our test, Remixd is installed and activated on the Geth node to be in listening mode through port 65520 to receive the smart contract and transfer it to the wallet "Mist." Afterward, Remix web application is connected to the local Geth node via Remixd plugin.

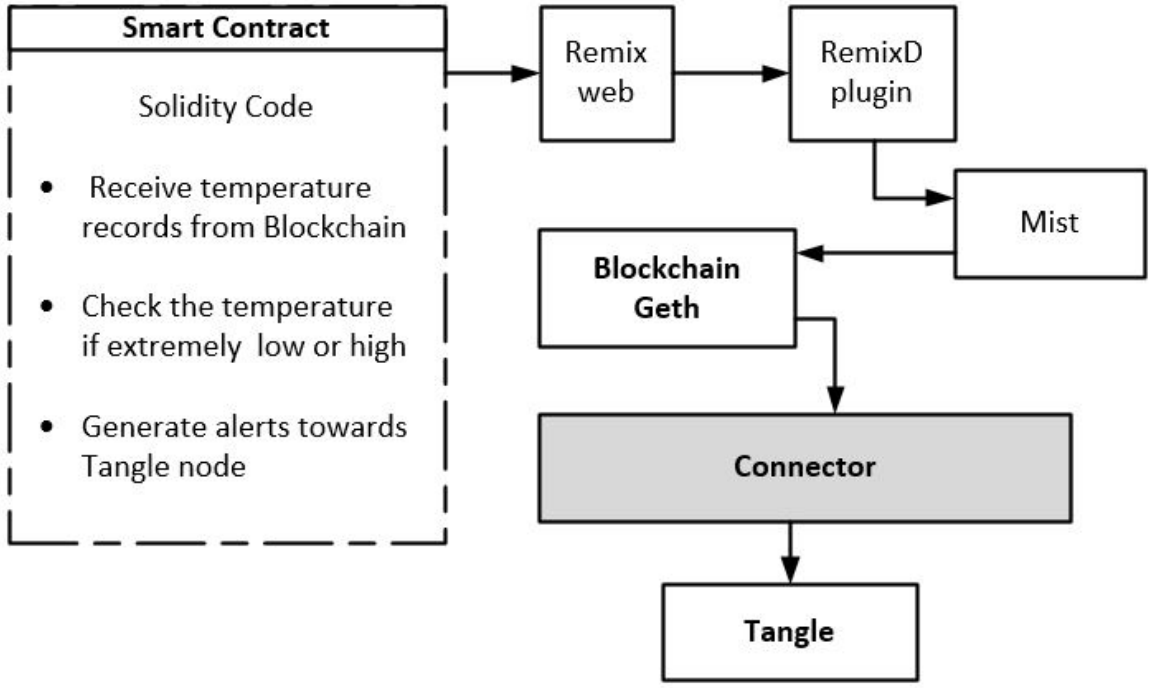


Fig. 4.12 Smart contract implementation

To check the doability of running smart contracts inside IOTA, we simulate two different experiments of the aforementioned approaches. The first experiment validates the scenario when a super node is located at the same connector level, connecting to Tangle and Blockchain. In this scenario, the node can trigger the smart contract directly via Blockchain EVM and transfer it back to the connector. The latter converts it into tryte format and attaches it to the Tangle. Again, the smart contract results will be forwarded as a simple transaction to the Blockchain ledger via the regular connector. In the second experiment, we treat the

normal scenario where Tangle-based node triggers smart contracts while having no direct connectivity to the Blockchain. This scenario simulates the majority of the Tangle-based nodes which are connecting to their Tangle only. A connector REST API is created to collect all the smart contracts deployed on the Blockchain to achieve this scenario. Thus, the node calls the API, which has its specific smart contract, and the latter executes it on the Blockchain level. Therefore, in detail, the request will pass and be attached firstly inside the Tangle, the connector receives and converts it into Blockchain format immediately, and forward to Blockchain EVM (or Remix) for execution. In the final stage, the results will go back to the nodes through the connector and be transferred to the Blockchain for registration.

In our second experiment related to the end-to-end smart contracts, we added two main functions to the initial connector, which are specialized in delivering transactions from Blockchain to Tangle and exploring ongoing/outgoing transactions. We define a new smart contract on the Blockchain with three functions: login(), store(), and get() in order to test their functionality from the IOTA client side. The upgraded connector has the ability to verify the incoming data type and which smart contract function(s) is triggered by the IOTA client and thus it forwards the exact request to the Blockchain. in the opposite side when the data is treated by the smart contract, the connector explores the returned smart contract results before transforming them into tryte format and delivers them to the requestor node. Parsing smart contract data on the connector level will be further developed in future work.

4.7 Conclusion

This chapter addresses the solution that is the center of the thesis's objective by establishing a platform that facilitates the integration of IoT-based supply chains with the Distributed technology. The proposed solution combines Blockchain and IOTA technologies into one platform where the decentralized applications can be installed in the Tangle, the frontend component. In the backend, the Blockchain is installed to mirror and store the data permanently. In the middleware, a connector is responsible for managing the Tangle traffic towards Blockchain. We highlight the connector component and detail its architecture and implementation. The experiments show that the connector's efficiency in connecting both DLTs allows us to integrate many IoT devices and enable the smart contract on the DAG side. Also, we reap other features such as high scalability, the ability to work offline, and low transaction fees. In vast incoming data, three parameters are responsible for tackling the system stability: the buffering feature of IOTA including ZMQ protocol, the number of distributed connectors, and the Blockchain computing mechanism, which is represented

mainly by the consensus algorithm. To further enhance the proposed solution of the third thesis objective , we investigate in the next chapter how low-resources IoT devices will interact with the DAG-based application to validate and attach their transactions to the Tangle.

Chapter 5

IOTA Computing Resource Allocation

5.1 Introduction

In the previous chapter, we proposed a new decentralized architecture with the Blockchain platform, the tangle-based platform, and the connectors between the two platforms. This chapter aims to enhance the proposed platform of the thesis's third objective in order to reach a highly performed DLT environment. The DAG-based IOTA platform consists mainly of various IoT devices, PCs, and servers distinguished by their hardware resources. IOTA categorizes its network participants into full and light nodes. The full node stores the IOTA ledger, computes transactions and attaches them to the Tangle directly. The light node is a device with low resources that requires utilizing full node resources to validate and attach its transaction to the Tangle. Hence, an efficient mechanism within the IOTA platform to allocate full nodes' resources is required. In this chapter, we propose a resource allocation mechanism to allocate the full nodes' resources to the light node while maintaining a load balancing. Such proposal is motivated by the following points:

- A light node is not directly connected to the Tangle; instead, it is connected to a full node. Light nodes consume the full node's resources arbitrarily to validate and attach their transactions to the tangle [69].
- The light nodes connections are not distributed fairly between full nodes. It happens that a full node has a high number of linked connections than others. Thus, it performs huge computing tasks while other full nodes are in idle state, leading to a performance issue during the peak time;

. The established connection between light and full node is unstable since the latter is not replicated, and it is not guaranteed to be online all the time. This type of connection is considered as a single point of failure.

Therefore, an efficient mechanism is required to allocate the full nodes' resources with load balancing. This chapter proposes a resource allocation scheme to fairly redistribute the decentralized computing loads between the IOTA full nodes. The target is to balance the computing tasks among all full nodes. This can be achieved by the collaboration between the nodes to maintain the maximum system performance.

5.1.1 Related Work

In the context of IoT, few nodes with high capacity can perform more transactions quickly. However, many devices with poor computing resources may not be capable of performing the POW difficulty. The root cause refers to the POW difficulty is fix for all nodes. Reducing the POW difficulty would help the small devices, but it undoubtedly leads to spam issues and network congestion. To avoid such circumstances and push full nodes to issue transactions fairly, IOTA introduces recently the adaptive POW [153] in the coordicide [40]. The adaptive PoW algorithm allows all nodes to issue transactions while penalizing any spamming actions. IOTA defines three new parameters on each node: basic difficulty, adaptive rate, and the number of transactions. The basic difficulty represents the threshold difficulty level that fits with any small device capacity. The adaptive rate is calculated based on *mana* owned by the node [40] and the number of transactions which is issued by this node within a time w. The new difficulty of each node equal the basic difficulty plus the adaptive rate multiplied by the number of issued transactions within a time interval w. Thus, the more a node issues transactions, the more its difficulty increases, and the allowed number of transactions is adjusted to be more complex and vice versa. The main advantage of such an algorithm is illustrated by empowering the low-resource devices to issue transactions with low difficulty. They participate directly in the main Tangle network. The algorithm allows different levels of POW difficulties to run upon various devices' specs. These devices must respect a margin of issued transactions number that end up with load balancing the computing resources. From our point of view, allowing low POW in some participant nodes is not the best practice or ideal solution as it reduces the Tangle's security. Our proposal hits almost the same goal of balancing the transactions load on each neighbor list while keeping the same POW difficulty level.

5.2 Resource Allocation Proposal

IOTA network consists mainly of various IoT devices, PCs, and servers distinguished by their hardware resources, including computing power and storage capacities. IOTA depends on these resources to run the platform with considerable performance. Therefore, IOTA categorizes the devices participating in the network into full and light nodes. The full node stores the IOTA ledger (Tangle), computes transactions and attaches them to the Tangle directly. The light node is a device with low resources linked indirectly to the Tangle through any active full node. The light nodes randomly try to select their full nodes. As a result, many light nodes connect to a few full nodes while other full nodes are almost idle, as illustrated in Figure 5.1, the current light node situation. Noticeably, this random connection does not consider the capacity of the selected full nodes. Thus, it affects the whole system performance and encourages us to propose a new mechanism to redistribute the loads equally among full nodes, as shown in figure 5.1, based on their different resources. Before dive into the proposal, we reclassify the IoT nodes into three main types to fit with our proposal requirements:

- Full node: is similar to the full node categorized by IOTA. Such nodes are essential in the P2P system and are characterized by the full ledger size and high computing power. Full nodes are the only components of the IOTA network to attach the transactions to the Tangle.

- Light node: also similar to the light nodes categorized by the IOTA; it is the node that has computing capacity much less than the full nodes and higher than the zero nodes (defined below). The light node can create and sign transaction, but it does not store the ledger or attach its transaction to the Tangle directly.

- Zero node: the node that does not share its resource with any node and requests assistance from other nodes to attach its transaction(s) to the Tangle.

  Zero nodes are divided into two categories: permanent and temporary. The permanent zero nodes represent the weak IoT devices that cannot perform computing effort or store ledger information. This type of zero nodes does not participate in the Tangle network directly. However, they are attached to one of the active nodes. They are similar to the lightweight node in the current IOTA classification and assigned to nearly similar tasks. The second category is a temporary zero node that is one of either full nodes or light nodes which stops sharing their resources with other nodes and decides to request assistance from other nodes according to our algorithm rules. An active full node is turned into a temporary zero node in the below cases:

- High traffic: an active node with a high number of transactions that bypasses a predefined limit. It forcibly turns into a temporary zero node and redistributes the incoming transactions to all other nodes based on the proposed resource allocation algorithm;
- Offline status: in case of maintenance, loss of connection, or any other hardware failure, the node will be suppressed from all the neighbor lists. However, it can generate offline transactions in some cases;
- Owner decision: The user can manually turn off the share node activities.

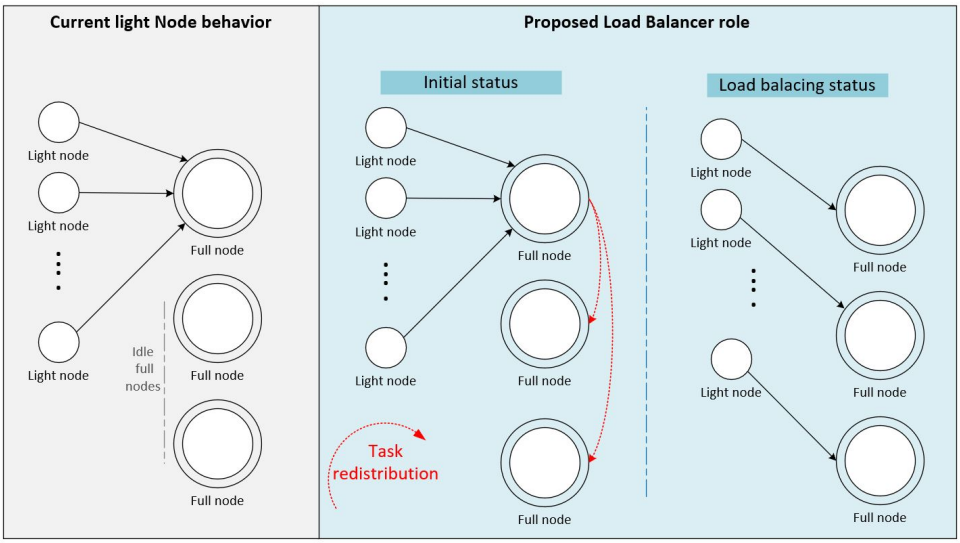


Fig. 5.1 Load balancer role: each node should act as a load balancer to distribute the incoming random tasks fairly among full nodes.

Table 5.2 shows our classification versus the current IOTA classification in terms of the main network tasks. The new classification adds flexibility to the network by empowering full nodes to manage the computing requests and share their free resources with other nodes. For example, in a cluster of different neighbor nodes, the full nodes cooperate according to a new resource allocation algorithm to perform the transaction requests from the light, permanent, and temporary zero nodes.

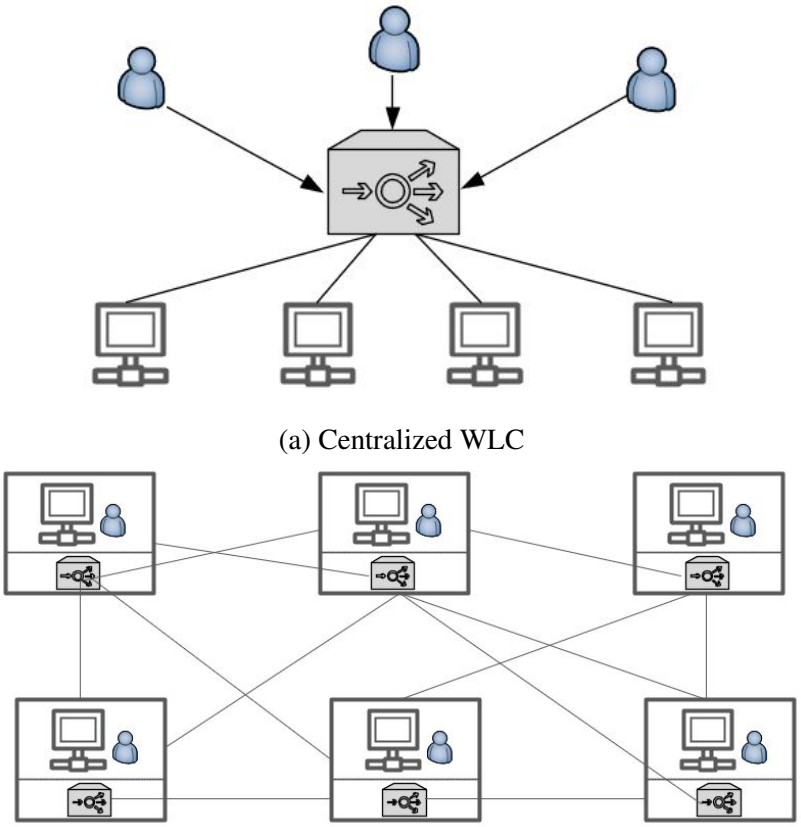
Functions	IOTA Structure		Proposed Structure			
	Full Node	**Light Node**	**Full Node**	**Light Node**	**Temporary Zero Node**	**Permanent Zero Node**
Stores the Tangle	✓	x	✓	x	✓	x
Communicate with neighbors	✓	x	✓	x	✓	x
Bundle, create, sign tx	✓	✓	✓	✓	✓	✓
Tip selection	✓	x	✓	x	✓	x
Validation	✓	x	✓	x	✓	x
POW locally	✓	✓	✓	x	✓	x
Attach to Tangle	✓	x	✓	x	✓	x
Receive Transaction request	✓	x	✓	x	x	x

5.2.1 Resource allocation with load balancing

In this subsection we briefly overview the algorithms related to the allocation with load balancing. Load balancing algorithms are broadly classified into dynamic and static categories [154]. The latter depends on the load at the time of node selection, whereas it is achieved by providing preliminary information about the system. This approach does not consider the system's current state while making allocation decisions, and, therefore, it weakens the overall system performance [155]. Obviously, the static approach is unsuitable for DLT systems since the participant nodes frequently enter and exit the network without prior notifications. Dynamic load balancing algorithms perform load distribution at runtime [156] and monitor any alteration of the system workload to redistribute the tasks based on the current state of the whole system. Usually, dynamic load balancing is considered a central solution that acts as a proxy between end-users and servers.

In the literature, there are several types of dynamic load balancers. For example, round-robin scheduling [157] directs the application requests from the network to nodes in a round-robin manner. It is widely used and easy to implement. However, it considers all nodes are equals in terms of resources and number of connections and unsuitable for our case.

Weighted round-robin is an improved version of round-robin where a weighted coefficient is assigned to the node according to its capacity. Nevertheless, such weight estimation does not take into account the number of current connections. Another algorithm based on the number of active connections is the least-connection scheduling algorithm that assigns the received requests from the network to the node with the least number of established connections. In our case, the limitation of this algorithm refers to neglecting the nodes' resources. The weighted least-connection scheduling is a developed version of the least-connection scheduling that considers both the capability of the node and the number of current connections to prevent overloading and achieve load balancing. Thus, our proposed resource allocation scheme to distribute computing loads between the IOTA full nodes is based on WLC.



(a) Centralized WLC

(b) Decentralized WLC

Fig. 5.2 Centralized versus decentralized WLC.

5.2.2 The proposed WLC Algorithm

WLC algorithm considers a superset of active connections on each node and its assigned weight based on the node processing capabilities [158]. This algorithm is used in a centralized environment, such as web server, SQL Server, etc., as illustrated in figure 5.2a to load balancing the incoming traffic from the clients' side. In our use case, the contest is to adapt WLC to a decentralized system where no one node can dominate the load balancing role and task distribution as depicted in figure 5.2b.

The network nodes share their nodes and connection number with their neighbors to achieve the WLC load balancing in such decentralized environment. Nevertheless, each neighbor list is up to nine nodes maximum [17][159]. This is a good point to limit the negative impact of the overhead due to the communications.

Each node of the system uses its hardware resources to retrieve the initial weight and uses the number of connections and the sum of its neighbors' connections parameters. Hence, each node in the network, considered as a load balancer, will be active whenever it is assigned to an external task. Therefore, at the time of request arrival, the node runs the WLC algorithm against its weight and other nodes' resources to assign the request.

Once the request is assigned, the remaining weight value of the assigned node decreases to be checked with the next incoming request, and so on. In this way, all the nodes contribute to balancing the loads among them and fulfill the scalability and performance enhancements without a central load balancer.

Supposing the neighbor set of n nodes in a network is:

$$I = \{1,2,3...,n\}$$

Node i has W_i Weight and C_i number of connections. The sum of current connection numbers is:

$$C_{SUM} = \sum_{i \in I} C_i$$

The incoming network connection will be directed to the node j, in which

$$\frac{C_j/C_{SUM}}{W_j} = min_{i \in I}\{\frac{C_i/C_{SUM}}{W_i}\}$$

Since the C_{SUM} is a constant in this lookup, there is no need to divide C_i by the C_{SUM} value. Thus, it can be reduced to be as below:

$$\frac{C_j}{W_j} = min_{i \in I}\{\frac{C_i}{W_i}\} \tag{5.1}$$

The weight of a node is equivalent to its computing resources and can be captured as a digit number. Let V_i be the processing speed of the CPU of the node i (in MHz) and C_{V_i} be the consumed capacity of the CPU of the node i. Thus, Vr_i the idle processing ratio of the node i CPU is given by: $Vr_i = 1 - (C_{V_i}/V_i)$.

Let M_i be the Memory size of the node i (in MB) and C_{M_i} be the consumed part of the memory of the node i. Thus Mr_i the free memory ratio of the node i: $Mr_i = 1 - (C_{M_i}/M_i)$.

The weight of node i is given as follows:

$$W_i = (\alpha \times Vr_i + (1-\alpha) \times Mr_i) \times 100 \tag{5.2}$$

This weight W_i is a load indicator between 0 and 100. Higher value of the weight reflects that the node is able to accept new request. $0 < \alpha < 1$ is a weight coefficient of the CPU idle ratio and $(1-\alpha)$ is a weight coefficient of the free memory ratio.

The component diagram of Figure 5.3 depicts the behavior of a new node that aims to join the network and initiate a new transaction. The node could be zero, light, or full. The network system filters out the device with weak resources, nominates it as a permanent zero node, and establishes a direct connection with one of the active full nodes based on the WLC algorithm. The zero node has no WLC algorithm running locally; instead, it triggers the full node to attach its transaction to the Tangle. The non-weak devices are either full or light nodes, where the full ones join the main Tangle network. The light node can possess the WLC algorithm and run it to select a suitable node. Then, the full node that receives the request runs the WLC to double-check that it is the best node in the group. Otherwise, the request will be directed to the best node. In the case of the active full node, the WLC permits to assign the transaction to the node itself if its workloads are below certain limits. Otherwise, the active node is considered fully charged and will not be considered in the current selection. It also turns into a temporary zero node for a while, and its transaction will be assigned to another available node according to the WLC rules. As per the peer-to-peer concept, all the nodes are free to leave and rejoin the network at any time. Therefore, the active node can turn into a temporary zero node for any reason such as maintenance mode, network disconnection, etc. Moreover, the selected node by the WLC algorithm can accept or refuse the computing request. Once a node accepts the task, it increases its connections by one and publishes the updated load balancer parameter to be available to the next node request and accessible by all the neighbors' list members. This mechanism of a node, while initiating transactions, is repeated instantly for each node within its neighbors' list to achieve the load balance of the computing tasks all over the neighbors' lists of the DLT system.

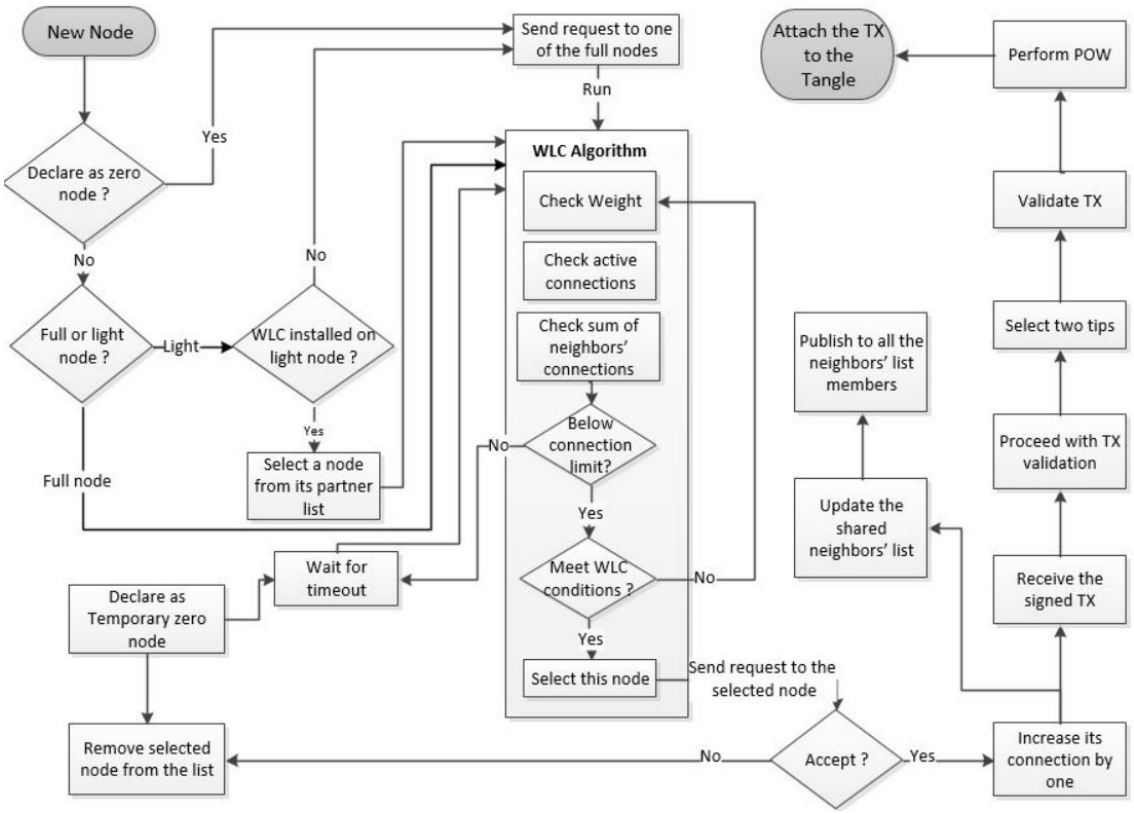


Fig. 5.3 Flowchart diagram of the proposed solution.

5.3 Experiments and Results

The WLC implementation can be performed with different scenarios. It can be installed either on the light node, on the full node, or both. We start by testing the WLC algorithm on the light node against a few Tangle nodes. The WLC is implemented in a private Tangle network consisting of several virtual machines that act as full nodes with different specs, and one virtual machine works as a light node. All the nodes are connected to the same network. The light node is represented by IOTA wallet software that can create and sign transaction only. Therefore, it should be connected to a full node to perform PoW tasks and attach its transaction to the Tangle. In this scenario, the light node runs the WLC algorithm of [158] to connect to one of the nodes in the list. Thus, load balance is achieved based on the WLC decision. In addition to the experiment done above, the WLC algorithm is evaluated on the full nodes using a simulation environment through a Java-Based tool, demonstrating the effectiveness of the load balancing algorithm. α is the coefficient rate to determine the CPU/Memory resources importance of a node. For example, setting α to 0.25 means that when calculating the weight of a node, we give less importance to the CPU rate than the

memory, and so on. In our evaluation, we set α = 0.5 (CPU and memory are equal), and we distinguish between different scenarios. Below is the algorithm used in our proposal. The condition introduced in statement 5 contains the sum of connections for each network to allow running the algorithm within environment of multiple networks.

Algorithm 1 Select the node j.

1. N: number of nodes in a neighbor' list
2. **for** $j \leftarrow 0$ to N ; $N > 1$ **do** $j \leftarrow j + 1$
3. **if** $W_j > 0$ **then**
4. **for** $i = j+1$; $i < N$ **do**
5. **if** $C_j \times CSUM_i \times W_i > C_i \times CSUM_j \times W_j$ **then**
6. $j = i$
7. **end if**
8. **end for**
9. return j
10. **end if**
11. **end for**
12. return *null*

5.3.1 Implementation: WLC in a Private Tangle

In this experiment, the proposed algorithm is embedded within the light node, as shown in Figure 5.4a, that runs against the full nodes to select the best available node. In this scenario, the light node is the only part that determines its connection. The light node runs the directly involved WLC algorithm within the Tangle. Inspired by IOTA client load balancer [160], we create a node js application that replaces the random selection method (RandomWalkStrategy.js) with the WLC algorithm. We use the IOTA libraries to build the load balance algorithm that can be installed on light and full nodes. The libraries include @iota/core, iota/client-load-balancer, iota/converter. Besides, we use the "node-os-utils" library to determine the load information of each full node. The experiment's result that is

limited to a few nodes within a private Tangle network shows the tasks are distributed based on the highest weight and least connection of the WLC algorithm.

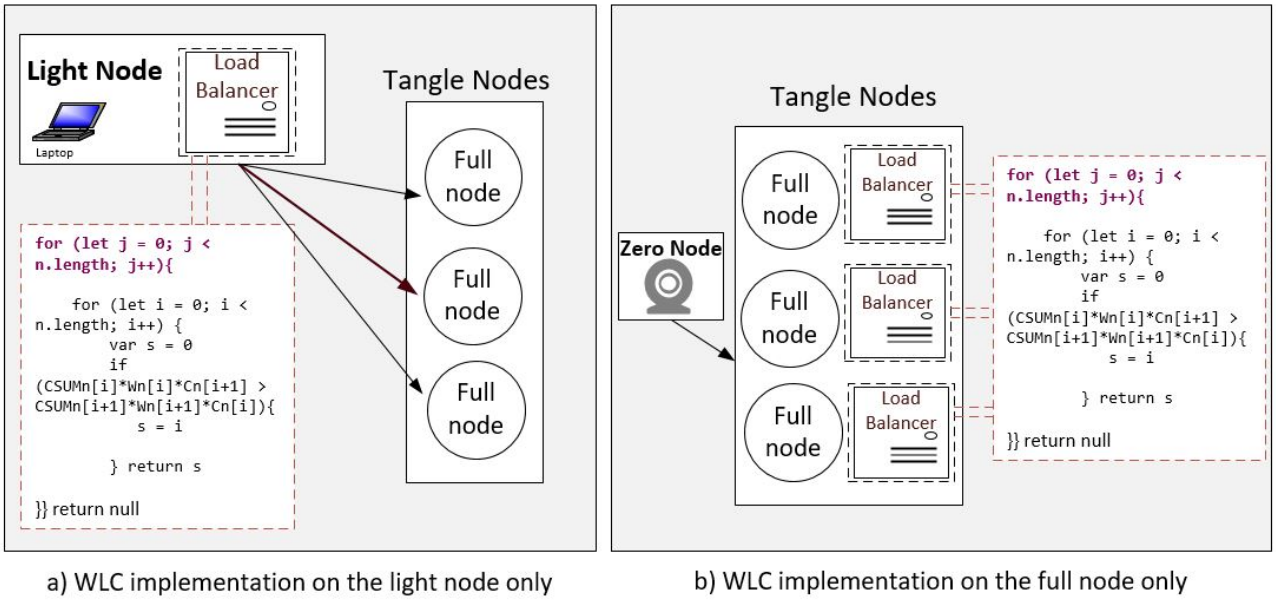


Fig. 5.4 WLC implementation with zero node and light node scenarios. With zero node scenario, the WLC is running on the full node network only. With light node scenario, WLC is running on light node directly.

5.3.2 Simulation: Decentralized WLC

We use a simulation environment based on the Java compiler to build a network of considerable Tangle nodes receiving huge data that simulates the WLC behavior within a decentralized environment. We first build the datacenter class to store all the network components. The simulation code is available on GitHub repository [161]. The class node generates nodes with random CPU values ranging from 1 KHZ to 6 GHZ and random RAM ranging from 500 MB to 16 GB. Furthermore, a JSON file is introduced to manually determine the values of the resources. This file permits us to create nodes either with similar or different resources to test different scenarios, as shown in the next section. Each connection consumes a fixed amount of resources and deducts the same value from any assigned node. Accordingly, the weight of that node is updated according to Equation (2). We set the connection request parameters to 10 MHZ as CPU and 50 MB as RAM in all the below tests. The performance indicators resulting from the simulations are: the weight of the node that reflects the available resource of the node and the ratio indicator C_i/W_i that reflects the load of the node.

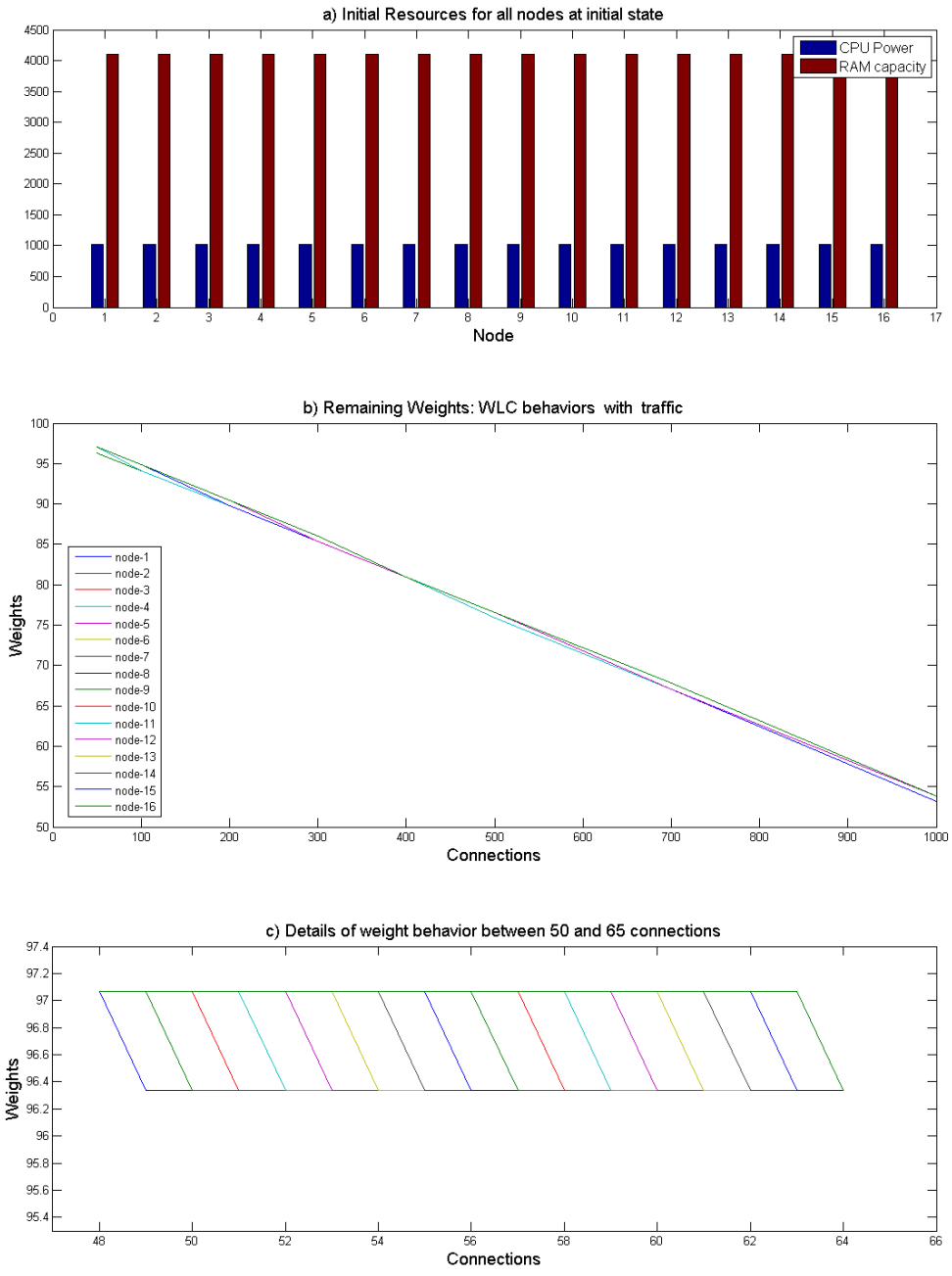


Fig. 5.5 Validation of the WLC algorithm using 16 similar nodes. the WLC behavior demonstrates the validity of the WLC algorithm.

5.3.2.1 Nodes with Similar Resources

In this scenario, we validate the implemented WLC algorithm and consider a network of 16 nodes where all of which have same CPU and RAM resources as shown in Figure 5.5a with 1000 Mhz for the CPU and 4000 MB for the RAM. The initial network is built upon one default connection assigned to all nodes in the first place to distinguish the different initial resource weights. Without losing generality, this test assumes that all the incoming connections require the same resources in terms of CPU and RAM. We activate the WLC algorithm for the nodes of different incoming requests ranging from 50 to 1000 and record the snapshots output. Before any connection request, the maximum initial weight of each node, which represents their resource consumption and maximum capacity ratio, is close to 100. This number reflects that the nodes are still in an idle state. After being assigned to connection requests, the nodes' resources decrease, and thereby, their weights decrease relatively, i.e., the available resources of the node decrease. As illustrated in Figure 5.5b, connections are distributed evenly over the nodes, and all nodes' remaining weights decrease in a similar way because they all have similar capacities. Figure 5.5c highlights the weights of the nodes when the number of connections is between 50 and 65. Thus, the WLC algorithm distributes the tasks orderly and fairly.

5.3.2.2 Nodes with Different Resources

Afterward, the second test distinguishes 16 nodes with variable weights as depicted in Figure 5.6a. We also assume that all the incoming connections require the same resources in terms of CPU and RAM. The target of this test is to generate the maximum traffic and monitor the WLC behaviors in terms of the remaining node resources. Accordingly, the number of connections is progressively increased, as illustrated in Figure 5.6b. For further clarification, Figure 5.6c details 25 successive incoming connections to these different nodes and shows the WLC behavior precisely. It is noted that with every new connection, the node with high weight and least connections is selected.

As the nodes are with different resources, we also plot the indicator C_i/W_i in Figure 5.7a to illustrate loads of the different nodes within the system. Based on the WLC algorithm, the node with the minimum load is selected when receiving a request. One can see that the values of this indicator for the different nodes are close to each other. The result shows that the traffic is distributed equally among the 16 nodes based on their remaining weights and previous active connections. With the traffic increase, all nodes' remaining weights decrease proportionally, demonstrating the elimination of the node overloading aspect. Figure 5.7b details the WLC behavior of the different nodes with connections ranging from 200 and 225.

This test's microscopic view is another proof of the nodes' response to the WLC distributed load balancer.

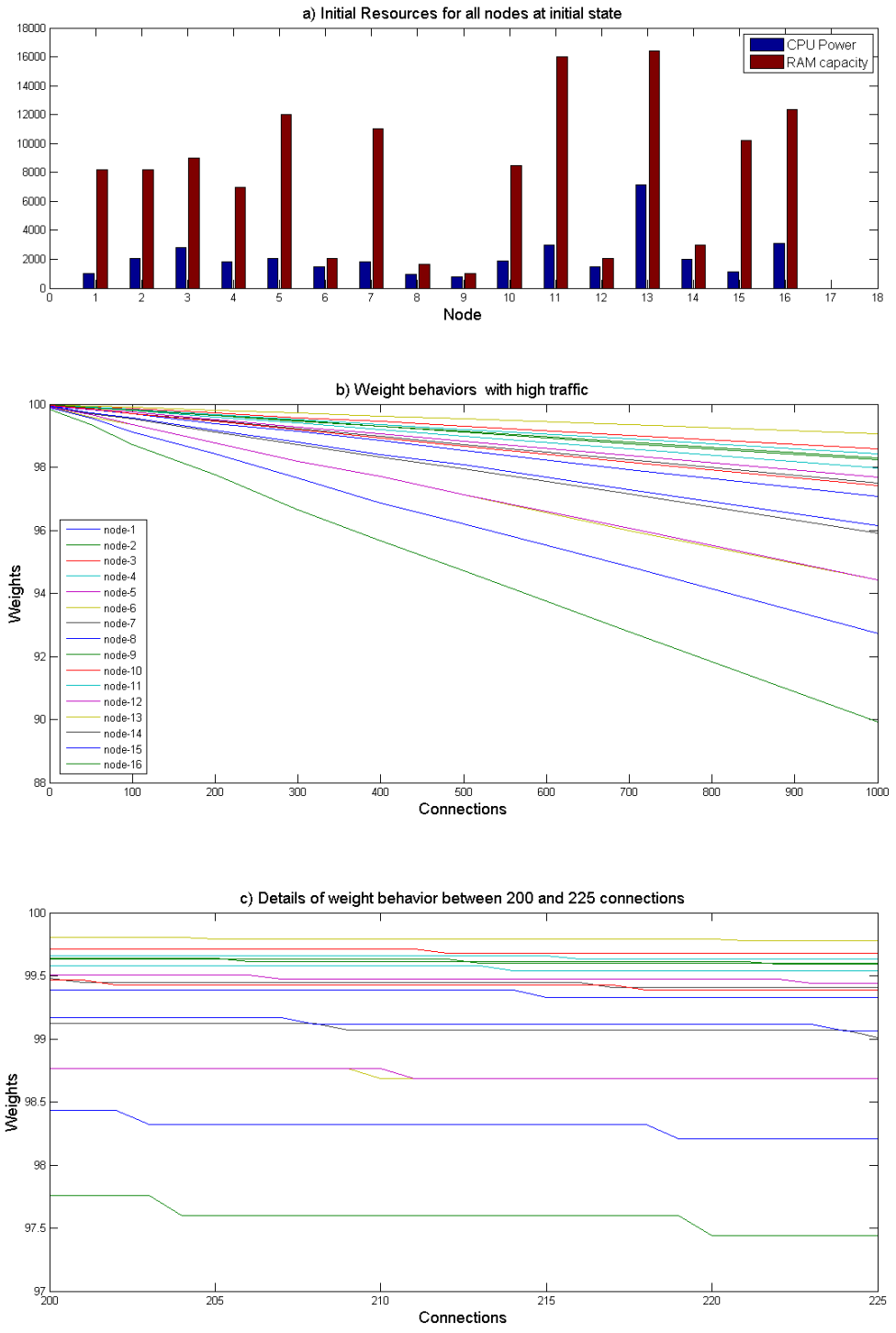


Fig. 5.6 Nodes with different resources.

2

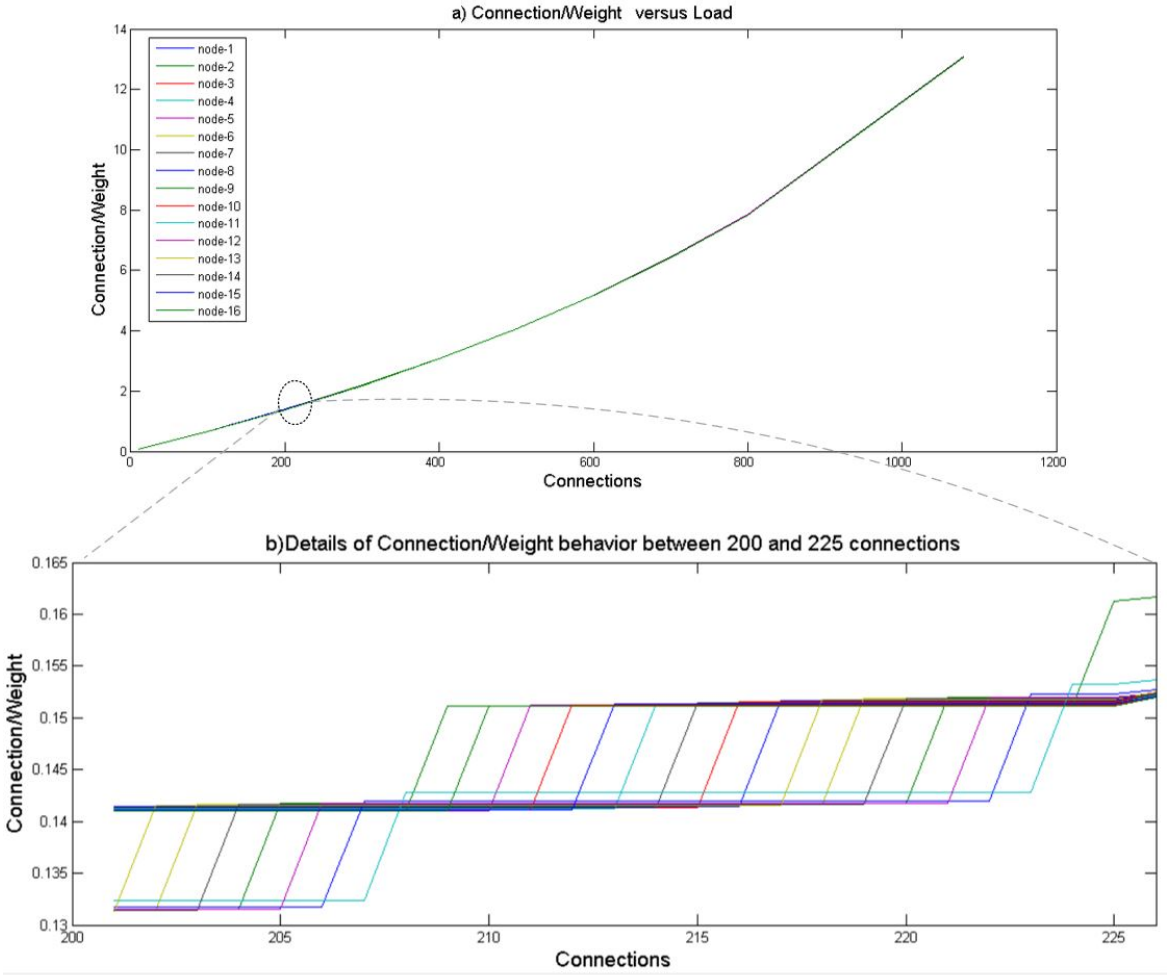


Fig. 5.7 Nodes with different resources: C_i/W_i.

5.3.3 Extension to a Tangle with Multiple Networks

In this case, the Tangle is composed of multiple networks each node has its own neighbor list based on the node distribution across their locations and their network addresses. Figure 5.8 depicts an example of a few full nodes distributed in three network clusters.

Node i has a neighbor list that contains all nodes so that all these nodes have node i as a common neighbor in their lists. Node j belongs to two neighbor lists, so its visibility is limited to list 1 and 3 only. Thus, Node j can assign tasks or it can be assigned to tasks by these two lists' nodes.

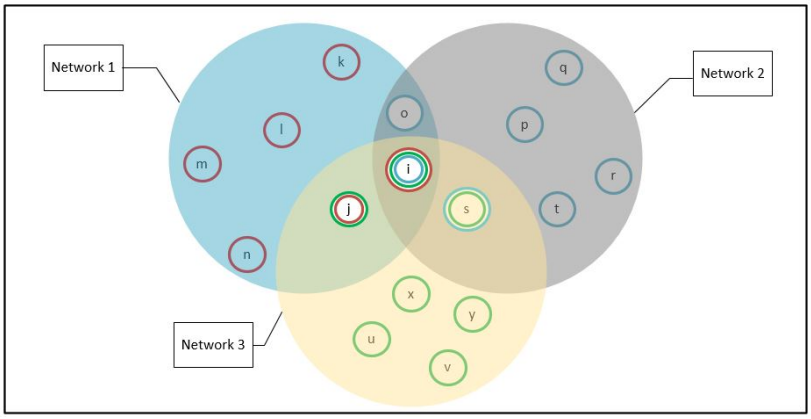


Fig. 5.8 Neighbor lists of the adjacent nodes.

However, other nodes like s, o have different neighbors that have, in turn, different neighbor nodes. Such behavior represents the main characteristic of decentralization where the information propagates from one node to another following the Gossip protocol [162]. The difference in these lists is normal in a P2P network that contains enormous number of participants. In addition, the neighbor list on each node is periodically updated since participants enter and leave the network randomly. The peer-to-peer system can scale to millions of processes, each of which can join or leave whenever it pleases without seriously disrupting the system's quality of service [163].

To best manage the massive workload within the huge number of networks while assuring the load balancing of the incoming traffic, we distinguish between different neighbor lists by a different sum of connections C_{SUM}. In this case, the sum of connection should not be reduced, as it is not the same for the whole network. Thus, the WLC is implemented in each network where C_{SUM_1} is the sum of the connections in the network 1, C_{SUM_2} is the sum of the connection in the network 2 and C_{SUM_3} is the sum of the connections in the network 3. As j belongs to two neighbor lists, when running WLC, Node j uses Min(C_{SUM_1}, C_{SUM_3}). Additionally, Node s uses Min(C_{SUM_2}, C_{SUM_3}), Node o uses Min(C_{SUM_1}, C_{SUM_3}) and Node i uses Min($C_{SUM_1}, C_{SUM_2}, C_{SUM_3}$). We simulate the three networks where the 16 nodes are with similar resources to validate the ability of the proposed mechanism to load balance the incoming connections. The simulation generates 1000 connections towards the three networks. In the beginning, the nodes have the same weight, and each network has an equal number of nodes, so the $C_{SUM_1}, C_{SUM_2}, C_{SUM_3}$ are equal. Once a connection is assigned to a node, the node's resources and weight are updated, and the C_{SUM_h} of the network h where the node exists will increase.

Figure 5.9 shows the increasing number of connections per network. One can see that the

connection loads are distributed efficiently among the multiple networks. For example, in the case of 1000 connections, the results show a load balancing between networks and nodes where each node is allocated to around 63 or 64 connections. Note that the total number of connections is greater than 1000 because the connections of the node j are counted in network 1 and also in network 3. Similar remarks for the nodes o, s, and i according to the corresponding networks.

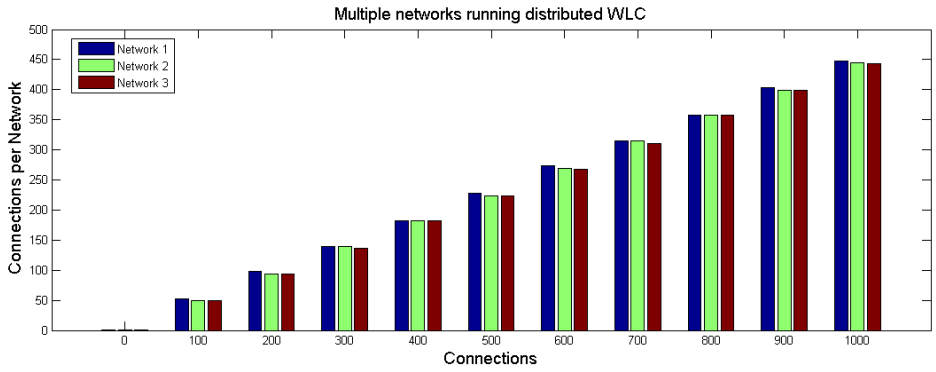


Fig. 5.9 Multiple networks running distributed WLC.

5.4 Conclusion

This chapter aims to improve the main platform proposal in relation to the thesis's third objective. We enhanced the tasks distribution among different nodes of the IOTA platform as a part of the architecture proposed in chapter 4 regarding low resources IoT devices. The enhancement is done by introducing a resource allocation scheme to handle the incoming workload transactions. Our proposal is based on the WLC scheduling load balancing algorithm, which distributes the incoming external requests fairly among nodes based on their resource capacities (weights) and connection numbers. Consequently, we modified the original WLC algorithm by distinguishing between the different "sum of connections" in multiple decentralized networks. The proposed algorithm is tested in a private Tangle and through simulations. The results denote an efficient selection of the suitable node based on the available resources and active connections in different circumstances.

Chapter 6

Data Transparency in the supply chain

6.1 Introduction

In previous chapters, we addressed the three thesis' objectives and arrived at a new architecture proposal that addresses the major drawbacks of integrating DLT with the supply chain. This proposal has a positive impact on the supply chain because it offers unique features and advances the supply chain's progress. Nonetheless, the new data transparency feature merits further investigation in order to achieve the thesis's primary goal of defining a typical DLT-based platform appropriate for the supply chain. Data transparency is one of the DLT features demanded by the supply chain to achieve traceability and high collaboration among stakeholders. However, the DLT transparency feature remarkably reveals all of the data, including stakeholders' undesired information. In this context, we observe that the transparency feature could hinder the DLT integration with the supply chain. Therefore, we investigated the existing projects' behaviors concerned with data transparency subject and collected the available technique that boosts the transparency. Besides, we investigated our proposal platform for an enhancements over existing DLT transparency. After working on a detailed analysis, we highlighted several existing mechanisms that could help achieving the goal and we concluded that transparency must be in control. this chapter includes the following points:

- We surveyed the existing DLT-based supply chain projects leveling data transparency;
- We investigated the techniques utilized in the data transparency enhancement process;
- We shed light on the importance of transparency and borders between transparency and

opacity through access control to successfully integrate Blockchain into a supply chain;

- We highlighted the smart contract and IoT technology roles in achieving controllable data transparency, and call for further investments;
- We show up the importance of our proposal that provides one platform supporting IoT and smart contract technologies. Thus, the data transparency can be well improved in our proposal rather than the other Blockchain-based platforms.

6.1.1 Transparency versus traceability in supply chain

Transparency enables the different participants in the supply chain to obtain full visibility in terms of the data, services, and products being introduced and exchanged. Different works in the literature have used the terms transparency and traceability to describe this feature. However, these two terms designate two related yet different features [164]. Data transparency is defined [165] as the ability to easily access and work with data, independently of where they are located or what application has created them. On the other hand, traceability in a supply chain is described by ISO 9000:2005 as the ability to identify a product at any stage in the supply chain. It is also defined as a process of tracking the products' provenance and their inputs from the start phase to the end-use. From our perspective, transparency in the supply chain refers to the disclosure of information to trading partners, shareholders, customers, consumers, and regulatory bodies. It captures high-level information along the supply chain, such as product components, suppliers' names, the different locations involved, and associated certificates. Referring to the previous definitions, we conclude that traceability is a prerequisite to transparency realization. Traceability provides opportunities to determine supply chain efficiency, meet regulatory requirements, and verify sustainability claims. To this end, many modern supply chain projects use a different technical solution to achieve traceability, and hence achieve a high level of transparency.

In addition, trust is an essential requirement in a transparent supply chain. Research studies [166–168] show that mistrust among the partners of a supply chain is a significant issue, which hinders collaboration [169, 170]. The supply chain is composed of independent partners, each of which represents a standalone centralized system. Consequently, data transparency may be compromised by a lack of trust among the partners and require more solid trust to be developed [171, 172]. Furthermore, consumers may request details concerning the products, including manufacturing origin, quality of service, and proof of safety. Thus, building trust is achieved by enabling transparency along the chain so that individuals and

companies can trace their products back to their origin. This can be achieved using Internet of Things (IoT) technology [2, 173].

6.1.2 DLT transparency and related works

In order to overcome the issues related to trust, Blockchain and, more generally, Distributed Ledger Technology (DLT), is a good candidate which enables the full transparency of data records. It enhances trust between partners through a cryptographic-based, peer-to-peer decentralized platform that underlies a supply chain [174]. Using the Blockchain platform for the supply chain eliminates the ambiguity behind the group of independent databases of traditional supply chain systems, as all records are stored within the ledger on every stakeholder system. Furthermore, Blockchain is immutable against the altering or removal of any records without leaving traces. This is because all partners have a copy of the same updated ledger that leads to a clear vision over the ledger contents. According to many studies [175, 79, 70] that have surveyed the critical aspects of implementing Blockchain solutions, Blockchain is a convenient tool to overcome trust and collaboration issues in a supply chain. It is called the "truth machine" [53], and discourages companies from any misconduct. Moreover, many proofs-of-concept (POCs) or piloting schemes have been developed in recent years using technology to study supply chains for traceability and transparency purposes [70]. Data transparency is a built-in feature of Blockchain due to the decentralized nature of the platform. In this context, the ability to control data privacy or opacity within the public Blockchain is questionable, while stakeholders in the supply chain have sensitive data that should not be disclosed to the public.

Sources	Roles
[176]	Elaborates the role of NGO's brand collaboration in enhancing the supply chain transparency
[177]	Develops system architecture to integrate Blockchain, IoT, and data analytics to provide sustainable products
[178]	Studies the relevance of supply chain transparency to supply chain sustainability governance
[179]	Conducts the Adoption of Blockchain for supply chain transparency
[74]	Reviews transparency/traceability of supply chain Blockchain-based in the litterature
[180]	Develops smart contracts to mitigate directly the supply chain transparency
[181]	Proposes multi-chain platform to enhance cross-border e-commerce supply chain traceability

Table 6.1 Existing studies related to Blockchain-based supply chain data transparency

Supply chain projects go far beyond the offered transparency and add their enhancement preferences in addition to the current Blockchain transparency feature. Despite its high importance in building the modern supply chain, there are no comprehensive studies that categorize and analyze the Blockchain-based supply chain's data transparency. There are a few of the intended projects shown in table 6.1 that shed light on this topic.

6.2 Supply Chain Transparency Challenges and Processes

6.2.1 Data Transparency Challenges

At present, the global supply chain consists of a complex network of stakeholders across industries to coordinate collaborative tasks and achieve mutual agreements. Figure 6.1 depicts the significant supply chain challenges that has direct and indirect negative impacts on the data transparency achievements: centralized systems, lack of transparency, scalability, challenges to IoT integration and the upcoming technologies.

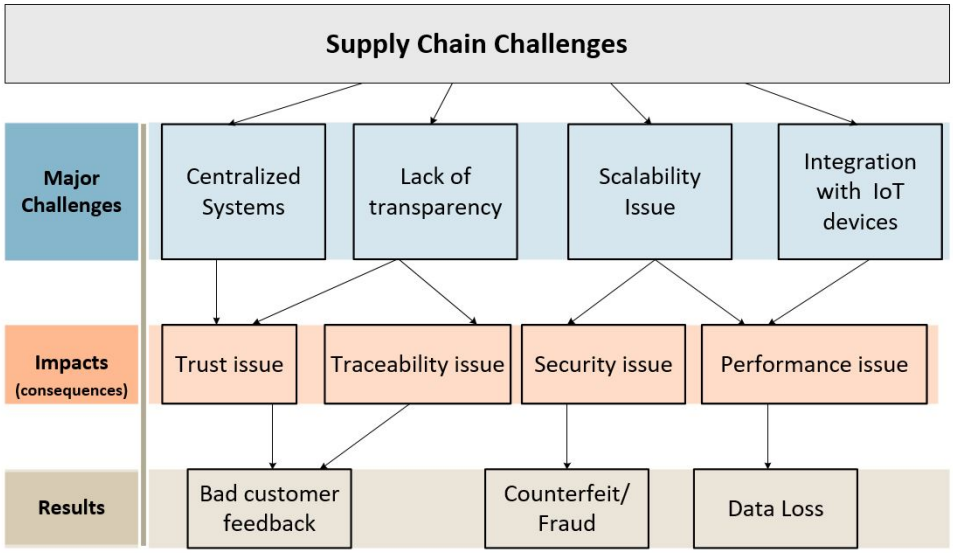


Fig. 6.1 Technical Supply Chain Challenges.

The existing centralized supply chain systems struggle unproductively to provide a portion of the vital requirements using workarounds and trusted third parties [9], in addition to the great integration of new technologies. Such independent databases have trust issues resulting in negative customer feedback and dissatisfaction. In addition, there is no reliable shared information within most of the supply chain, and that is the main transparency issue with a centralized system. Lack of transparency leads to traceability and trust issues, in addition to negative feedback from customers. Furthermore, as mentioned in chapter 3, scalability is a major problem of the supply chain [57], which leads to security and performance issues. Therefore, these cause counterfeits in the data of the intended products and, in many cases, data loss. Moreover, the current supply chain infrastructure cannot exploit IoT's full potential and manage/analyze the massive incoming data well within the centralized circumstances [9]. In this way, a considerable portion of the IoT power is dismissed. Currently, there are unreliable frameworks and infrastructures designed to connect billions of heterogeneous

and disparate IoT devices and their associated services, as well as data aggregation and data analysis [61].

6.2.2 Data Transparency Motivation

The supply chain has encountered enormous changes over time due to the high demands for supply chain transparency and traceability. These demands represent the main motivations for creating transparent systems. For example, when consumers increasingly wonder about where and how their clothes are made, or just how sustainable their potential new electric vehicle might be, given the raw materials required to make it, transparency in global supply chains becomes a notable issue, which needs to be addressed [182]. Moreover, the supply chain has become increasingly involved in the diversity of partners, products, and customer desires. Recently, the challenges have ranged from the heterogeneity of the systems to the additional technological requirements. Thus, besides the above challenges, the motivations behind supply chain transparency are the following:

- Independent Database: The current supply chain infrastructure is a group of centralized-based systems where each stakeholder represents a centralized system which belongs to one or more supply chains. These systems rely heavily on centralized, often disparate, and standalone information management platforms [79]. The group of databases involved in the production process is distributed, heterogeneous, and autonomous [183]. Therefore, data interchange between different databases is inflexible, due to the hard-coded nature of different data standards; Walmart and Cisco are two obvious examples [54]. Practically, the organizations' tendency to use their platform and control their data would limit collaboration.

- Lack of cooperation: The supply chain challenges are mainly related to the heterogeneity of the involved stakeholders, different data forms and lack of communications among the involved systems. Collaborative relationships determine how data are shared between companies, and project them to the underlying business processes. Collaboration is an opportunity for modern businesses to optimize their relationships with their trading partners. However, achieving collaboration poses complex contests between the supply chain actors. In this setting, there is a broad spectrum of collaborative initiatives, disparate standards for communication, and various levels of trading partner competencies and business processes [184].

- Data Loss: The widespread of IoT adoption triggers profound changes in global manufacturing [58]. The IoT systems are usually heterogeneous and categorized under

different administrative domains [185]. IoT technology ameliorates the production progress and provides a high level of control that advances transparency, but it charges servers and peripheral devices with a high data volume [4]. The current network infrastructure cannot exploit the full IoT potential and cannot thoroughly manage/analyze the massive incoming data well within the centralized circumstances. Investing in IoT technologies in the current supply chain infrastructure surcharges these traditional systems with high data load, so part of the information is considered lost [9]. Moreover, most valuable products are controlled and tagged electronically; these tags may be cleared/replaced during the transition between stakeholders without leaving traces, leading to trust and security concerns. The probability of data alteration is very high through the current supply chain processes [186, 187], where data loss and fraud are likely to happen in many situations.

- Product Complexities: Today's products and services' dispersed natures require their supply chains to be adequately visible to avoid obscurity and provide transparency and traceability features [70]. However, many manufacturers and sellers encounter information insufficiency, and therefore fail to provide customers with the required information due to lack of transparency. Hence, the supply chain complexity is increasingly evolving, as the diversity of the products and requirements requires the integration of many multi-tier supply chains. The availability of high transparency achieves a multi-tier supply chain and manages the different supply chain network parties. Thus, the centralized system's uncontrolled informational data leads to massive counterfeit, massive trade losses and bad business reputations.

6.2.3 Security Challenges

Many different security factors challenge the supply chain in a way that may hinder the whole production processes.

- IoT technology proliferation: It is involved in most supply chain chain productions and processing tasks. Their proliferation will exceed half-trillion within the next few years [188]. The IoT devices communicate among themselves, servers and storages, producing massive transaction numbers along with supply chain production lines, leading to to numerous security challenges to protect the devices and the sensitive data from any leakage or attack.

- Data opacity requirement: Usually, the manufacturing processes are accompanied by several private aspects, including proper planning, recipes, manufacturing intelligence,

etc. Data privacy is one of the apparent concerns of the supply chain areas. Therefore, all systems may face data breaches, theft, leaks, unauthorized access, eavesdropping, etc. Accordingly, data opacity must be maintained by all the stakeholders that form a supply chain. By definition, a system is opaque if an external observer is unable to infer a "secret" about the system behavior [189]. Consequently, the decentralized platform that manage the supply chain should consider the opacity requirements.

6.2.4 Supply Chain Policy Enforcement

To achieve the supply chain transparency target as planned, a deep understanding of the intended goods and their requirements is desired. Furthermore, it is required to map suppliers and processes and clarify information gaps. Unfortunately, there is unclear description of the transparency processes that illustrate the road-map of a supply chain project in the literature. In [190] a practical guide to defining, understanding, and building supply chain transparency in a global economy is presented. It is done by: identifying and visualizing risk, using transparency levers to close information gaps, managing, and finally monitoring. In the below, we set the transparency processes for a supply chain to be well employed within better conditions:

- Self-identification: this is the first step that should be settled for a supply chain to identify the environment's overall components, including suppliers and sub-suppliers. Consequently, they should define each component issue and the common intersection among the partners. Accordingly, the risks and the goals are determined afterward, based on the different regulations and rules of the internal/external stakeholders in addition to the common factor impact on the business success.

- Collect information: Collecting data about the production processes, goods, gaps and others, practically on sites, is the most sensitive step. Nowadays, companies increasingly require more data from their suppliers. Collecting accurate data, in this step, is significantly crucial and impacts directly the overall supply chain transparency.

- Expose: the decisions are taken in the last step where the company has a complete picture of the supply chain. The decision takes into account meeting the relevant regulatory requirements and internal/external stakeholders' demands. Furthermore, the company should clarify how the information is disclosed.

6.3 DLT-Based Supply Chain Benefits

Blockchain is a good candidate to address the above supply chain issues. It is a technology used for storing and transmitting data, which guarantees its integrity and transparency. A DLT platform that works without a trusted third party contains the history of the data exchanged in the network. This secure database is replicated in all the network nodes. Blockchain contains a chained set of blocks; each block contains a list of transactions and some other specific data. It is a fully decentralized P2P (peer-to-peer) system that guarantees trust between the non-trusted partners [13]. The main features of Blockchains are their decentralization, shared ledger, tamper evidence, tamper resistance, record-keeping, immutability, distributed trust, multiple-party consensus and independent validation [191].

The Blockchain serves the supply chain against many limitations and improves its functionalities in reference to the features mentioned below:

- Decentralization: The distributed ledger of a Blockchain-based supply chain empowers the involved partners to detect any deterioration of information. Thus, Blockchain tackles data corruption, hacking, or crashing issues in the centralized and independent systems and increases the information validity [192]. Moreover, this decentralized system can be inexpensively implemented among the suppliers [193];

- Trust: transparency is the main consequence of the distributed ledger technology where participants have a complete vision of the current contemporary information. Furthermore, privacy and anonymity are enabled because of the cryptography system [194]. Thus, it is unnecessary to evaluate the trustworthiness of the participants in the network with a decentralized supply chain. Evaluating trust between participants is due to the Blockchain's underlying technology, which guarantees the integrity of data records even in the presence of fraudulent nodes. Therefore, participants recognize that the information is accurate because each involved party has the same data, which cannot be altered or deleted. For this reason, resolving trust issues is discussed as one of the main arguments of the DLT implementation [195];

- Automation: Blockchain applications are mainly based on smart contracts to verify the execution of transactions between two or more parties relying on predefined rules and conditions. The smart contract is a self-executed program or script, which is located on Blockchain ledger [196]. It executes its code once triggered, either from a participant node or from another smart contract. Then, it broadcasts the content to all network nodes for validation and updates the ledgers accordingly in case the contractual terms agree. This automated process reduces the apprehension behind the

traditional contract of a supply chain where there is no need for human intervention and trusted intermediaries [197].

6.4 DLT Techniques for the Supply Chain Transparency

The emerged DLT-based supply chain proposals involve several techniques and solutions on top of their decentralized platforms. These techniques are presented in this section to be reused solely or unitedly by researchers for their under-construction supply chain systems. Then, in Section 6.5, we explore existing projects, and we show how they use the existing techniques related to data transparency and traceability to achieve the modern supply chain requirements. Below are the most valuable techniques:

6.4.1 Blockchain Core Improvement

The peer-to-peer system surcharges IoT devices with computing tasks and high storage demands. Many nodes are designed and prepared with top resources for computing and transaction validation in the mining and cryptocurrency field, which is not the case with heterogeneous IoT devices. Modifying some critical Blockchain characteristics boosts the integration of IoT devices with the DLT technology. Block size, creation time, and consensus algorithm are the areas where altering and adjusting the Blockchain in accordance with IoT requirements occur. In terms of data transparency, the enhancements of the transaction format have a significant impact compared to the others. The transaction in its current status lacks many essential details. Thus, developing the transaction format to include some real identity, references, blockinfo, etc., will increase the challenges related to the data transparency.

6.4.2 Smart Contract

Smart contracts are automated contracts embedded in the Blockchain, which make the entire process decentralized. Upon the deployment of the smart contracts, it is almost impossible to alter its code. Smart contract is a recent term that is widely used to refer to low-level code scripts running on an Ethereum Blockchain Smart contracts have recently attracted interest due to their importance in business applications and supply chains. In addition to the smart contract's role in ensuring the contract progress, it is also considered an excellent tool to enhance the data supply chain transparency [180]. When a smart contract is executed, all the intended parties within the supply chain are informed of the result and, therefore, they can trace and monitor their products, which increases the transparency level.

6.4.3 Involvement of IoT Device

At present, IoT technology represents one of the core elements of any modern supply chain. It has two main functions: capturing data from media and transmitting them to their destination. Moreover, IoT devices play a central role in ensuring the success of the supply chain's product traceability. Exerting additional efforts has an extensive role in improving the IoT functionalities, to make them suitable for Blockchain-based manufacturers' requirements. Considering the IoT side by the DLT system and its application is the best practice. Some projects [100, 109, 82, 103] mentioned in this study have contributed to the IoT improvements in terms of detecting data accurately, to improve the visibility of the data. The transparency is enhanced, and the traceability will be more efficient with the IoT technology involved in the DLT-based supply chain [79].

6.4.4 Merkle Tree Tool

The Merkle tree structure [13] is a binary tree with an associated value for each node, where each one is the hash of its children. These data structure trees are created by repeatedly hashing pairs of nodes until only one hash is left. The last node of a tree (leaf) is a hash of transactional data where other nodes are hash of their previous hashes. This allows any party to quickly verify the validity of data in a branch or leaf using the tree's root hash. Blockchain, and especially Bitcoin and Ethereum, fundamentally use it. Merkle tree has three main advantages over transactional processing. First, it guarantees the integrity and validity of the data. Second, it consumes less memory and CPU resources, as the proofs are computationally easy. Third, Merkle processing requires tiny data to be sent over the network and stored on disks. We involved the Merkle tree in the list of transparency techniques due to its importance in traceability within a supply chain.

6.4.5 Zero-Knowledge Proof

Zero-knowledge proof (ZKP) [198] is an encryption scheme where service providers do not recognize the data stored on their servers. The Prover can prove that a specific statement is true to the other verifier party without revealing any additional information. It can be used in messaging, authentication, storage protection, and for any other sensitive information. ZKP can also be integrated with Blockchain and, more specifically, with the private Blockchain, so that whatever the number of Blockchain nodes, ZKP adds a robust layer of security to the data ledger. Integrating ZKP with Blockchain encourages the supply chain to increase its transparency level, while their data confidentiality is preserved [199].

6.4.6 Our proposal: Blockchain and DAG combination

We have proposed in chapter 4 a new platform that mitigates many gaps behind Blockchain limitations within the supply chain. The proposal that combines IOTA and Blockhain into one platform enforces IoT devices to run on a DAG platform instead of a block system. Also, it enables smart contracts on peripheral DAG-based devices. This combination technique allows the enhancements of data transparency throughout the IoT and smart contract technologies.

6.5 Existing DLT-Based Supply Chain Solutions

The integration of DLT into legacy industries and different stakeholders aims to revolutionize the global supply chain with decentralization features, smart contracts, and IoT technology. Currently, many DLT-based projects seek to acquire trust, transparency, collaboration, and cost/time-saving throughout their innovative DLT platforms. In chapter 3, we presented several supply chain projects and shown their technical details. We analyze these projects in terms of data transparency and depict their enhancements in this topic. In the literature, many business projects integrate DLT into their platform. Still, Most of them consist of API interfaces run on Ethereum, the well-known global Blockchain, but they do not have explicit technical references or detailed publications. [81] listed, for example, around 105 DLT-based projects integrated with IoT since 2008 and categorized them into four types without revealing their technical sides. This section sheds light on the DLT-based supply chain projects while focusing on data transparency and traceability. Therefore, in addition to the projects listed in chapter 3, some interesting projects tackle data transparency and enhance overall privacy. Below are the intended projects that employ DLT in their supply chain:

- Dietrich et al. [180]: proposes an academic framework designed to tackle supply chain transparency by employing a new smart contract approach. The authors achieve their goals by following three steps. In the first step, the framework identifies and enlists all the partners involved in the manufacturing process. The first step is not an easy mission in a complex supply chain, but it is necessary to simplify the manufactured product's concrete process affiliation and composition. This framework assumes that each asset should have a unique identifier. Accordingly, a link is established between each physical asset and the Block-chain platform by generating smart contract's unique identification numbers. These numbers are called virtual identities or Hash'ID, where each one is mapped to a unique physical asset. Hash IDs can also refer to licenses, certificates, or other types of non-physical assets. They are attached to a bar-code

form such as Radio Frequency Identification (RFID) or Quick Response (QR) code to link these numbers to the Blockchain. The proposal introduces two types of players in the framework, the supplier and the Certifier. The certifier's role is to assign certification to suppliers in order to create the Hash'IDs. Depending on the supply chain's characteristics, the Certifier's role can be taken over by the manufacturer and other independent organizations. In the second step, they logically attach all the supply chain processes logically into the Blockchain platform through the smart contract. Furthermore, the last step makes the final decision based on a multiple smart contract recorded on the immutable Blockchain ledger.

- CoC [200] refers to "Chain on Blockchain", a supply chain management platform based on hybrid Blockchain to mainly tackle the trust issue of multiple entities. In general, in an authorized network, some nodes are promoted for block creation and validation. CoC distinguishes between the record submission and block-building using a hybrid model to organize the underlying distributed ledger. Submitted records are limited to users, third-party users, and supporting entities only, while building blocks are opened to the public users, named helpers. CoC invented an approach to build a distributed ledger called "Two-Step Block Construction" within their hybrid platform. Step 1 is the generation of reservation blocks by users, and step 2 is to generate data blocks. In step 1, a user submits a request to reserve predictive blocks. The request includes requester information, the fee the user wants to pay for the block, the helper's identity and who creates it, and other essential information. The helpers have to reach a consensus to reserve the block. In step 2, the user uses their reserved block(s) to send data to the ledger. There is no proof-of-work computation effort for the reserved block in this step, since helpers already validate it at the reservation time. The two-step block reservation does not reduce the latency for the overall performance. It provides a mechanism to shift the latency as long as a user has enough reservation. The latency of adding a new supply chain record can be very low. In short, CoC proposes a new DLT hybrid mechanism, but in terms of transparency, it relies on the embedded Blockchain features only.

- Aqua-Chain [201] is a traceable system for the water supply chain management based on Blockchain and can be implemented by either Ethereum or hyperledger Blockchains. The data transparency is guaranteed, since IoT devices collect data along the supply chain and store them within the Blockchain ledger. Therefore, Aqua-chain software is adapted to provide full traceability to their customers under the classical notion "from-supplier-to-buyer." It is composed of a layered architecture that relies on Blockchain

and IoT to achieve traceability. Aqua-chain can be integrated into existing traditional systems such as ERP and CRM. The front-end layer is composed of API REST applications that can easily be integrated with other software. The middle layer is called the controller. It is responsible for transforming the high-level function call into a low-level Blockchain call, and vice versa. Aqua-Chain enables integrating IoT and DLT technologies, and creating transparent, fault-tolerance, immutable and auditable records that can be used for the water traceability system.

- ProductChain [118] is a consortium Blockchain, introduced to enhance the traceability of the food supply chain (FSC), taking into account the speeding up the transaction rate into less than one second. It mainly relies on a three-tiered sharding architecture to improve scalability and ensure data availability to consumers. It also introduces the Access Control List (ACL) to limit access to competitive partners, collectively managed by consortium members, and provides read and write access. In addition to its improvement over scalability, it introduces transaction vocabulary to store different types of information and interactions, which encompass all FSC processes. The transaction vocabulary can link the final product to multiple raw ingredients relevant to a broad range of SCs. Productchain enhancements provide data transparency so that a user can quickly trace it back to specific key ingredients and a consortium-governed access control, which guarantees that no participant controls the Blockchain;

- Bext360 [122] is a supply chain platform used to enhance the global food commodities and provide full transparency from farmer to table. It is a software as a service (SaaS), which integrates Blockchain and sustainability measurements to provide a traceable fingerprint from manufacturers to consumers. It runs a RESTful API that allows retailers and wholesalers to insert the technology into their websites, point-of-sale systems, or supply chain management tools. The SaaS platform allows each stakeholder to track food products independently throughout each phase of their supply chain and enhances its overall transparency;

- Fr8 [202] is a supply chain network that aims to modernize logistics with an improved solution for the industry in general, leveraging Blockchain technology at its core. It is based on coupling shipment tracking IDs, RFIDs, and other documentation to create meaningful relationships among multiple datapoints. The Fr8 protocol is composed of five layers. The transport document layer contains the data and metadata of a shipment. The permission & ID Layer manages data integrity and permissions. The interface Layer exchanges data between the document layer and the service Layer. The service Layer connects the Fr8 Protocol with applications. The application Layer works with

services and interface layers to display the data. To ensure transparency, Fr8 relies heavily on the Blockchain principle as a single source of truth for shipment data. All of the involved stakeholders will have unprecedented visibility into shipments and their associated data;

- NextPakk [203] is a delivery service that tackles the last mile issues based on Stellar's Blockchain due to its speed and scale. It allows customers to schedule delivery within an hour at home when the package arrives. Furthermore, NextPakk uses Blockchain technology to track packages while protecting customer identity and ensuring a punctual delivery This adds transparency to the delivered goods, where customers can instantly track their packages online. Nextpakk involves Blockchain in elaborating the entire last mile, so that the consumers can track the driver and obtain complete transparent information on their packages' exact arrival time.

6.6 Discussion

Production stakeholders seek collaboration to optimize the supply chain processes and maintain robust relationships with trading partners. Collaboration among different independent systems challenges the supply chain partners, as there is a broad range of collaborative initiatives, disparate communications, and numerous levels of trading competencies and business processes. A collaborative supply chain requires suppliers and sub-suppliers to share data within a fully transparent environmental media to entirely realize the benefits of collaborative business. Before Blockchain, one of the well-known methods used to achieve transparency is called one step up, one step down. Many supply chains use this principle for traceability purposes [204]. This principle requires each supplier to share their information between the other adjacent ones. In other words, it is a chain of shared information where each supplier receives enough information on the incoming commodity, and then they thoroughly deliver the complete information to all the involved suppliers. It is a neighboring process for actors to share the information among themselves. However, this method is limited to two strides of visibility and, therefore, the transparency is not fully achieved. Furthermore, FarmaTrust [111] finds that technologies, such as holographic tamper-proof labels and unique serial numbers, are not sufficiently effective within the current centralized supply chains. In addition, the challenges mentioned in Section **??** necessitate the intervention of a decentralized Blockchain, coinciding with the development of many other technologies, such as IoT and others. Certainly, Blockchain is a quantum leap toward a new supply chain concept. The new supply chain data are collected differently and added to the decentralized chronological system, which is immutable, anti-counterfeit, transparent, and trusted. Nevertheless, as

transparency represents the core of a successful supply chain, what else can be done to the standard traits of any Blockchain network?

We have previously mentioned various solutions targeting the modern supply chain improvements integrated with Blockchain, which enriches the system with trust, transparency, and traceability. These projects integrate the Blockchain within their platforms to overcome the trust issue at the first stage and obtain the other DLT systems' added values. Besides the excellent facilities of Blockchain, the listed techniques in Section 6.4 are used/introduced by several projects and implemented in various ways to achieve more flexibility in data transparency and traceability. Table 6.2 shows that these projects' techniques are used to enhance product traceability and data transparency. Referring to the above classification, the most utilized techniques involve IoT device and the smart contract. Most of the projects use these two techniques differently based on their requirements. IoT technology is often used for tracking and tracing items using technologies, such as QR codes, smart tags, RFID tags, NEC, and mobile applications. Moreover, there are some additional IoT devices which are essentially constructed for supply chain transparency purposes. Some projects utilize the smart contract as it was programmed with Blockchain, such as Ethereum. Furthermore, the smart contract is developed to ensure the transparency of off-chain networks outside the Blockchain environment. Some smart contract enhancement tools are represented by assigning different roles or defining multiple smart contracts within the same project, such as setting the standard requirements and measurements of Ambrosus [102]. The Merkle tree algorithm is a technique used to quickly and accurately filter out the wrong data inputs using the crypto-hash functions. The zero-knowledge proof is used to protect sensitive data and enhance transparency. At the level of Blockchain core improvements, one of the techniques used is changing the Blockchain transaction format to include additional fields, which enhance transparency and facilitate traceability.

The Blockchain integration with the supply chain radically solves the data transparency and provides end-to-end traceability, with clear visibility of all the platform components. Moreover, some of these projects employ extra efforts and propose an additional layer of transparency. They target data traceability, by introducing mechanisms with added values over the current Blockchain features. Different enhanced tracking methods are deployed, ranging from involving new sensors to tags and tracers, as shown in Table 6.2. Vechain and Ambrosus are notable projects, which employ different methods. Ambrosus takes advantage of the Merkle tree in their transactional processes, since it is based on hash cryptography. With this tree algorithm, users can immediately find their data and filter out the wrong inputs. The tree algorithm can also be used with other IoT devices or mobile scanner applications that distinguish between massive Blockchain records. In other terms, it enhances the tracing

Project Name	Transparency Technique	Tool
Ambrosus [102]	Merkle Tree Algorithm	Hash-based data structure
	Smart contract	Measurement and requirement smart contracts
Modum [103]	IoT device involvement	"track and trace" QR code
	IoT device involvement	Modum temperature logger
	Smart contract	Normal utilization
Vechain [101]	Blockchain core improvement	Block transaction format (ID, DependsOn, Blockref)
	Smart contract	Normal utilization
Chronicled [115]	IoT device involvement	Smart tag (cryptographically secured chip)
WaltonChain [100]	IoT device involvement	RFID tag IC
	Smart contract	Manage parent chain and sub-chains contracts
Devery [105]	Smart contract	Smart contracts for registration and verification
OriginTrail [82]	Smart contract	Off-chain utilization
	Zero-Knowledge Proof	Sensitive data protection
Cargocoin [107]	Smart contract	Normal utilization
Bext360 [122]	Smart contract	Normal utilization
Shipchain [104]	Smart contract	Normal utilization
WABI [109]	IoT device involvement	RFID cryptographically secured chip
TE-Food [110]	IoT device involvement	Plastic security seals (1D/2D barcodes)
	Smart contract	Normal utilization
FarmaTrust [111]	Smart contract	Normal utilization
	IoT device involvement	QR code scanner via mobile SMS/voice label code on traditional mobile
ProductChain [118]	IoT device involvement	Transaction vocabulary
BlockGrain [112]	Smart contract	Public/private Blockchain managment
Zero defects [113]	Blockchain core improvement	IOTA DLT platform
Everledger [117]	IoT device involvement	Inteliggent Labelelling: RFID, NFC
FR8 [202]	IoT device involvement	Combines RFID, ID, product information
Our proposal [69]	IoT device involvement and smart contract	Combines DAG and Blockchain

Table 6.2 Transparency techniques of supply chain DLT-based Projects

function of the supply chain and speeds up the transparency process. Vechain is moving towards the improvement in the core of Blockchain for additional service refinements. This modifies Blockchain's transaction format by defining new fields: ID, DependsOn, Blockref, and Expiration for each transaction. From a logical standpoint, the Vechain proposal can be commonly used within any DLT-based supply chain. The new fields of vechain can be classified under tracking parameters that can be used with any DLT platforms without challenging their functions. These parameters improve the data transparency and aid in the perfect traceability achievement. However, most Blockchain-based supply chain projects support smart contracts, but no one boosts the proliferation of IoT devices at a large scale. Our proposal supports both IoT and smart contract to run on the supply chain platform, thereby providing a suitable environment for the data transparency enhancement.

6.6.1 IoT for Transparency Enhancement

The importance of IoT integration with Blockchain to enhance supply chain transparency and traceability rises with IoT technology development. The IoT devices' prominent features are represented by collecting accurate data, quick adaptation, and always-on availability services compared to traditional manual methods. Under the current central structure, IoT experiences the difficulty of achieving a genuine cooperation because the relevant parties of such cooperation often belong to different suppliers with complex or uncertain trust relationships. Therefore, the collaboration of the current IoT devices can only be employed in a trusted environment. As a technology that offers the service of trust, Blockchain can ensure the authenticity of data on the network. IoT ensures the true effectiveness of information when uploaded from the original source. The combination of IoT with Blockchain opens up a road of innovation, with unlimited possibilities. It can be used primarily to track the history of different goods. Thus, IoT technology is essential for new business systems. Furthermore, the IoT helps to establish a harmonious relationship between Blockchain and the world, as IoT devices are the physical interfaces that collect data. In addition, the IoT technology can reduce the disturbing factors from the source to ensure the data's actual effectiveness. Mainly there are five IoT techniques involved in the industrial field [4]: RFID, wireless sensor network (WSN), middleware, cloud computing, and IoT software. In contrast to human abilities, IoT techniques assist producers in collecting data accurately, such as perceiving temperature variation, calculating the elapsed time, and the color degree [205].

Many projects enforce the transparency of the supply chain by introducing the IoT technology within their projects, as illustrated in Table 6.3. Each project utilizes this technology differently. Waltonchain is directly related to the inventor of RFID technology. It introduces an enhanced RFID version for a Blockchain-based supply chain that provides tamper-resistance, reliability, anti-counterfeiting, and traceability to the business system. Thus, in addition to Blockchain features, the Waltonchain project includes an RFID tag IC and reader IC, appropriate for Blockchain applications. The ICs are characterized by integrating an elliptic curve and decryption acceleration module based on the existing RFID technology and a communication interface protocol for Blockchain applications. Waltonchain solves major IoT problems in Blockchain-based applications. It exempts tags from data storage and limits its responsibility to signature verification. Tags automatically generate random public keys private keys to ensure that the IoT application tag is unique, authentic, and tamper-resistant. Thereby, tags can reduce the amount of information stored to solve overload with large amounts of data in IoT applications. Moreover, tags solve the problem of slow encryption and decryption in asymmetric encryption technology. Modum fabricates another RFID IoT device called Modum logger temperature. The logger is an IoT temperature sensor

designed for medical products that do not require active cooling during transport. During the shipment process, the monitored temperature is stored in the logger memory. Using Bluetooth technology, the shipment can be checked without opening it. The results of each evaluation are stored in a smart contract inside the immutable Blockchain. This combination of IoT, Bluetooth and smart contract demonstrates that drugs have not been exposed to conditions which may compromise their quality and integrity. Vechain upgrades the chip layer of a traditional IoT component by adding personal identification with an asymmetric key algorithm. It generates random IDs of 20 bytes, hashes and transforms them into In this way, every IoT equipment is defined by a unique ID and asymmetric key. These IDs are managed by smart contracts and permanently stored on the Blockchain. Different technologies can be used to achieve the same goal. Wabi and Everledger are both interested in linking digital and physical assets through IoT and Blockchain. However, they use different IoT tag devices.

Project	**IoT technology**	**IoT role**	**Technology Base**
Modum [103]	Modum temperature logger	Trace drug temperature instantly	Smart contract and BLE
WaltonChain [100]	IOT-RU20 (RFID tag IC and reader IC)	Upload data direct to Blockchain and realizes Anti-counterfeit	UHF Android Smart RFID Reader/Writer
Vechain [101]	Encrypted chips tag technology development	Monitor and trace	Adds ID and asymmetric keys to IoT devices
Wabi [109]	Walimai	Links digital and physical assets through RFID labels	Secure RFID label Authentication is done through mobile consumers
Everledger [117]	Intelligent Labeleing	Links digital and physical assets through RFID, NFC,	NFC, RFID beacons, and synthetic DNA

Table 6.3 IoT-enabled DLT-based supply chain projects

6.6.2 Smart Contract for Transparency Enhancement

The complex manufacturing networks' structures challenge the supply chain transparency and affect the overall collaborative system. The smart contract can reasonably tackle the transparency gap and organize the collaboration. In addition to its central role in drawing legal contracts among Blockchain members, a smart contract enforces the tracking and monitoring of the content of the intended product's data. Some of the Blockchain-based supply chain projects listed in Table 6.2 use smart contracts for transparency enhancement purposes. They integrate it differently, based on their infrastructure needs. In [180], a

smart contract is used for transparency by proposing a framework that interconnects the smart contracts and the manufacturing supply chain' assets. In this proposal, each asset is assigned a unique identification number by generating a particular smart contract stored on the Blockchain. Therefore, the Blockchain ledger can be seen as a database of timestamps that offers anyone the ability to notice that a certain thing has occurred. Ambrosus involves smart contracts in a novel way by introducing two types of smart contracts: measurement and requirement. All the assets and standards are periodically used in the measurement contracts, and the smart contract requirements determine whether a product continuously meets the standards defined by an interested participant in the network. In this framework, the smart contract is utilized as a new protocol to set quality standards and compared directly to the Measurements Smart Contract items. Vechain uses Ethereum virtual machine (EVM) with additional extensions on the contracts called built-ins. It has six smart contract extensions for further data reliability.

Generally, the complexities of attaining transparency are caused by the stakeholder's incompatibility in rules and conditions, leading to difficulties in reconciling transparency requirements. The partners experience the obstacle of not revealing private data while attaining intended transparency. The smart contract is a trusted tool that plays a significant role in achieving transparency and some data privacy. All regulations, rules, and conditions related to different supply chain partners should be collected at the first step to identify the risks and goals. Hence, a smart contract transcribes/records and stores all the regulations, conditions, and risks on the immutable Blockchain ledger. It is committed to executing the partners' recommendations by literally and intelligently following their predefined code content. The smart contract can then help achieve the planning requirement, and can assist it in reaching its targets successfully. Coupling smart contracts with IoT technology interacts directly with the sensors to ensure precise execution. The registered data represent a source of trust for all partners, since it is recorded on an authentic ledger. Finally, the decisions to expose data are taken through a dynamic and trusted platform, considering all the supply chain' network complexities.

6.6.3 Transparency Versus Opacity: Access Control

In addition to the above-mentioned technical limitations, there are further obstacles that would affect the ability to achieve full transparency. Full (uncontrolled) transparency goes against the opacity and privacy required by stakeholders that intend to hide sensitive information such as plans, cost, secret ingredients, etc. In a Blockchain-based supply chain, and since its introduction, Blockchain ensures the use of multiple keys for signing transactions so that, each time, a new key is generated and used once. This method protects user privacy

on the cryptography level. However, it requires an advanced method to enable parties to customize their transparency and opacity levels based on their requirements and regulations. For example, some sensitive data are shared among partners/companies only for collaboration purposes in a supply chain. Thus, the decentralized platform is requested to protect such data from leakage and provide certain opacity using access control. At this level, questions are raised about the effectiveness of the aforementioned techniques on transparency control. How can we mitigate the gap behind Blockchain data transparency and obtain access control?

In this context, the fully decentralized system (public Blockchain) prevents partners from controlling their data as if it were in the centralized systems. This inability to control opacity leads the partners to prefer the private Blockchain to the public one, knowing that the latter is much more recommended for the global supply chain. Hence, there is a need to accomplish the access control feature within the global Blockchain. Table 6.4 depicts the techniques' impacts on the transparency access control, their advantages, and limitations. Starting with the public Blockchain, the ZKP promises to preserve their privacy, encouraging them to go public. Other cryptographic proposals would also have a large impact on data privacy, such as homomorphic encryption integrated with Blockchain [206]. These algorithms protect privacy and advance public Blockchain usage. However, they have a medium impact on data transparency and opacity control. The Merkle tree technique facilitates traceability without exerting a significant impact on the control side. Regarding transparency, smart contracts and IoT techniques can significantly provide access control if employed precisely. The recent projects listed above, which investigated smart contract development, ignore the transparency access control and concentrate on their functionality part only.

To satisfy both transparency and opacity requirements, a hybrid Blockchain is an appropriate solution to regain partners' confidence in the supply chain decentralization. On the one hand, partners are able to run and store their sensitive data off-chain, thus achieving opacity. On the other hand, partners could publish different data to the Blockchain to ensure transparency. In addition, a hybrid smart contract [207] was recently proposed, which permits the control of off-chain data and lets partners build smart contracts that cover both on-chain and off-chain data. In the context of data opacity, improving data transparency leads to more control over data and therefore more control over opacity. Our proposal contributes in providing suitable platform for data transparency enhancements and opacity control.

6.6.4 Summary and Open Issue

The aforementioned projects lack transparency standards to manage and organize the data transparency requirements within the new DLT technology. This study does not prompt actors to choose between different projects (like Vechain, Ambrosus, OriginTrail, etc.). Instead, it

Techniques	Transparency Access Control Impact	Benefits	Limitations
Zero-Knowledge-Proof	Medium	Ensure privacy in public Blockchain and encourage merging supply chains	Unable to recover lost user credentials
Merkle tree	Medium	Facilitate extract and tracking data	Hash collision and overhead syncing
Blockchain core improvement	Low	Facilitate the access control in case of improving transaction format and roles	Have no direct impact unless the improvements become related to data transparency
Smart Contract	Very High	Apply conditioning access control and automate the traceability process	Complexity in a scalable environment
Involvement of IoT devices	High	Rapid data correlation and facilitate automation	Unable to be managed in a vast centralized system

Table 6.4 Current techniques impacts on transparency access control

sheds light on the available techniques. It drives stakeholders to integrate more techniques in different ways to mitigate the gap behind the transparency concerns of the newly introducing DLT-based supply chain. Another goal is to highlight the transparency access control topic and its influence on decentralized supply chain projects. The analyses highlight the open issue related to inventing more tools to improve transparency in general and advance the progress in the transparency/opacity access control in specific. Besides, other cryptographic techniques, such as the ZKP, encourage enterprises to accord with the public Blockchain while conserving their privacy. This technique may drive the adoption of open supply chain platforms in the future. We define three policy enforcement steps to define the transparency requirements and clarify the whole process. After that, any supply chain planning to move into Blockchain could pass through the above policy enforcement steps for the required validation to recognize the best-fit Blockchain type and techniques. Consequently, it can explore the techniques mentioned above that fit its requirements.

As a result of these analyses, the Blockchain offers an attractive embedded transparency feature to the entire supply chain and improves the overall processes. Furthermore, the techniques presented in this study assist in the achievement of further transparency and support supply chain actors in building their platforms. The current Blockchain-based supply chain solutions lack transparency access control, and thus, restructuring their platform

is required. The techniques that could be used are very different. Obviously, the smart contract and IoT techniques have the highest impacts on transparency access control. The IoT technology integrated with smart contracts automates the traceability process to enhance transparency and reduce the overall risks. Nevertheless, the existing Blockchain projects do not have a severe solution to the high proliferation of IoT devices which hinders the IoT/smart contract techniques in enhancing transparency. In this context, our proposal, which is a combination of DAG and Blockchain, enforces the proliferation of IoT devices with smart contracts. Thus, the proposal provides feasible infrastructure and paves the way for a typical DLT platform with data transparency improvements.

6.7 Conclusions

This work highlights essential questions related to the Blockchain-based supply chains' data transparency. It considers the transparency challenges, the DLT transparency techniques, and additional measures that can be employed. Accordingly, the existing projects are presented with their adopted techniques. It is noted that some of them implement standard Blockchain features, including transparency and traceability. However, some other projects exploit additional techniques to enhance transparency and satisfy their requirements. We highlight these techniques and analyze them to investigate their impacts on a Blockchain-based supply chain and to achieve the thesis main goal of typical DLT-based platform for the supply chain. Few projects use alternative methods, such as involving cryptographic tools like Merkle tree and zero-knowledge. IoT technology and an advanced smart contract are the most-used techniques to achieve more transparency, as well as what Blockchain provides. our proposal, which is a combination of DAG and Blockchain, enforces the proliferation of IoT devices with smart contracts. Thus, the proposal provides feasible infrastructure and paves the way for a typical DLT platform with data transparency improvements. We conclude that further enhancements are needed to achieve the required data transparency in the supply chain and to control unlimited access to sensitive data according to the opacity requirements.

Chapter 7

Conclusion and Future Works

DLT is considered a promising solution that addresses the existing supply chain drawbacks, such as independent stakeholders, lack of transparency, and visibility, which lead to traceability issue. While existing centralized supply chains suffer from such limitations, the innovative Blockchain-based supply chain projects do not provide a typical platform suitable for the scalability requirements of huge participants, including the IoT devices. The main problem is that all of the current solutions adopt Blockchain as a decentralized platform and put efforts into addressing its shortcomings. Yet, improving Blockchain components is essential but still cannot be relied on its platform to fully manage the supply chains because the main Blockchain issue is related to its linear block structure, where transactions flow into its ledger are governed by the block rule and consensus mechanism. Therefore, the enormous incoming transactions are objected to latency problem. Previously, we introduced IOTA, the alternative Blockchain which is based on the DAG mechanism. Although the IOTA platform's high scalability and its suitability for IoT environments, the research on running supply chains on the DAG platform are very rare. This refers to the new decentralized concept that is still not ready for the supply chain as it is not entirely decentralized and the smart contract limitation. At this point, we proposed in chapter four a new platform that combines both Blockchain and IOTA as their benefits/drawbacks complement each other. The proposal includes distributed connector which intermediates both DLTs to translate the transaction formats and provide connectivity among Tangle users and their Blockchain ledger. The proposed platform comprises a Tangle application and connector in the front end and a Blockchain running implicitly in the backend. It is worth noting that the supply chain users' visibility is limited to their Tangle platform, where no access is granted to the Blockchain side. Besides, we proposed a resource allocation mechanism that addresses the IOTA distribution tasks and provides load balancing among its nodes.

Once the proposed architecture is settled and validated, we address the transparency

feature and its negative influence on the supply chain that lead to sensitive data revelation with no control. In the last chapter, we analyze all the related works and highlight the transparency impacts. The analysis provides some mechanisms that could be used to enhance transparency. However, the main issue behind this feature is not well-addressed, and further effort is required.

7.1 Contributions

The current Ph.D. thesis contributes to proposing a new DLT platform that tackles the issues behind the massive IoT devices in a supply chain system. The new platform is embodied in a combination of Blockchain and IOTA in which the latter represents the frontend application, and the former represents the backend Blockchain service. Our thesis proposed a distributed connector software running in the middleware for a successful combination. The proposal allows smart contracts to run on the DAG applications while they are executed on the Blockchain ledger. Also, an efficient resource allocation scheme has been introduced to distribute the tasks fairly among IOTA nodes, and it is based on the Weight least Connection load balancing algorithm. Due to many challenges faced by transparency in the supply chain, we elaborated state of art to highlight its requirements and challenges. We also presented how different projects and applications tackled data transparency issues by involving the Blockchain in their core platform differently. Furthermore, we analyzed the projects' techniques and tools utilized to customize transparency. We concluded that further enhancements are needed to set a balance between data transparency and process opacity required by different partners to assure the confidentiality of their processes and control access to sensitive data.

7.2 Discussions and Future Work

Apart from DAG scalability and negligible transaction fees suitable for IoT environments, the combination of Blockchain and IOTA brings many benefits. The IoT data is spread on two different ledgers, which empowers applications to rely on Tangle or Blockchain to get the required data. IOTA takes into consideration the weak IoT resource capabilities and performs snapshots every specific time so that not all data can be found on Tangle. The IoT data are stored on the Tangle ledger and streamed toward the Blockchain ledger, the permanent destination. The permanent database stored in the Blockchain consists of all data starting from genesis until the last transaction. That is, we have no worries about data storage in terms of availability and physical location since it is doubled and distributed throughout

the Blockchain ledger. Therefore, the application investigates the Tangle ledger first for the required data then the Blockchain ledger in case the required data are no longer available on the Tangle. It can be said that the IoT application and its database are partially separated since it has a permanent online full copy in the Blockchain ledger. Furthermore, the latter plays the data backup role for the Tangle nodes in case of corruption or security breaches.

Transactions flow from the application site towards its final destination inside the Blockchain ledger. Hence, Tangle rules will be applied first. That is, Tangle will force Blockchain to follow its footsteps, and as a result, the Tangle is chaining Blockchain. In other words, the features of Tangle are still available, as well as the Blockchain benefits. The ability to work offline is one of the added values of Tangle, where offline nodes create TXs and broadcast them later to the network. On the Blockchain side, Enabling smart contracts on Tangle network is possible, although DAG does not have the concept of time series. The smart contract will be running on the Blockchain platform towards IoT nodes. Besides, This combination eliminates the need for keeping IoT nodes online since storage is a decentralized up and running service. The proposed system supports all IoT devices to be entirely disconnected or powered off during a specific time.

Contrarily to single DLT -either Blockchain or Tangle- users are not relying hardly on each other to execute queries since they have two different data sources, which adds flexibility to the Tangle nodes. In other words, the number of Tangle nodes is independent of Blockchain nodes, and their proliferation does not affect the Blockchain functionality as these nodes are not involved directly in the Blockchain scheme in either mining or block creation. Precisely, Blockchain is only constrained by the number of arrival TXs into its ledger, which could hinder the whole process or suppose delays in TX processes. Finally, the proposal leads us to further future investigations in terms of scalability and the security topic and others. The Below subsections present the topics of our future research:

7.2.1 Rate Control

Every communication network aims to handle the injected traffic of its nodes to control the data system better and to avoid any unpleasant situations. Decentralized systems are similar to any other network in terms of congestions and bottlenecks when it comes to traffic load larger than what the network can manage.

Generally, the proposed connector processes and delivers the incoming transactions immediately to the Blockchain. In high traffic, the transactions are generally processed on the Tangle side with high performance compared to the low traffic because of the DAG nature. Accordingly, the Tangle-based application will not be affected. On the Blockchain side, high transactions could overcharge the Blockchain ledger with high loads and result in further

delays. Actually, the Blockchain is not involved in real-time processing since the application is running on the Tangle. Therefore, the proposal tolerates the delays that occurred to the transactions after being attached to the Tangle. Additionally, the connector can buffer the data to a certain limit if the Blockchain is busy or unavailable.

Ideally, when data streamlines double DLT systems, they should meet an acceptable transaction rate to guarantee the continuity of the platform. The goal is to keep both Tangle and Blockchain in a maximum synchronizing state. The rule of thumb is to respect that the amount of issued Tangle-based TXs does not exceed the Blockchain nodes' capacities too much. The cloud may play an essential role in providing the flexibility of adding nodes on demand and enhancing the Blockchain network to fit the Tangle loads. Also, the tools described previously, such as modifying the core of Blockchain by involving a light consensus algorithm, can provide an accepted performance without troublesome delays. In future work, we will be working on enhancing the transaction rate between Blockchain and IOTA and set the ideal requirements to reach this target. Also, we will sets a synchronization mechanism among these DLTs to negotiate the transaction status.

7.2.2 Security

With the adoption of Blockchain and IOTA across the supply chain ecosystem, we need to ensure that all DLT-related security risks are identified and addressed to maintain the system's safety and stability. During our study, analysis, and implementation of our proposal, we referred to the default security provided by both DLTs. They are considered secure with high immunity against several types of attacks. However, decentralization is usually more vulnerable to security attacks due to its newness or absence of control. On the security level, the connector can be adjusted in our future work to only deliver the high-priority transactions rather than the immediate delivery of tips.

7.3 Publications

1. **Journals Articles**
   First Article: Houssein Hellani, Layth Sliman, Abed Ellatif Samhat, and Ernesto Exposito. "On Blockchain Integration with Supply Chain: Overview on Data Transparency." Logistics 5, no. 3 (July 2, 2021): 46. https://doi.org/10.3390/logistics5030046.
   Second Article: Houssein Hellani, Layth Sliman, Abed Ellatif Samhat, and Ernesto Exposito. "Computing Resource Allocation Scheme for DAG-Based IOTA Nodes."

Sensors 21, no. 14 (July 9, 2021): 4703. https://doi.org/10.3390/s21144703.

Third Article: Houssein Hellani, Layth Sliman, Abed Ellatif Samhat, and Ernesto Exposito. “Overview on the Blockchain-Based Supply Chain Systematics and Their Scalability Tools.” Emerging Science Journal 4 (August 23, 2021): 45–69. https://doi.org/10.28991/esj-2021-SP1-04.

2. **Conferences Articles**
   First Publication: Houssein Hellani, Layth Sliman, Motaz Ben Hassine, Abed Ellatif Samhat, Ernesto Exposito, and Mourad Kmimech. "Tangle The Blockchain: Toward IOTA and Blockchain integration for IoT Environment." In International Conference on Hybrid Intelligent Systems, pp. 429-440. Springer, Cham, 2019.
   Second Publication: Houssein Hellani, Layth Sliman, Abed Ellatif Samhat, and Ernesto Exposito. “Tangle the Blockchain:Towards Connecting Blockchain and DAG”. 30th IEEE International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), 2021, pp. 63-68, https://doi.org/10.1109/WETICE53228.2021.00023.

References

[1] D. Kiel, C. Arnold, M. Collisi, and K.-I. Voigt, "The impact of the industrial internet of things on established business models," in *Proceedings of the 25th international association for management of technology (IAMOT) conference*, pp. 673–695, 2016.

[2] N. Dey, A. E. Hassanien, C. Bhatt, A. Ashour, and S. C. Satapathy, *Internet of things and big data analytics toward next-generation intelligence*. Springer, 2018.

[3] Y. Li, "An integrated platform for the internet of things based on an open source ecosystem," *Future Internet*, vol. 10, no. 11, p. 105, 2018.

[4] I. Lee and K. Lee, "The internet of things (iot): Applications, investments, and challenges for enterprises," *Business Horizons*, vol. 58, no. 4, pp. 431–440, 2015.

[5] F. Griffiths and M. Ooi, "The fourth industrial revolution-industry 4.0 and iot [trends in future i&m]," *IEEE Instrumentation & Measurement Magazine*, vol. 21, no. 6, pp. 29–43, 2018.

[6] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[7] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[8] F. Shrouf, J. Ordieres, and G. Miragliotta, "Smart factories in industry 4.0: A review of the concept and of energy management approached in production based on the internet of things paradigm," in *2014 IEEE international conference on industrial engineering and engineering management*, pp. 697–701, IEEE, 2014.

[9] A. Rejeb, J. G. Keogh, and H. Treiblmaier, "Leveraging the internet of things and blockchain technology in supply chain management," *Future Internet*, vol. 11, no. 7, p. 161, 2019.

[10] M. H. Hugos, *Essentials of supply chain management*. John Wiley & Sons, 4 ed., 2018.

[11] S. Nakamoto, "Bitcoin whitepaper," *URL: https://bitcoin. org/bitcoin. pdf-(: 17.07. 2019)*, 2008.

[12] H. F. Atlam, A. Alenezi, M. O. Alassafi, and G. Wills, "Blockchain with internet of things: Benefits, challenges, and future directions," *International Journal of Intelligent Systems and Applications*, vol. 10, no. 6, pp. 40–48, 2018.

[13] H. Hellani, A. E. Samhat, M. Chamoun, H. E. Ghor, and A. Serhrouchni, "On BlockChain technology: Overview of bitcoin and future insights," in *2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET)*, IEEE, nov 2018.

[14] R. Sekaran, R. Patan, A. Raveendran, F. Al-Turjman, M. Ramachandran, and L. Mostarda, "Survival study on blockchain based 6g-enabled mobile edge computation for iot automation," *IEEE Access*, vol. 8, pp. 143453–143463, 2020.

[15] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for iot," in *2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI)*, pp. 173–178, IEEE, 2017.

[16] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE international congress on big data (BigData congress)*, pp. 557–564, IEEE, 2017.

[17] R. Alexander, *IOTA - Introduction to the Tangle Technology: Everything You Need to Know about the Revolutionary Blockchain Alternative*. Independently published, ISBN:198041887X 2018.

[18] C. Fan, H. Khazaei, Y. Chen, and P. Musilek, "Towards a scalable dag-based distributed ledger for smart communities," in *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, pp. 177–182, Ieee, 2019.

[19] M. Almakhour, L. Sliman, A. E. Samhat, and A. Mellouk, "Verification of smart contracts: A survey," *Pervasive and Mobile Computing*, p. 101227, 2020.

[20] X. Xu, C. Pautasso, L. Zhu, Q. Lu, and I. Weber, "A pattern collection for blockchain-based applications," in *Proceedings of the 23rd European Conference on Pattern Languages of Programs*, ACM, jul 2018.

[21] G. Hileman and M. Rauchs, "2017 global blockchain benchmarking study," *Available at SSRN 3040224*, 2017.

[22] S. Tikhomirov, "Ethereum: state of knowledge and research perspectives," in *International Symposium on Foundations and Practice of Security*, pp. 206–221, Springer, 2017.

[23] A. Wahab and W. Mehmood, "Survey of consensus protocols," *arXiv preprint arXiv:1810.03357*, 2018.

[24] X. Liu, G. Zhao, X. Wang, Y. Lin, Z. Zhou, H. Tang, and B. Chen, "Mdp-based quantitative analysis framework for proof of authority," in *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, pp. 227–236, IEEE, 2019.

[25] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "Pbft vs proof-of-authority: Applying the cap theorem to permissioned blockchain," 2018.

[26] N. Szabo, "The idea of smart contracts," *Nick Szabo's papers and concise tutorials*, vol. 6, no. 1, 1997.

[27] M. Staples, S. Chen, S. Falamaki, A. Ponomarev, P. Rimba, A. Tran, I. Weber, X. Xu, and J. Zhu, "Risks and opportunities for systems using blockchain and smart contracts. data61," *CSIRO), Sydney*, 2017.

[28] C. D. Clack, V. A. Bakshi, and L. Braine, "Smart contract templates: foundations, design landscape and research directions," *arXiv preprint arXiv:1608.00771*, 2016.

[29] G. Governatori, F. Idelberger, Z. Milosevic, R. Riveret, G. Sartor, and X. Xu, "On legal contracts, imperative and declarative smart contracts, and blockchain systems," *Artificial Intelligence and Law*, vol. 26, no. 4, pp. 377–409, 2018.

[30] C. Dannen, *Introducing Ethereum and solidity*, vol. 318. Springer, 2017.

[31] B. Gramlich, "Smart contract languages: A thorough comparison," *ResearchGate Preprint*, 2020.

[32] K. Delmolino, M. Arnett, A. Kosba, A. Miller, and E. Shi, "A programmer's guide to ethereum and serpent," *URL: https://mc2-umd. github. io/ethereumlab/docs/serpent_tutorial. pdf*, pp. 22–23, 2015.

[33] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[34] E. Buchman, *Tendermint: Byzantine fault tolerance in the age of blockchains*. PhD thesis, 2016.

[35] M. Araoz, D. Brener, F. Giordano, S. Palladino, T. Paivinen, A. Gozzi, and F. Zeoli, "zeppelin_os: An open-source decentralized platform of tools and services on top of the evm to develop and manage smart contract applications securely," 2017.

[36] I. Starlander, "Counterparty credit risk on the blockchain," 2017.

[37] M. Divya and N. B. Biradar, "Iota-next generation block chain," *International journal of engineering and computer science*, vol. 7, no. 04, pp. 23823–23826, 2018.

[38] E. Heilman, N. Narula, T. Dryja, and M. Virza, "Iota vulnerability report: Cryptanalysis of the curl hash function enabling practical signature forgery attacks on the iota cryptocurrency," *URL: https://github. com/mit-dci/tangled-curl/blob/master/vuln-iota. md*, 2017.

[39] S. Popov, "The tangle," *cit. on*, p. 131, 2016.

[40] S. Popov, H. Moog, D. Camargo, A. Capossele, V. Dimitrov, A. Gal, A. Greve, B. Kusmierz, S. Mueller, A. Penzkofer, *et al.*, "The coordicide," 2020.

[41] S. Popov and W. J. Buchanan, "Fpc-bi: Fast probabilistic consensus within byzantine infrastructures," *arXiv preprint arXiv:1905.10895*, 2019.

[42] E. F. Codd, *Cellular automata*. Academic Press, 2014.

[43] J. R. Douceur, "The sybil attack," in *International workshop on peer-to-peer systems*, pp. 251–260, Springer, 2002.

[44] T. Koens and E. Poll, "Assessing interoperability solutions for distributed ledgers," *Pervasive and Mobile Computing*, vol. 59, p. 101079, 2019.

[45] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille, "Enabling blockchain innovations with pegged sidechains," *URL: http://www. opensciencereview. com/papers/123/enablingblockchain-innovations-with-pegged-sidechains*, vol. 72, 2014.

[46] B. E. Kwon, J., "Cosmos whitepaper," *Whitepaper. https://github.com/cosmos/ cosmos/blob/master/WHITEPAPER.md*.

[47] S. Thomas and E. Schwartz, "A protocol for interledger payments," *URL https://interledger.org/interledger.pdf*, 2015.

[48] L. Kan, Y. Wei, A. H. Muhammad, W. Siyuan, G. Linchao, and H. Kai, "A multiple blockchains architecture on inter-blockchain communication," in *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, pp. 139–145, IEEE, 2018.

[49] G. Wood, "Polkadot: Vision for a heterogeneous multi-chain framework," *White Paper*, 2016.

[50] Oneledger, "Oneledger white paper," *URL https://www.oneledger.io/hubfs/Website/Whitepaper/oneledger-whitepaper.en.pdf*.

[51] M. Kaleem and W. Shi, "Demystifying pythia: A survey of chainlink oracles usage on ethereum," *arXiv preprint arXiv:2101.06781*, 2021.

[52] Y. Jiang, C. Wang, Y. Wang, and L. Gao, "A cross-chain solution to integrating multiple blockchains for iot data management," *Sensors*, vol. 19, no. 9, p. 2042, 2019.

[53] G. Perboli, S. Musso, and M. Rosano, "Blockchain in logistics and supply chain: A lean approach for designing real-world use cases," *IEEE Access*, vol. 6, pp. 62018–62028, 2018.

[54] B. Lev, S. Radhakrishnan, and W. Zhang, "Organization capital," *Abacus*, vol. 45, no. 3, pp. 275–298, 2009.

[55] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," *International Journal of Production Research*, vol. 57, no. 7, pp. 2117–2135, 2019.

[56] J. Yadav and R. Shevkar, "Performance-based analysis of blockchain scalability metric," *Tehnički glasnik*, vol. 15, pp. 133–142, mar 2021.

[57] H. Haswell and M. Storgaard, "Maersk and ibm unveil first industry-wide cross-border supply chain solution on blockchain," *IBM, http://www-03. ibm. com/press/us/en/-pressrelease/51712. wss*, 2017.

[58] L. He, M. Xue, and B. Gu, "Internet-of-things enabled supply chain planning and coordination with big data services: Certain theoretic implications," *Journal of Management Science and Engineering*, 2020.

[59] M. F. I. Suny, M. M. R. Fahim, M. Rahman, N. T. Newaz, and T. M. N. U. Akhund, "Iot past, present, and future a literary survey," in *Information and Communication Technology for Competitive Strategies (ICTCS 2020)*, pp. 393–402, Springer, 2021.

[60] C.-W. Tsai, C.-F. Lai, M.-C. Chiang, and L. T. Yang, "Data mining for internet of things: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 77–97, 2014.

[61] J. Manyika, M. Chui, P. Bisson, J. Woetzel, R. Dobbs, J. Bughin, and D. Aharon, "The internet of things: mapping the value beyond the hype. mckinsey glob inst 144," 2015.

[62] J.-M. Liang, J.-J. Chen, H.-H. Cheng, and Y.-C. Tseng, "An energy-efficient sleep scheduling with qos consideration in 3gpp lte-advanced networks for internet of things," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 3, no. 1, pp. 13–22, 2013.

[63] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, "Survey on blockchain for internet of things," *Computer Communications*, vol. 136, pp. 10–29, 2019.

[64] B. Westermann, D. Gligoroski, and S. Knapskog, "Comparison of the power consumption of the 2nd round sha-3 candidates," in *International Conference on ICT Innovations*, pp. 102–113, Springer, 2010.

[65] L. Hang and D.-H. Kim, "Design and implementation of an integrated iot blockchain platform for sensing data integrity," *Sensors*, vol. 19, no. 10, p. 2228, 2019.

[66] X. Sun and N. Ansari, "Dynamic resource caching in the iot application layer for smart cities," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 606–613, 2017.

[67] X. Xu, I. Weber, and M. Staples, *Architecture for blockchain applications*. Springer, 2019.

[68] D. Dujak and D. Sajter, "Blockchain applications in supply chain," in *SMART supply network*, pp. 21–46, Springer, 2019.

[69] H. Hellani, L. Sliman, M. Ben Hassine, A. E. Samhat, E. Exposito, and M. Kmimech, "Tangle the blockchain: Toward iota and blockchain integration for iot environment," *Springer 2019 HIS India*, 2019.

[70] Y. Wang, J. H. Han, and P. Beynon-Davies, "Understanding blockchain technology for future supply chains: a systematic literature review and research agenda," *Supply Chain Management: An International Journal*, 2019.

[71] J. Al-Jaroodi and N. Mohamed, "Blockchain in industries: A survey," *IEEE Access*, vol. 7, pp. 36500–36515, 2019.

[72] K. S. Hald and A. Kinra, "How the blockchain enables and constrains supply chain performance," *International Journal of Physical Distribution & Logistics Management*, 2019.

[73] Y. Wang, M. Singgih, J. Wang, and M. Rit, "Making sense of blockchain technology: How will it transform supply chains?," *International Journal of Production Economics*, vol. 211, pp. 221–236, 2019.

[74] M. Pournader, Y. Shi, S. Seuring, and S. L. Koh, "Blockchain applications in supply chains, transport and logistics: a systematic review of the literature," *International Journal of Production Research*, vol. 58, no. 7, pp. 2063–2081, 2020.

[75] R. Azzi, R. K. Chamoun, and M. Sokhn, "The power of a blockchain-based supply chain," *Computers & industrial engineering*, vol. 135, pp. 582–592, 2019.

[76] P. Scully and M. Höbig, "Exploring the impact of blockchain on digitized supply chain flows: A literature review," in *2019 Sixth International Conference on Software Defined Systems (SDS)*, pp. 278–283, IEEE, 2019.

[77] Y. Tribis, A. El Bouchti, and H. Bouayad, "Supply chain management based on blockchain: A systematic mapping study," in *MATEC Web of Conferences*, vol. 200, p. 00020, EDP Sciences, 2018.

[78] P. Helo and Y. Hao, "Blockchains in operations and supply chains: A model and reference implementation," *Computers & Industrial Engineering*, vol. 136, pp. 242–251, 2019.

[79] S. Saberi, M. Kouhizadeh, and J. Sarkis, "Blockchains and the supply chain: Findings from a broad study of practitioners," *IEEE Engineering Management Review*, vol. 47, no. 3, pp. 95–103, 2019.

[80] P. Gonczol, P. Katsikouli, L. Herskind, and N. Dragoni, "Blockchain implementations and use cases for supply chains-a survey," *Ieee Access*, vol. 8, pp. 11856–11871, 2020.

[81] "Ucl cbt report (last access may 2020)," *https://bit.ly/3dO6KeF*.

[82] "Origintrail whitepaper (last accessed on lanuary 2020)," *URL : https://origintrail.io/storage/documents/Origin Trail-White-Paper.pdf*, 2015.

[83] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 17–30, 2016.

[84] A. E. Gencer, R. van Renesse, and E. G. Sirer, "Short paper: Service-oriented sharding for blockchains," in *International Conference on Financial Cryptography and Data Security*, pp. 393–401, Springer, 2017.

[85] H. Dang, T. T. A. Dinh, D. Loghin, E.-C. Chang, Q. Lin, and B. C. Ooi, "Towards scaling blockchain systems via sharding," in *Proceedings of the 2019 international conference on management of data*, pp. 123–140, 2019.

[86] M. Zamani, M. Movahedi, and M. Raykova, "Rapidchain: Scaling blockchain via full sharding," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pp. 931–948, 2018.

[87] Y. Liu, B. Dong, B. Guo, J. Yang, and W. Peng, "Combination of cloud computing and internet of things (iot) in medical monitoring systems," *International Journal of Hybrid Information Technology*, vol. 8, no. 12, pp. 367–376, 2015.

[88] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1508–1532, 2019.

[89] F. H. Pohrmen, R. K. Das, and G. Saha, "Blockchain-based security aspects in heterogeneous internet-of-things networks: A survey," *Transactions on Emerging Telecommunications Technologies*, vol. 30, no. 10, p. e3741, 2019.

[90] J. Kwon and E. Buchman, "Cosmos: A network of distributed ledgers," *URL https://cosmos.network/whitepaper*, 2016.

[91] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," in *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, pp. 1–5, IEEE, 2017.

[92] K. Ashritha, M. Sindhu, and K. Lakshmy, "Redactable blockchain using enhanced chameleon hash function," in *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*, pp. 323–328, IEEE, 2019.

[93] G. Ateniese, B. Magri, D. Venturi, and E. Andrade, "Redactable blockchain–or–rewriting history in bitcoin and friends," in *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, pp. 111–126, IEEE, 2017.

[94] H. Hellani, L. Sliman, A. E. Samhat, and E. Exposito, "On blockchain integration with supply chain: Overview on data transparency," *Logistics*, vol. 5, no. 3, p. 46, 2021.

[95] H. Hellani, L. Sliman, A. E. Samhat, and E. Exposito, "Computing resource allocation scheme for dag-based iota nodes," *Sensors*, vol. 21, no. 14, p. 4703, 2021.

[96] S. Panikkar, S. Nair, P. Brody, and V. Pureswaran, "Adept: An iot practitioner perspective," *IBM 2015*, 2015.

[97] L. Baird, M. Harmon, and P. Madsen, "Hedera: A governing council & public hashgraph network," *The trust layer of the internet, whitepaper*, vol. V1 2018, 2018.

[98] J. McKinney, "Light client protocol," *github. com/ethereum/wiki/wiki/Light-client-protocol*, 2017.

[99] "Iota light nodes vs full nodes," *https://iota.readme.io/v1.2.0/docs/light-vsfull-node*.

[100] "Waltonchain whitepaper (last access may 2020," *URL https://www.waltonchain.org/upload/1507947 652573.pdf*, 2017.

[101] "Vechain whitepaper," *Homepage: https://vechain.com*.

[102] "Ambrosus whitepaper," *URL : https://whitepaperdatabase.com/ambrosus-amb-whitepaper*.

[103] "Modum whitepaper," *URL https://whitepaper.io/document/213/modum-whitepaper*.

[104] "Shipchain whitepaper 2017 (last access may 2020)," *https://shipchain.io*.

[105] "Devery whitepaper 2017 (last access may 2020," *https://devery.io/*.

[106] "cargox whitepaper 2015," *https://cargox.io/*.

[107] "cargocoin whitepaper (last access may 2020)," *https://thecargocoin.com/docs/CargoCoin-Whitepaper.pdf*, 2018.

[108] "Bext360 (last access may 2020)," *https://www.bext360.com/*, 2016.

[109] "Tael wabi, 2017 (last access may 2020)," *https://www.taelpay.com/*, 2017.

[110] "Te-food whitepaper," *https://www.te-food.com/te-food-white-paper.pdf*, 2015.

[111] "Farmtrust whitepaper 2019," *URL https://www.farmatrust.com/*.

[112] "Blockgrain whitepaper 2018," *URL https://pages.agrichain.com*.

[113] "Iota blog (2020)," *URL https://blog.iota.org/zero-defects-digital-twins-and-iota-8568f54c3925*.

[114] B. B. A.-C. Solution, "Blockverify.io," 2017.

[115] "Chronicled inc.,linking the physical world to the blockchain, 2016," *Available: http://www.chronicled.com/*.

[116] N. Lomas, "Everledger is using blockchain to combat fraud, starting with diamonds," *Tech Crunch*, vol. 29, 2015.

[117] g. d. c. exchange, "White paper transforming diamonds into a new financial asset class,"

[118] S. Malik, S. S. Kanhere, and R. Jurdak, "Productchain: Scalable blockchain framework to support provenance in supply chains," in *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)*, pp. 1–10, IEEE, 2018.

[119] "Trademarkea," *URL www.trademarkea.com*.

[120] F. Tian, "An agri-food supply chain traceability system for china based on rfid & blockchain technology," in *2016 13th international conference on service systems and service management (ICSSSM)*, pp. 1–6, IEEE, 2016.

[121] "Devery whitepaper 2017 (last access october) 2020," *https://devery.io/*.

[122] "Bext360 (last access october 2020)," *https://www.bext360.com/*, 2016.

[123] S. Kim, Y. Kwon, and S. Cho, "A survey of scalability solutions on blockchain," in *2018 International Conference on Information and Communication Technology Convergence (ICTC)*, pp. 1204–1207, IEEE, 2018.

[124] X. Li, Y. Wang, and X. Chen, "Cold chain logistics system based on cloud computing," *Concurrency and Computation: Practice and Experience*, vol. 24, no. 17, pp. 2138–2150, 2012.

[125] L. R. Saragih, M. Dachyar, T. Y. M. Zagloel, and M. Satar, "The industrial iot for nusantara," in *2018 IEEE International Conference on Internet of Things and Intelligence System (IOTAIS)*, pp. 73–79, IEEE, 2018.

[126] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and iot integration: A systematic survey," *Sensors*, vol. 18, no. 8, p. 2575, 2018.

[127] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A survey on the adoption of blockchain in iot: Challenges and solutions," *Blockchain: Research and Applications*, p. 100006, 2021.

[128] P. K. Sharma, N. Kumar, and J. H. Park, "Blockchain technology toward green iot: Opportunities and challenges," *IEEE Network*, vol. 34, no. 4, pp. 263–269, 2020.

[129] G. Yu, X. Wang, K. Yu, W. Ni, J. A. Zhang, and R. P. Liu, "Survey: Sharding in blockchains," *IEEE Access*, vol. 8, pp. 14155–14181, 2020.

[130] Litecoin, "The cryptocurrency for payments, available online: https://litecoin.org/,"

[131] E. Lombrozo, J. Lau, and P. Wuille, "Segregated witness (consensus layer)," *Bitcoin Core Develop. Team, Tech. Rep. BIP*, vol. 141, 2015.

[132] M. A. Javarone and C. S. Wright, "From bitcoin to bitcoin cash: a network analysis," in *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, pp. 77–81, 2018.

[133] X. Dai, J. Xiao, W. Yang, C. Wang, and H. Jin, "Jidar: A jigsaw-like data reduction approach without trust assumptions for bitcoin system," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, pp. 1317–1326, IEEE, 2019.

[134] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, "Omniledger: A secure, scale-out, decentralized ledger via sharding," in *2018 IEEE Symposium on Security and Privacy (SP)*, pp. 583–598, IEEE, 2018.

[135] A. Manuskin, M. Mirkin, and I. Eyal, "Ostraka: Secure blockchain scaling by node sharding," in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pp. 397–406, IEEE, 2020.

[136] H. C. Team, "Hercules whitepaper," *Available at SSRN 3442330*, 2018.

[137] Harmony, "Harmony" available online: https://harmony.one,"

[138] "Ethereum sharding 2.0, ethereum sharding 2.0" buterin. ethereum sharding faq. available online: https://github.com/ethereum/wiki/wiki/ sharding-faq.,"

[139] "Logos available online: https://cryptodiffer.com/logos-network-ico,"

[140] ""nxt" whitepaper available online: https://whitepaper.io/coin/nxt,"

[141] "Lemahieu, colin. "nano: A feeless distributed cryptocurrency network." nano 16 (2018): 17. available online: https://nano.org/en/whitepaper,"

[142] A. Churyumov, "Byteball: A decentralized system for storage and transfer of value," *URL https://byteball. org/Byteball. pdf*, 2016.

[143] Y. Lewenberg, Y. Sompolinsky, and A. Zohar, "Inclusive block chain protocols," in *Financial Cryptography and Data Security*, pp. 528–547, Springer Berlin Heidelberg, 2015.

[144] Y. Sompolinsky, Y. Lewenberg, and A. Zohar, "Spectre: a fast and scalable cryptocurrency protocol.," *IACR Cryptol. ePrint Arch.*, vol. 2016, no. 1159, 2016.

[145] Y. Sompolinsky and A. Zohar, "Phantom," *IACR Cryptology ePrint Archive, Report 2018/104*, 2018.

[146] C. Li, P. Li, D. Zhou, Z. Yang, M. Wu, G. Yang, W. Xu, F. Long, and A. C.-C. Yao, "A decentralized blockchain with high throughput and fast confirmation," in *2020 {USENIX} Annual Technical Conference ({USENIX}{ATC} 20)*, pp. 515–528, 2020.

[147] Y. Ribero and D. Raissar, "Dagcoin whitepaper," *Whitepaper, no. May*, pp. 1–71, 2018.

[148] J. Teutsch and C. Reitwießner, "A scalable verification solution for blockchains," *arXiv preprint arXiv:1908.04756*, 2019.

[149] H. Kalodner, S. Goldfeder, X. Chen, S. M. Weinberg, and E. W. Felten, "Arbitrum: Scalable, private smart contracts," in *27th {USENIX} Security Symposium ({USENIX} Security 18)*, pp. 1353–1370, 2018.

[150] M. Shaw, "Procedure calls are the assembly language of software interconnection: Connectors deserve first-class status," in *Workshop on Studies of Software Design*, pp. 17–32, Springer, 1993.

[151] F. Akgul, *ZeroMQ*. Packt Publishing Ltd, 2013.

[152] A. M. Antonopoulos and G. Wood, *Mastering ethereum: building smart contracts and dapps*. O'reilly Media, 2018.

[153] L. Vigneri, W. Welz, A. Gal, and V. Dimitrov, "Achieving fairness in the tangle through an adaptive rate control algorithm," in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 146–148, IEEE, 2019.

[154] D. Grosu and A. T. Chronopoulos, "Noncooperative load balancing in distributed systems," *Journal of parallel and distributed computing*, vol. 65, no. 9, pp. 1022–1034, 2005.

[155] A. M. Alakeel *et al.*, "A guide to dynamic load balancing in distributed computer systems," *International Journal of Computer Science and Information Security*, vol. 10, no. 6, pp. 153–160, 2010.

[156] P. Beniwal and A. Garg, "A comparative study of static and dynamic load balancing algorithms," *International Journal of Advance Research in Computer Science and Management Studies*, vol. 2, no. 12, pp. 1–7, 2014.

[157] R. V. Rasmussen and M. A. Trick, "Round robin scheduling–a survey," *European Journal of Operational Research*, vol. 188, no. 3, pp. 617–636, 2008.

[158] Y. Shengsheng, Y. Lihui, L. Song, and Z. Jingli, "Least-connection algorithm based on variable weight for multimedia transmission," in *World Scientific and Engineering Academy and Society*, pp. 1441–1445, 2002.

[159] IOTA-documents, "Run a goshimmer node," *https://docs.iota.org/docs/node-software/0.1/goshimmer/how-to-guides/run-the-node*.

[160] "Iota foundation https://docs.iota.org/docs/load-balancer/1.0/overview,"

[161] H. Hellani, L. Sliman, A. E. Samhat, and E. Exposito, "Github," in *https://github.com/housseinh/IOTA-WLC (accessed on Juin 2021)*.

[162] K. Birman, "The promise, and limitations, of gossip protocols," *ACM SIGOPS Operating Systems Review*, vol. 41, no. 5, pp. 8–13, 2007.

[163] S. Voulgaris, M. Jelasity, and M. Van Steen, "A robust and scalable peer-to-peer gossiping protocol," in *International Workshop on Agents and P2P Computing*, pp. 47–58, Springer, 2003.

[164] V. Roy, "Contrasting supply chain traceability and supply chain visibility: are they interchangeable?," *The International Journal of Logistics Management*, 2021.

[165] C. D. E. 1981-2019., "data transparency. the computer language company inc. 20 feb. 2021 https://encyclopedia2.thefreedictionary.com/data+transparency,"

[166] M. Barratt, "Understanding the meaning of collaboration in the supply chain (2004)," *Supply Chain Management: an international journal 9(1), 30–42*, 2004.

[167] F. O. Olorunniwo and X. Li, "Information sharing and collaboration practices in reverse logistics (2010)," *Supply Chain Management: An International Journal*, 2010.

[168] U. Ramanathan, "Performance of supply chain collaboration–a simulation study," *Expert Systems with Applications*, vol. 41, no. 1, pp. 210–220, 2014.

[169] Y.-H. Chen, T.-P. Lin, and D. C. Yen, "How to facilitate inter-organizational knowledge sharing: The impact of trust," *Information & Management*, vol. 51, no. 5, pp. 568–578, 2014.

[170] S. E. Fawcett, M. A. Waller, and A. M. Fawcett, "Elaborating a dynamic systems theory to understand collaborative inventory successes and failures," *The International Journal of Logistics Management*, 2010.

[171] M. Zorzini, L. C. Hendry, F. A. Huq, and M. Stevenson, "Socially responsible sourcing: reviewing the literature and its use of theory," *International Journal of Operations & Production Management*, 2015.

[172] J. H. Grimm, J. S. Hofstetter, and J. Sarkis, "Exploring sub-suppliers' compliance with corporate sustainability standards," *Journal of Cleaner Production*, vol. 112, pp. 1971–1984, 2016.

[173] Y. Li, "An integrated platform for the internet of things based on an open source ecosystem," *Future Internet*, vol. 10, no. 11, p. 105, 2018.

[174] S. Agarwal *et al.*, *Blockchain technology in supply chain and logistics*. PhD thesis, Massachusetts Institute of Technology, 2018.

[175] F. Longo, L. Nicoletti, A. Padovano, G. d'Atri, and M. Forte, "Blockchain-enabled supply chain: An experimental study," *Computers & Industrial Engineering*, vol. 136, pp. 57–69, 2019.

[176] A. Brun, H. Karaosman, and T. Barresi, "Supply chain collaboration for transparency," *Sustainability*, vol. 12, no. 11, p. 4429, 2020.

[177] V. Venkatesh, K. Kang, B. Wang, R. Y. Zhong, and A. Zhang, "System architecture for blockchain based transparency of supply chain social sustainability," *Robotics and Computer-Integrated Manufacturing*, vol. 63, p. 101896, 2020.

[178] T. A. Gardner, M. Benzie, J. Börner, E. Dawkins, S. Fick, R. Garrett, J. Godar, A. Grimard, S. Lake, R. K. Larsen, *et al.*, "Transparency and sustainability in global commodity supply chains," *World Development*, vol. 121, pp. 163–177, 2019.

[179] K. Francisco and D. Swanson, "The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency," *Logistics*, vol. 2, no. 1, p. 2, 2018.

[180] F. Dietrich, D. Palm, and L. Louw, "Smart contract based framework to increase transparency of manufacturing networks," *Procedia CIRP*, vol. 91, pp. 278–283, 2020.

[181] Z. Liu and Z. Li, "A blockchain-based framework of cross-border e-commerce supply chain," *International Journal of Information Management*, vol. 52, p. 102059, 2020.

[182] I. J. Fraser, M. Mueller, and J. Schwarzkopf, "Transparency for multi-tier sustainable supply chain management: A case study of a multi-tier transparency approach for sscm in the automotive industry," *Sustainability*, vol. 12, no. 5, p. 1814, 2020.

[183] C. Hsu, *Service science: design for scaling and transformation*. World Scientific, section 8.1 page 245, 2009.

[184] T. Anthony, "Supply chain collaboration: success in the new internet economy," *Achieving supply chain excellence through technology*, vol. 2, pp. 41–44, 2000.

[185] L. Liu, X. Liu, and X. Li, "Cloud-based service composition architecture for internet of things," in *Internet of Things*, pp. 559–564, Springer, 2012.

[186] M. Ahlmeyer and A. M. Chircu, "Securing the internet of things: A review.," *Issues in information Systems*, vol. 17, no. 4, 2016.

[187] Q. Gou, L. Yan, Y. Liu, and Y. Li, "Construction and strategies in iot security system," in *2013 IEEE international conference on green computing and communications and IEEE internet of things and IEEE cyber, physical and social computing*, pp. 1129–1132, IEEE, 2013.

[188] S. M. Idrees, M. Nowostawski, R. Jameel, and A. K. Mourya, "Security aspects of blockchain technology intended for industrial applications," *Electronics*, vol. 10, no. 8, p. 951, 2021.

[189] R. Jacob, J.-J. Lesage, and J.-M. Faure, "Opacity of discrete event systems: models, validation and quantification," *IFAC-PapersOnLine*, vol. 48, no. 7, pp. 174–181, 2015.

[190] D. Linich, "The path to supply chain transparency: a practical guide to defining, understanding, and building supply chain transparency in a global economy," *Deloitte Consulting LLP, Cincinnati, OH, USA*, 2014.

[191] M. Rauchs, A. Glidden, B. Gordon, G. C. Pieters, M. Recanatini, F. Rostand, K. Vagneur, and B. Z. Zhang, "Distributed ledger technology systems: a conceptual framework," *Available at SSRN 3230013*, 2018.

[192] F. Tian, "An agri-food supply chain traceability system for china based on rfid & blockchain technology," in *2016 13th international conference on service systems and service management (ICSSSM)*, pp. 1–6, IEEE, 2016.

[193] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains everywhere-a use-case of blockchains in the pharma supply-chain," in *2017 IFIP/IEEE symposium on integrated network and service management (IM)*, pp. 772–777, IEEE, 2017.

[194] M. Crosby, P. Pattanayak, S. Verma, V. Kalyanaraman, *et al.*, "Blockchain technology: Beyond bitcoin," *Applied Innovation*, vol. 2, no. 6-10, p. 71, 2016.

[195] M. J. Casey and P. Wong, "Global supply chains are about to get better, thanks to blockchain," *Harvard business review*, vol. 13, pp. 1–6, 2017.

[196] G. W. Peters and E. Panayi, "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money," in *Banking beyond banks and money*, pp. 239–278, Springer, 2016.

[197] T. Bocek and B. Stiller, "Smart contracts–blockchains in the wings," in *Digital marketplaces unleashed*, pp. 169–184, Springer, 2018.

[198] O. Goldreich and Y. Oren, "Definitions and properties of zero-knowledge proof systems," *Journal of Cryptology*, vol. 7, no. 1, pp. 1–32, 1994.

[199] F. Fatz, P. Hake, and P. Fettke, "Confidentiality-preserving validation of tax documents on the blockchain," *Proc. 15. Internationale Tagung Wirtschaftsinformatik (WI 2020)*, 2020.

[200] Z. Gao, L. Xu, L. Chen, X. Zhao, Y. Lu, and W. Shi, "Coc: A unified distributed ledger based supply chain management system," *Journal of Computer Science and Technology*, vol. 33, no. 2, pp. 237–248, 2018.

[201] N. MAOURIYAN and A. A. KRISHNA, "Aquachain-water supply-chain management using distributed ledger technology," in *2019 3rd International Conference on Computing and Communications Technologies (ICCCT)*, pp. 204–207, IEEE, 2019.

[202] "whitepaper (last access january 2021," *Available: https://fr8.network/wp-content/uploads/2021/01/Fr8-Network- Whitepaper.pdf.*

[203] "whitepaper (last access january 2021," *Available: https://s3.amazonaws.com/nextpakk-assets/docs/pakka-icowhitepaper. pdf.*

[204] D. K. Mishra, A. Sekhari, S. Henry, and Y. Ouzrout, "Traceability in product supply chain: a global model," in *IFIP International Conference on Product Lifecycle Management*, pp. 377–384, Springer, 2016.

[205] A. Tzounis, N. Katsoulas, and T. Bartzanas, "Internet of things in agriculture, recent advances and future challenges.," *Biosyst.Eng.*, vol. 164, pp. 31–48, 2017.

[206] R. Shrestha and S. Kim, "Integration of iot with blockchain and homomorphic encryption: Challenging issues and opportunities," in *Advances in Computers*, vol. 115, pp. 293–331, Elsevier, 2019.

[207] R. Bennett, T. Miller, M. Pickering, and A.-K. Kara, "Hybrid approaches for smart contracts in land administration: Lessons from three blockchain proofs-of-concept," *Land*, vol. 10, no. 2, p. 220, 2021.