



HAL
open science

Enhancing *Maritime Logistics* with **Blockchain Technology**: Application to secure and trace dangerous goods in smart ports

Rim Abdallah

► **To cite this version:**

Rim Abdallah. Enhancing *Maritime Logistics* with *Blockchain Technology*: Application to secure and trace dangerous goods in smart ports. Computer Science [cs]. Normandie Université, 2024. English. NNT: 2024NORMLH05 . tel-04652638

HAL Id: tel-04652638

<https://theses.hal.science/tel-04652638>

Submitted on 18 Jul 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

THÈSE

Pour obtenir le diplôme de doctorat

Spécialité **INFORMATIQUE**

Préparée au sein de l'**Université Le Havre Normandie**

**Enhancing Maritime Logistics with Blockchain Technology:
Application to secure and trace dangerous goods in smart
ports**

Présentée et soutenue par

RIM ABDALLAH

Thèse soutenue le 18/06/2024

devant le jury composé de :

M. CYRILLE BERTELLE	PROFESSEUR DES UNIVERSITES - Université Le Havre Normandie	Directeur de thèse
M. YOUNES BENNANI	Professeur à l' Université de Paris XIII - UNIVERSITE PARIS 13 PARIS-NORD	Membre du jury
M. JÉRÔME BESANCENOT	DOCTEUR - HAROPA PORT	Membre du jury
MME SAMIA BOUZEFRANE	PROFESSEUR DES UNIVERSITES - CNAM DE PARIS	Membre du jury
M. CLAUDE DUVALLET	MAÎTRE DE CONFERENCES - Université Le Havre Normandie	Membre du jury
M. FRANÇOIS VERDIER	PROFESSEUR DES UNIVERSITES - UNIVERSITE CÔTE D'AZUR	Rapporteur du jury
MME BESMA ZEDDINI	MAÎTRE DE CONFERENCES (HDR) - CY TECH CERGY PARIS	Rapporteur du jury

Thèse dirigée par **CYRILLE BERTELLE** (LABORATOIRE D'INFORMATIQUE DE TRAITEMENT DE L'INFORMATION ET DES SYSTEMES)



AUTHOR'S PUBLICATION LIST

Peer Reviewed articles and Journal

- Abdallah R, Besancenot J, Bertelle C, Duvallet C, Gilletta F. (2023). An Extensive Preliminary Blockchain Survey from a Maritime Perspective. *Smart Cities*. 6(2):846-877.(Abdallah et al., 2023e)
- Abdallah, R., Besancenot, J., Bertelle, C., Duvallet, C., Gilletta, F. (2023). Seamless Seas Leveraging Blockchain. *International Conference on Cybersecurity, Cybercrimes, and Smart Emerging Technologies (CCSET2023)*. 5-7 December 2023 | Riyadh, Saudi Arabia. (Abdallah et al., 2023f)
- Abdallah, R., Bertelle, C., Besancenot, J., Duvallet, C., Gilletta, F. (2023). Repositioning Blockchain Technology in the Maritime Industry for Increased Accountability. In: Machado, J.M., et al. *Blockchain and Applications, 5th International Congress. BLOCKCHAIN 2023. Lecture Notes in Networks and Systems, vol 778*. Springer, Cham. (Abdallah et al., 2023a)
- Abdallah, R., Bertelle, C., Besancenot, J., Duvallet, C., Gilletta, F. (2023) Blockchain for the maritime : A modular proposition. In *proceedings of French Conference on Complex Systems (FrCCS 2023)*, pp 438-441, May 31- June 2, Le Havre, France. (Abdallah et al., 2023b)
- Abdallah, R., Bertelle, C., Besancenot, J., Duvallet, C., Gilletta, F. (2023) Privileging permissioned blockchain deployment for the maritime sector. In *proceedings of French Conference on Complex Systems (FrCCS 2023)*, pp 446-449, May 31- June 2, Le Havre, France. (Abdallah et al., 2023c)
- Abdallah, R., Besancenot, J., Bertelle, C., Duvallet, C., Gilletta, F. (2023). Assessing Blockchain Challenges in the Maritime Sector. In: Prieto, J., Benítez Martínez, F.L., Ferretti, S., Arroyo Guardado, D., Tomás Nevado-Batalla, P. (eds) *Blockchain and Applications, 4th International Congress . BLOCKCHAIN 2022. Lecture Notes in Networks and Systems, vol 595*. Springer, Cham. (Abdallah et al., 2023d)
- Abdallah, R., Bertelle, C., Duvallet, C., Besancenot, J., Gilletta, F. (2022). Blockchain Potentials in the Maritime Sector: A Survey. In: Daimi, K., Al Sadoon, A. (eds) *Proceedings of the ICR'22 International Conference on Innovations in Computing Research. ICR 2022*.

Advances in Intelligent Systems and Computing, vol 1431. Springer, Cham. (Abdallah et al., 2022)

- Abdallah, R., Abdallah, R. (2022). A Blockchain Based Methodology for Power Grid Control Systems. In: Daimi, K., Al Sadoon, A. (eds) Proceedings of the ICR'22 International Conference on Innovations in Computing Research. ICR 2022. Advances in Intelligent Systems and Computing, vol 1431. Springer, Cham. (Abdallah and Abdallah, 2022).
- Simon C, Abdallah R, Bertelle C, Duvallet C. (2021) Simulateur du passage portuaire d'un conteneur avec notarisation dans une blockchain sous Ethereum pour certifier sa traçabilité. Smart Corridors and Logistics. 2021 Nov 24:89. (Serry, 2022)
- HBS | Harvard teaching case : Beyond Borders with Blockchain – Deloitte's Digital Vision

Certificates and awards

Best speaker award

During The 4th International Congress on Blockchain and Applications in 2022 we won the best speaker award for our paper presentation.

Hackathon Winner

During the 6th International Blockchain School 2023 we were voted among the top three projects for the Deloitte use case.

United Nations Conference on Trade and Development Certified

UNCTAD empowerment programme for national trade facilitation committees - The use of blockchain in trade facilitation

RÉSUMÉ

Cette thèse s'inscrit à l'avant-garde de la logistique maritime et explore le potentiel transformateur de la technologie blockchain pour améliorer la traçabilité de la chaîne d'approvisionnement et faciliter l'échange de données sécurisé et multi-source.

À travers une analyse approfondie des applications de la blockchain, ce travail de recherche examine méticuleusement comment cette technologie émergente peut contribuer de manière significative à renforcer la transparence, la traçabilité et la sécurité au sein du commerce international. En s'appuyant sur un cadre théorique complet et des études de cas concrets, cette étude universitaire met en lumière les défis et les opportunités à multiples facettes liés à l'intégration de la blockchain dans la logistique maritime. Elle évalue de manière critique l'impact de cette technologie sur la traçabilité des données critiques au sein des systèmes d'information maritimes, telles que les marchandises dangereuses et les journaux d'identification, avec le potentiel de s'étendre à un échange de données inter et intra plus large.

Cette thèse vise non seulement à enrichir les connaissances universitaires, mais également à servir d'appel à l'action pour les innovateurs et les décideurs politiques des secteurs maritime et technologique. Elle préconise une approche innovante qui favorise un engagement plus profond avec les possibilités de transformation offertes par la blockchain. Cette approche considère la blockchain non pas comme un substitut, mais comme une couche complémentaire aux systèmes d'information maritime existants. Elle envisage une intégration et une utilisation transparentes d'une technologie blockchain personnalisée et évaluée au sein du secteur maritime, garantissant ainsi sa cohérence avec les exigences spécifiques de l'industrie et les tendances actuelles de numérisation. Ce travail de recherche vise à fournir des éclairages qui permettent de mieux comprendre les implications de la technologie blockchain pour le paysage en évolution du commerce et de la logistique mondiaux.

Mots-clés : Ports intelligents, traçabilité, blockchain.

ABSTRACT

At the forefront of maritime logistics, this dissertation explores the transformative potential of blockchain technology to enhance supply chain traceability and facilitate secure, multi-source data exchange.

Through a deep analysis of blockchain applications, the research meticulously examines how this emerging technology can significantly elevate transparency, strengthen traceability, and fortify security within the global trade arena. By weaving together a comprehensive theoretical framework and real-world case studies, this scholarly endeavour sheds light on the multifaceted challenges and opportunities associated with integrating blockchain into maritime logistics. It critically evaluates the technology's impact on the traceability of critical data within maritime information systems, such as dangerous goods and identification logs, with the potential to extend to broader inter- and intra-data exchange.

This dissertation not only contributes to academic knowledge but also serves as a compelling call to action for innovators and policymakers in the maritime and technology sectors. It advocates for an innovative approach that fosters deeper engagement with the possibilities of blockchain-driven transformation. This approach views blockchain not as a replacement, but as a complementary layer to existing maritime information systems. It envisions seamless integration and utilization of customized and evaluated blockchain technology within the maritime sector, ensuring its coherence with industry-specific requirements and ongoing digitization trends. This research aims to provide insights that enhance the understanding of blockchain technology's implications for the evolving global trade and logistics landscape.

Keywords: Smart ports, traceability, Blockchain.

ACKNOWLEDGEMENTS

This journey of academic and professional exploration through my CIFRE thesis has been a remarkable chapter of my life, filled with learning and growth. I extend my heartfelt gratitude to all who have contributed to this endeavour, making this achievement not just possible but also incredibly rewarding.

Firstly, I wish to express my deepest appreciation to Mr. Cyrille Bertelle and Mr. Claude Duvallet, my academic supervisors at the University of Le Havre, Normandie. I am equally grateful to Mr. Jérôme Besancenot and Mr. Frédéric Gilletta, my industry mentors at HAROPA PORT. Thank you for your invaluable guidance, unwavering support, and insightful critiques throughout this research journey. Your expertise, encouragement, and dedication have been pivotal in shaping both my work and my academic growth.

I warmly thank all the jury members, including Ms. Samia Bouzefrane and Mr. Younès Bennani, for their great interest in my work. I also thank the reviewers, Mr. François Verdier and Ms. Besma Zeddini for taking on the task of critically reading this thesis.

My sincere thanks to HAROPA PORT and the National Association for Technological Research, for financially supporting my research through the CIFRE agreement. This unique partnership between academia and industry has been essential in facilitating my research and providing me with a comprehensive learning experience.

More generally, I thank all HAROPA PORT and University of Le Havre personnel and members of our teams with whom I have had the opportunity to exchange and work, who have also been a support throughout this journey, including Laboratory Director Mr. Laurent Heutte, Co-director of LITIS (le Havre), Mr. Eric Sanlaville, the Director of Terminals, Performance and Finances, Mr. Sylvain Levieux, computer development engineer, Mr. Florent Val, and computer system architect, Mr. Valentin Sibille. Your perspectives and feedback have been invaluable to my research and personal development.

I am thinking of all the professors and administrative staff I have met, who were always attentive and in good spirits! I also think of all the doctoral students, as well as those who are now doctors.

Special thanks to my family and friends, whose love, understanding, and patience have been my stronghold. Your unwavering belief in my capabilities and your constant encouragement have kept me motivated and focused throughout this journey. Without you, I would probably not be where I am today.

In loving memory of those who are no longer with us.

DEDICATION

For my parents, with all my love ...

CONTENTS

Author’s publication list	i
Résumé	iii
Abstract	v
Acknowledgements	vii
Dedication	ix
Contents	ix
List of Figures	xvi
List of Tables	xvii
Abbreviations	xix
1 General Introduction	1
1.1 Background and context	1
1.1.1 A history lesson	1
1.1.2 Community Systems	4
1.1.3 Traceability: A valuable feature of information systems	7
1.1.4 PCS for dangerous goods: About Timad	10
1.2 Motivation	10
1.3 Problem formulation and research questions	11
1.4 Research Scope	14
1.5 Thesis Structure and contributions	15
I State of the art	19
2 Blockchain technology Overview	21
2.1 Introduction to blockchain	22
2.2 Conceptual Understanding	25
2.2.1 The evolution and distinctiveness of distributed ledgers	25
2.2.2 Key Concepts and Properties of Blockchain	26

CONTENTS

- 2.2.3 Decentralization and Distribution 29
- 2.2.4 Consensus Mechanisms 29
- 2.2.5 Traceability and immutability amongst other characteristics 30
- 2.2.6 Smart Contracts: An evolution 31
- 2.2.7 Digital Wallets: The Gateway to Blockchain Interactions 33
- 2.2.8 Oracles 34
- 2.3 Blockchain topology 36
 - 2.3.1 Centralized Architectures: A State-of-the-Art-Overview 36
 - 2.3.2 Between distributed and decentralised 36
 - 2.3.3 Public, permissioned and private blockchains 37
- 3 Blockchain in the maritime sector 41**
 - 3.1 Maritime Information Systems 42
 - 3.1.1 The Genesis and Evolution of Community Systems 43
 - 3.1.2 Between Port and Cargo Community Systems 43
 - 3.1.3 Functionalities of Community Systems 44
 - 3.1.4 IMO: Into the maritime landscape 44
 - 3.1.5 Continuous Evolution and the Introduction of the MSW System 45
 - 3.2 Change prospects vs Innovational Resiliency 49
 - 3.2.1 Blockchain interest for the sector 50
 - 3.2.2 Partial Recognition and early adopters 51
- II Contributions: Implementing Blockchain for the maritime: from theory to proof of concept 55**
- 4 An Analysis from a Maritime Perspective on Blockchain 57**
 - 4.1 Bridging Blockchain’s Promise and Maritime Realities: A Pragmatic Approach to Sectoral Adoption 60
 - 4.1.1 An evident based approach 60
 - 4.1.2 key takeaways 69
 - 4.2 A methodology reflexion 70
 - 4.3 How can blockchain enhance the maritime industry’s performance? 70
 - 4.3.1 A global decentralized communication system 71
 - 4.3.2 Increase operational efficiency 71
 - 4.3.3 Reduced Data Storage 73
 - 4.3.4 Adjoint supplementary security priviliges 73
 - 4.3.5 Prevent and decrease pollutions 73
 - 4.3.6 Fight Fraud and prevent corruption 75
 - 4.3.7 Eliminate unnecessary intermediaries 76

4.3.8	An Extended Spectrum of Use Cases	76
4.4	Blockchain Challenges	78
4.4.1	Blockchain’s limited use outside of the private sector	78
4.4.2	Blockchain predates regulations	78
4.4.3	Scrutiny: The Result of Transparency	79
4.4.4	Security Challenges	79
4.4.5	Network and Technical Challenges	80
4.4.6	Data and Storage	80
4.4.7	The Nexus between Code and Logic in Business	82
4.4.8	Smart Contracts	83
4.4.9	Oracles	83
4.4.10	Interoperability	83
4.4.11	Common Code Sense	84
4.4.12	Unquantifiable Clauses	84
4.5	Discussion	85
5	Implementing Blockchain for the maritime: Preliminary work	89
5.1	PoC Specifications	90
5.2	Theoretical and Empirical Foundations	90
5.2.1	The Diffusion of Innovations Theories (Doi)	91
5.2.2	The Port: A key link for technological advancement	91
5.3	Implementation Approach	96
5.3.1	Technology Stack	96
5.3.2	Design principles	99
5.3.3	A Solution Strategy: Blockchain-based BAT access	101
5.3.4	Simulative Environment and Role of HAROPA PORT in the PoC	105
5.4	Towards implementation	106
6	Technical implementation - A blockchain infrastructure	107
6.1	Integrating Blockchain with Existing PCS Infrastructure	107
6.2	High-Level Conceptualization for Blockchain Integration	108
6.2.1	Current PCS State	109
6.2.2	Data Integration in Blockchain Implementation with TIMAD v2	110
6.3	Network Architecture	111
6.3.1	Envisioning the Integrated Blockchain-PCS Environment	111
6.4	Creating a Secure Blockchain environment	111
6.5	Organizational Structure	115
6.5.1	Permissions and roles	119

CONTENTS

- 7 Timad Oriented blockchain developments 129**
 - 7.1 About the network’s workflow 130
 - 7.2 PCS Blockchain liaisons 130
 - 7.3 Blockchain functioning logic 132
 - 7.3.1 Into Smart contracts 133
 - 7.4 Client targeted development | TIMAD 137
 - 7.5 Seamless Integration of Blockchain Infrastructure 144
 - 7.6 User-Centric Ledger Interaction within TIMAD 146

- 8 PoC Evaluation and Future Prospects 151**
 - 8.1 Evaluation of the Proposed PoC 151
 - 8.1.1 Evaluation Environment 152
 - 8.1.2 Network Communication Validation 153
 - 8.1.3 Hyperledger Fabric Implementation 154
 - 8.1.4 Performance Definition 155
 - 8.2 On-going Future works 158
 - 8.3 Inter-maritime Operations 159
 - 8.3.1 A maritime implementation 162
 - 8.4 Conclusion 165

- 9 Conclusion and future directions 169**
 - 9.1 Future Directions : Sharding 171
 - 9.2 Conclusion 174

- References 176**

- Appendix 202**
 - A Smart contracts algorithm 203**

LIST OF FIGURES

1	The seven types of cargo ships	3
2	Evolution of New Generation Container Ships (Brooks et al., 2014)	4
3	Normandy terminal port of Le Havre	6
4	A block is a group of transactions : An illustration by the author	22
5	A chain of blocks illustrated by the author	23
6	A network of nodes illustrated by the author	24
7	Hash function algorithm (St Denis and Johnson, 2007)	27
8	Merkle tree illustration by the author	28
9	Oracle role representation in a blockchain environment elaborated by the author.	35
10	An exemplary representation of port community members before and after PCS: a single-window solution elaborated by the author.	43
11	Maritime Information Systems taxonomy elaborated by the author.	48
12	Actors' strategic requirements analysis for a single-window system elaborated by the author.	49
13	A Conceptual architecture for the maritime sector	72
14	An illustration by the author of an example of a container's journey through PCSs across the globe	94
15	All hazardous materials transiting through the Port of Le Havre must be declared in the form of a 'Manifest' declaration. - TIMAD	103
16	Add a new manifest - TIMAD	103
17	Add a new manifest: List of possible dangerous goods - TIMAD	104
18	An illustration by the author of TIMAD v2 operational aspects	109
19	An illustration by the author of the envisioned wanted State	112
20	An illustration by the author of the created secure communication infrastructure	121
21	An illustration by the author of the created blockchain infrastructure	124
22	An illustration by the author of each peer ledger's components	125
23	An illustration by the author of the full created blockchain infrastructure	127
24	An illustration by the author: Timad as a client application within the secure blockchain environment	132
25	Bat Smart contracts	134

LIST OF FIGURES

26 Manifest Smart contract 135

27 BAT Access logic within PCS systems 135

28 Manifest Smart contract 136

29 First Time Connecting to TIMAD - Default connection page 138

30 First Time Connecting to TIMAD - BAT access prompt 138

31 First Time Connecting to TIMAD - Society creation 139

32 Society creation : A Seamless blockchain workflow integration woven into the fabric of the PCS 140

33 Manifest related Operations via TIMAD - Manifests List 142

34 Auth API 143

35 POST API 143

36 Get API 143

37 Blockchain related requests 143

38 Block queried data 144

39 A simplified TIMAD-Blockchain interaction scheme 145

40 A diagrammatic representation of the seamless integration of blockchain within the maritime logistics ecosystem, illustrating minimal impact on existing infrastructure and IS. 145

41 Snapshot of the TIMAD interface displaying all societies created within the system 147

42 Snapshot of the TIMAD interface displaying ledger information seamlessly integrated within the user’s workflow - All Societies view 147

43 Ledger information - A deleted Society 148

44 Deletion operation 156

45 An illustration of the envisioned maritime environment 162

46 A blockchain-based maritime platform for maritime entities 164

47 A full-scale blockchain-based maritime environment 167

48 Database Sharding (ByteByteGo, 2024) 172

LIST OF TABLES

2.1	Characteristics of different types of Blockchain	38
3.1	Blockchain projects' use cases in the maritime sector.	52
4.1	Extending blockchain's spectrum of domain applications.	77
8.1	PCS host machine characteristics	152
8.2	Blockchain host machine characteristics	153
8.3	Software versions	155
8.4	Smart Contract POST Test Results	157
8.5	Smart Contract GET Test Results	157

AIS	Automatic Identification System
AN	Ammonium Nitrate
API	Application Programming Interface
BAT	brokered authoritative transitional
CA	Certificate Authority
CS	Community Systems
CCS	Cargo Community System
DHT	Distributed Hash Tables
DLT	Distributed Ledger Technology
EDI	electronic data interchange
FAL	Facilitation of International Maritime Traffic
GUI	Graphical User Interface
HF	Hyperledger Fabric
IMDG	International Maritime Dangerous Goods
IMO	International Maritime Organization
IoT	Internet of Things
IPCSA	International Port Community System
IS	Information System
ISO	International Organization for Standardization
ITU	International Telecommunication Union
JWT	JSON Web Token
MSP	Membership service provider
MSW	Maritime Single Window
PCS	Port Community System
PoC	Proof of Concept
SC	Smart Contract
SDK	Software development Kit
SW	Single Window
SOLAS	Safety of Life at Sea
TLS	Transport Layer Security
TX	Transaction
UN/CEFACT	United Nations Centre for Trade Facilitation and Electronic Business
VGM	Verified Gross Mass
WWW	World Wide Web

GENERAL INTRODUCTION

Contents

1.1 Background and context	1
1.1.1 A history lesson	1
1.1.2 Community Systems	4
1.1.3 Traceability: A valuable feature of information systems	7
1.1.4 PCS for dangerous goods: About Timad	10
1.2 Motivation	10
1.3 Problem formulation and research questions	11
1.4 Research Scope	14
1.5 Thesis Structure and contributions	15

When the container ship Ever Given ran aground in the Suez Canal in March 2021 (Lee and Wong, 2021), global supply chains ground to a halt, costing billions in lost trade. This incident revealed the intricately interconnected nature of modern maritime commerce and the cascading effects even a single event can have on the increasingly complex technological systems underpinning today’s shipping networks. Today’s massive container ships and sophisticated ports form the backbone of global supply chains, with maritime trade facilitating an estimated 90 per cent of world commerce (Gu and Liu, 2023). As the sector remains a vital lifeline for international trade and the global economy, it also faces pressing challenges requiring innovative solutions and technological evolution. Today, we’re on the brink of a new digital transformation that has the potential to significantly influence global shipping: Blockchain technology.

1.1 Background and context

1.1.1 A history lesson

Maritime trade has its origins in ancient civilizations when human curiosity spurred seafaring voyages to explore the horizon. Vital sea routes enabling goods exchange were established as early as 3000 BCE (Chew, 2001). Early innovations in shipbuilding and naval technology laid the foundations for essential maritime commerce. As ship designs advanced from sail to steam,

Chapter 1. General Introduction

and hull construction from wood to steel, the maritime sector expanded significantly. A pivotal development came in the 1950s as containerized shipping was introduced.

Prior to containerization, ports functioned primarily as rudimentary loading and unloading points where cargo was manually managed. The introduction of container ships, capable of transporting numerous metal crates, necessitated a transformative shift in port operations. Containerization enabled the massification of cargo transportation.

It revolutionized global maritime trade by enabling efficient intermodal transportation. With uniform containers that could be easily transferred between ships, trains and trucks, the volume of cargo able to be transported by sea drastically increased. By allowing products to be shipped in larger batches, containers drove economies of scale and substantially reduced per-unit costs. Consequently, containerized seaborne trade became integral to global supply chains and just-in-time manufacturing and delivery systems that emerged.

Facing exponential growth in demand, the container shipping industry focused on optimal operations and efficiency to remain competitive while expanding economically. Larger (cf. Figure 2) and more diverse ships (cf. Figure 1) were built to accommodate surging volumes.

Port and terminal infrastructure upgraded with sizable gantry cranes designed for rapid loading/unloading of containers, along with purpose-built staging areas for container storage and transfer. As experts in container operations, ports took on more responsibilities across the intermodal supply chain (Singh, 2022).

Furthermore, the implementation of intermodal yards facilitated the seamless transfer of containers between rail and truck transport modes. As vessel capacities surged, docks underwent dredging efforts to accommodate deeper drafts. This robust expansion of port infrastructure played a pivotal role in propelling the remarkable growth of containerized shipping, which now serves as the bedrock of contemporary global supply chains. Nevertheless, this exponential increase in container volumes brought forth novel challenges in terms of traceability and tracking.

In the pre-containerization era, tracing was extremely limited, and goods were manually loaded with minimal documentation or identifiers. With the substantial growth of container volumes, ships now carried thousands of metal boxes with little visibility into their specific contents. This lack of granular traceability created major inefficiencies and risks. Cargo could sit unidentified for days, incurring heavy demurrage fees. Customs processes were hampered by missing data, causing shipment delays. Product recalls were nearly impossible without container-level traceability (Broeze, 2017).

To address these issues, ports gradually instituted more rigorous shipment documentation and primitive tracking measures. Paper manifests listing contents, origin/destinations, ports, and cargo serial numbers provided a minimum level of traceability. However, limited data sharing between maritime actors still hindered visibility. It quickly became evident that enhanced traceability was essential for both business optimization and regulatory compliance.

Shippers needed real-time tracking to improve logistics coordination, meet customer demands, and minimize inventory costs. Port authorities required detailed visibility to expedite

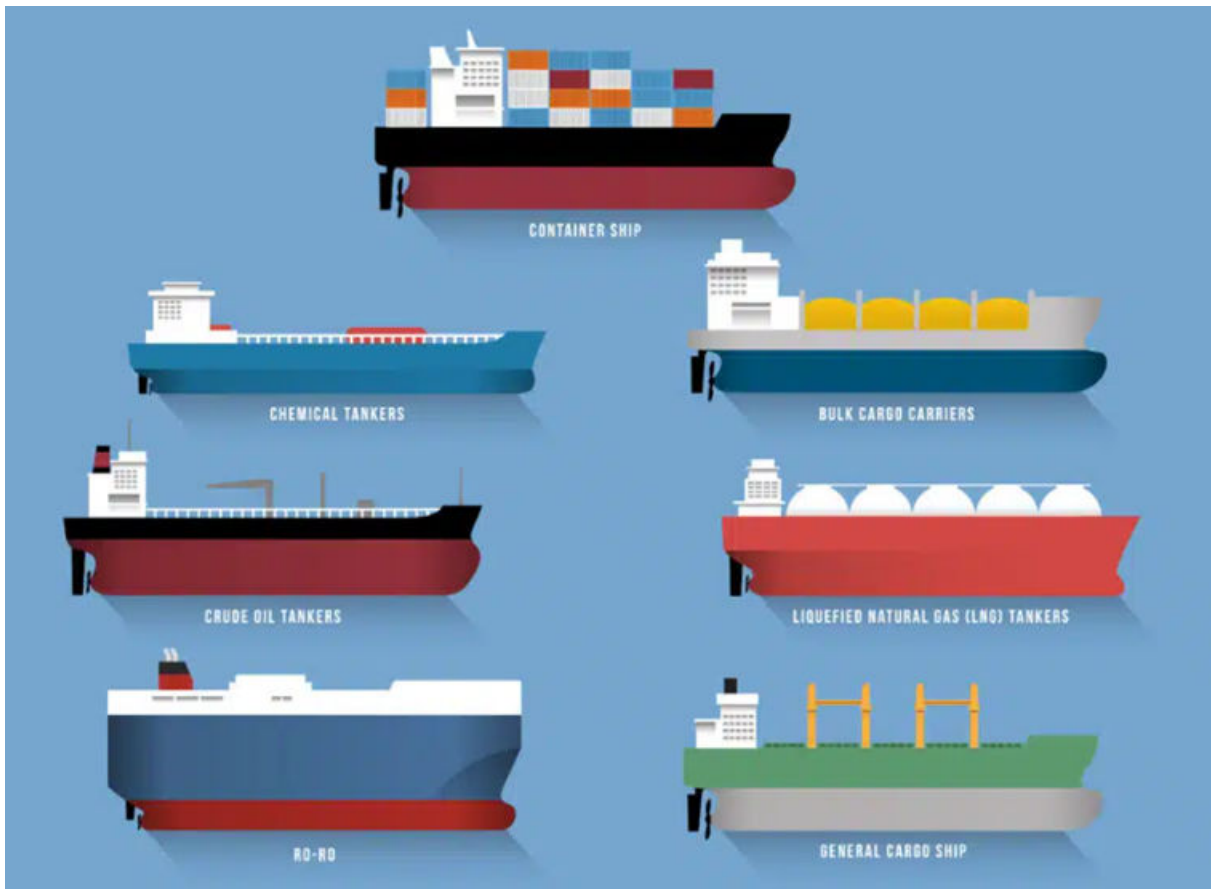


Figure 1: The seven types of cargo ships

clearances, improve security, and reduce congestion. These pressing needs along with the parallel emergence of digital technologies drove its integration into the sector to simplify data sharing across maritime supply chains.

Emerging technologies provide an opportunity to transition from physical to electronic records. Early computing systems allowed basic digital data storage. Port authorities and shippers alike began adopting mainframe computers and databases to maintain shipment logs and manifests electronically rather than solely on paper. This assumed faster information retrieval and sharing between entities.

Electronic Data Interchange However, the proprietary digital systems adopted by different actors within the maritime ecosystem presented new complexities. With shipping lines, freight forwarders, port authorities, customs brokers, and others maintaining distinct platforms, electronic data interchange (EDI) between organizations became extremely challenging. This fragmentation hampered attempts to benefit from the transition to digital traceability.

The next wave of advancement for the maritime came with EDI (Electronic Data Interchange) standards introduced in the late 20th century (Heilig et al., 2017). The need to smooth multi-party data flows led to the application of EDI technology, initially pioneered for military logistics systems. EDI introduced standardized structured messaging allowing automated transfer of

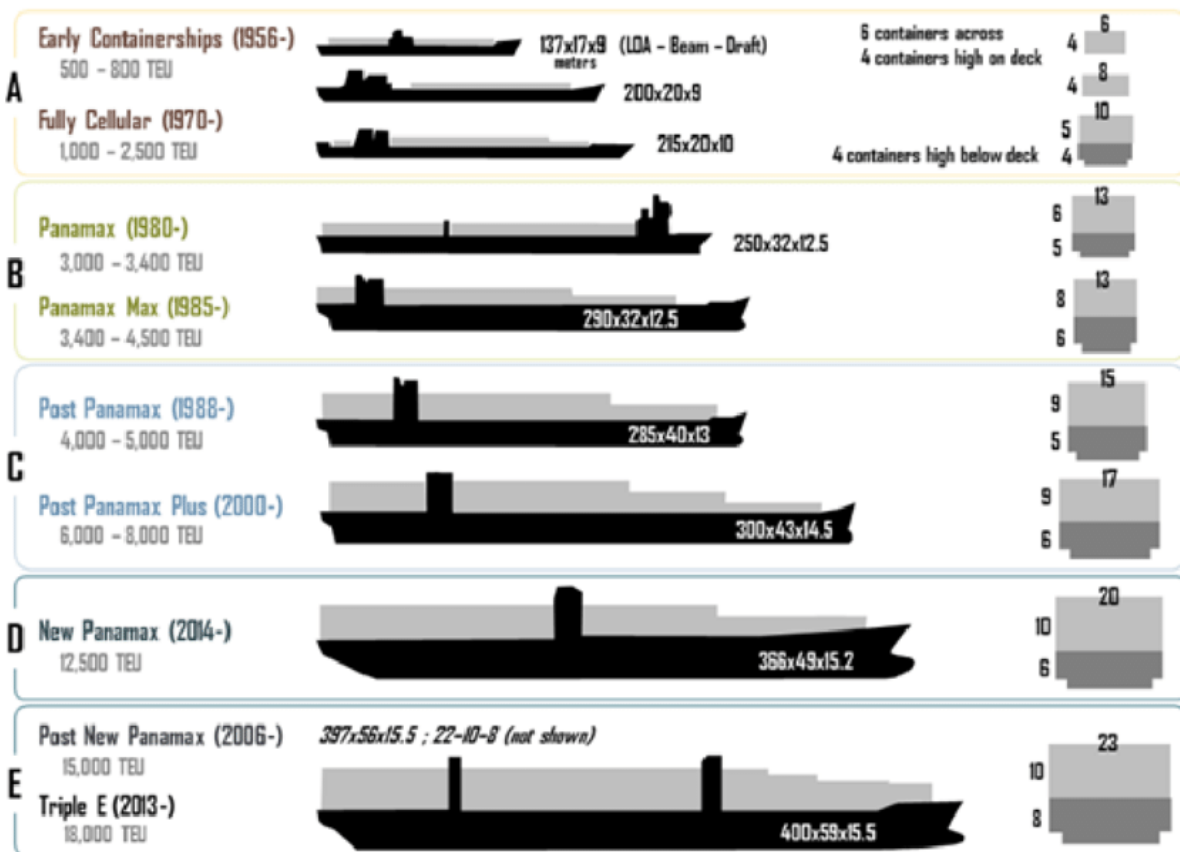


Figure 2: Evolution of New Generation Container Ships (Brooks et al., 2014)

shipment information between diverse platforms. Its conceptual underpinnings took form at the Berlin Airlift of 1948, which required streamlined logistics processes between air forces. Early EDI applications were replicated in the maritime sector. By structuring data into common codified formats, EDI delivered dramatic improvements in supply chain visibility, efficiency, and control. Standardized electronic manifests, cargo booking, and status updates enhanced granular traceability across fragmented information ecosystems. These exemplified initial efforts and the digital integration for maritime supply chains that laid the groundwork for today's clearance programs.

1.1.2 Community Systems

The integration of Electronic Data Interchange (EDI) standards into the maritime industry stands as a seminal transformation, reshaping the operational landscape and ushering in a new era of technological sophistication. This pivotal shift fundamentally redefined the modus operandi of maritime logistics, transcending conventional paradigms.

Moreover, the strategic clustering of businesses within portuary zones established a synergistic collaborative ecosystem. This coalescence of major industry players ranging from shipping companies to logistics experts highlighted the ports' digital vital roles on top of the evolution of its physical infrastructure and responsibilities. The efficiencies promised by these hubs and

spoke models required enhanced coordination amongst port community members to parallel the electronic data exchange adopted by the segregated various actors.

The proliferation of isolated information systems amongst various port stakeholders such as terminals, customs authorities, rail yards, and freight forwarders initially hampered unified visibility. Additionally, analogue paper processes proved inadequate given the pace and intricacies of trade and the need for a seamless transition between a diverse array of transportation modes. Hence a pressing need to unify stakeholders within a digital ecosystem quickly manifested.

Even as digital technologies allowed more data capture, lack of integration meant actors retained fragmented views of port operations. This hindered efforts to optimize processes and maximize benefits. It is crucial to underscore that this transformative period unfolded against the backdrop of an era preceding the widespread proliferation of peer-to-peer communication technologies (Androutsellis-Theotokis and Spinellis, 2004). Consequently, it was within this context that a new topology for maritime information systems emerged.

Exigency necessitated more sophisticated centralized platforms. As we proceed to tackle this information system evolution, we first need to define the port milieu. As stated by (Stopford, 2008), It proves beneficial to distinguish among three distinct entities within the environment, specifically: the port itself, the overseeing port authority, and the terminal infrastructure. These three entities come together to embody an interfacial liaison between the sea and the land. They amenities to merchant vessels and their cargo, alongside multimodal distribution, and all corresponding logistical endeavours. (Bichou, 2013).

- The port delineates the loading and unloading cargo geographical zone between land and sea (Stopford, 2008)
- Port Authority is the custodian overseeing port operations and maritime services integral to expediting vessels' arrival and departures. The architecture of their superstructure, however, varies significantly across public, private, and hybrid models. Public port authorities typically operate under governmental control, exemplified by entities such as the Port of Rotterdam Authority, governed by public regulations and policies. Scholars like Notteboom (Notteboom and Winkelmanns, 2001) have studied this structure, highlighting its emphasis on public interests and infrastructure development. Conversely, private port authorities, as depicted in research by (Verhoeven, 2010) are managed by private entities focused on profit maximization and operational efficiency. Hybrid models, as expounded by (Van Der Lugt et al., 2013) blend public and private interests, striving for a balance between commercial viability and public service obligations. These distinct architectural variations reflect divergent priorities in governance, management strategies, and stakeholder engagements within port authorities worldwide. The diverse superstructures of port authorities, whether public, private, or hybrid, significantly influence the development and implementation of technological advancements within port infrastructure. These variations in governance models often shape the pace, scale, and strategies of digitization

Chapter 1. General Introduction

and information system adoption. Consequently, impacting the efficiency, transparency, and interoperability of port operations accordingly.

- The Terminal (cf. Figure 3) is a designated area within a port's premises containing berths specialized for handling various cargo types. Terminal ownership structures differ across ports (e.g. shipping operators, port authorities), to efficiently manage goods flow (Stopford, 2008).



Figure 3: Normandy terminal port of Le Havre

These three entities constitute the beating heart of the maritime ecosystem. As the need for more sophisticated centralized communication platforms became apparent, Port Community Systems (PCS) and Cargo Community Systems (CCS) came to fruition revolving around these entities. (Stopford, 2008) expounds on the port environment, later embodied in the evolution of maritime systems. The foundational components of this milieu underline the nature of PCS and CCS. PCS tends to focus more on the port authority and the general port environment, while CCS leans toward terminals and is oriented towards shipping operators. These maritime systems embody centralized platforms reflecting different roles and orientations within distinct maritime information systems that facilitate data exchanges.

The inception of these information systems can be traced back to the late 20th century. They aimed to streamline communication and data sharing, stemming from centralised architecture between the numerous and distinct stakeholder clusters within the portuary areas. Their development gained momentum through collaborative efforts between all the stakeholders present and the distinct governing superstructure. The establishment of these systems was culminated and repudiated worldwide adjusting to the different superstructures and infrastructure. This creates various centralised platforms in the portuary environment that revolutionized the efficiency and transparency of maritime logistics.

These new platforms completely changed how data was handled, creating a single channel where everyone involved could easily share vital information. It was a huge change from the old ways of using lots of manual work and paper-based systems to this new digital way of exchanging

standardized data. This shift did not just make ports work better; it also made sharing information in the wider maritime industry much smoother and more organized.

The evolution of PCS and CCS, with the different superstructures and infrastructures utilized globally in portuary areas, has seen a gradual convergence in their functionalities. The distinct roles they once held within the maritime sphere role were blurred. Over time, the dichotomy led to confusion as systems evolved and stakeholders sought integrated solutions for comprehensive data exchange. This is why we refrain from a clear definition of the roles of these information systems in this introductory context cover.

According to the International Port Community System Association (IPCSA), these platforms are defined as “an open electronic platform that connects individual existing systems and databases of distinct companies and organizations” (Carlan et al., 2016b). This definition highlights the mentioned progression of the maritime information systems allowing secure and efficient communication within the ecosystem. In France, there are well-established frameworks for PCS and CCS. The country has implemented various digital initiatives to enhance efficiency and streamline processes within the industry. PCS and CCS such as (Timad, S)ONE, Ci5, . . .) play crucial roles in facilitating information exchange among stakeholders, optimizing logistics, and improving overall port operations. Several ports in France have adopted and integrated these systems to varying degrees. For instance, major ports like Marseille, Le Havre, Dunkirk, and others have implemented PCS and CCS to enhance their operational effectiveness, cargo handling, and logistics management. However, the specific details and implementations might vary among different ports and regions within France.

By providing shared data infrastructure, these systems fulfilled the need for system integration to maximize benefits from port community clustering. Their successes demonstrated the potentials of common digital ecosystems in maritime supply chains, paving the way for today’s smart port initiatives and global platforms.

A Setting Stone Despite their universality of purpose, the organizational principles and material configuration of ports exhibit considerable heterogeneity. Rather than adhering to a common archetype, the diverse contingencies surrounding each port promote tailored architectures that render every node distinctive in structure and practice.

Industry leaders recognized digitizing documentation flows could provide transparency, efficiency and coordination across multiple parties.

1.1.3 Traceability: A valuable feature of information systems

As these Information systems evolved, the critical importance of cargo traceability came to the forefront. With mounting risks from piracy, terrorism, hazardous materials, contraband, the need to track cargo movement and provenance across multiple handlers became an industry priority (Carlan et al., 2017). Port community and cargo systems, with their centralised data architectures,

Chapter 1. General Introduction

provided the foundations to enable granular monitoring across complex, interconnected logistics networks spanning vessels, ports, inland transporters and warehouses.

Traceability necessitates capturing data at every exchange point between actors across end-to-end supply chains (Wang, 2018). As emphasized in (Kelepouris et al., 2007) this requires standardized identification protocols for assets and event logging at material state changes. Consequently, the initial focus on documentation digitization within maritime systems expanded to incorporate unique identifiers, messaging standards and shared reference data for cargo, containers, conveyances and locations. Here we distinguish between physical and digital traceability.

Physical traceability refers to the ability to track the physical movement and state changes of assets through the supply chain. This requires linking the unique identity of assets (e.g. serial numbers on products) to the documentation of events when they move location or change state (e.g. when a product is unloaded from a ship).

Digital traceability builds on physical traceability by digitizing the documentation and data exchange at each process step. This means assigning digital identifiers (e.g. barcodes, RFID tags) to traceable assets which can then be scanned and linked to electronic event logs and supply chain data exchanges.

The initial focus around traceability in maritime shipping and ports was on digitizing paper-based documentation such as bills of lading and customs forms to enable digital information flows. However, full end-to-end digital traceability also requires standardized identification of physical objects like containers and cargo to link with these digital documentation systems.

Traceability via interconnected information systems and physical/digital asset tracking has become instrumental to improving maritime supply chain performance, promoting regulatory concessions, and proactively monitoring safety and sustainability. Standards bodies have introduced protocols like ISO6346 for container identification numbers (for Standardization, 2022) and GS1 standards for logistics units and product serialized tracking (GS1 Switzerland, 2022). These standardized ID formats allow data to be effectively exchanged and understood between different companies in the end-to-end chain.

For example, The International Maritime Organization (IMO) Convention for Safety of Life at Sea (SOLAS) specifically mandates container weight verification via certified methods like International Organization for Standardization (ISO) traceability standards to enable ship stability calculations and safe cargo loading (GCaptain, 2014).

Beyond loading efficiency, traceability also enables transparency for customs, biosecurity, and product authenticity to facilitate cargo flows under programs like ASEAN's National Single Windows framework (Suvannaphakdy, 2020).

By standardizing the digital communication and linkage of vessel, voyage, transport equipment, cargo, and event data to physical assets, both operational visibility and regulatory compliance are significantly enhanced. Specifically, maritime safety has greatly benefited from the adoption of Automatic Identification System (AIS) transponders. These devices are capable of digitally broadcasting the locations of all commercial and passenger vessels in near real-time,

in accordance with International Telecommunication Union (ITU) standards. This technological advancement has led to improved vessel traffic monitoring, marking a pivotal improvement in maritime operations. (Yeasmin et al., 2016). AIS data is actively used by port authorities to promote CDM (collaborative decision making) practices regulating risky cargo handling like ammonium nitrate transfers, enforce speed limits, validate regions of refuge and predict vessel arrivals - reducing misfiling, congestion and environmental risks (United Nations Statistics Division, 2023).

Traceability, both physical and digital including all types of data, in the maritime sector is paramount. It ensures accurate monitoring and linkage of vessel, cargo, and event data, bolstering operational visibility and regulatory compliance. It significantly enhances maritime safety by enabling swift response mechanisms, minimizing risks.

Emphasizing the significance of this feature within the maritime information system, are distressing instances of traceability failures in maritime history. These occurrences stand as a stark reminder of the critical need for seamless data tracking and linkage across vessel operations and cargo handling. Among these instances, the most recent and devastating was the catastrophic Beirut port explosion in 2020, claiming the lives of over 200 individuals and injuring thousands. The mishandling of improperly stored ammonium nitrate (AN), compounded by insufficient port oversight and fragmented governance (Valsamos et al., 2021), amplified the hazards. Investigations uncovered fundamental deficiencies in the visibility of dangerous cargo for port officials, emergency services, and the public, despite earlier flagged irregularities in AN shipment. This tragedy starkly contrasts the proactive measures taken by industrialized ports such as Brisbane, which have implemented rigorous coordination across the AN supply chain post-Beirut. This involves collaboration among port authorities, terminals, ships, trucks, emergency agencies, and the community.

The incident raised concerns about the global transportation conditions of ammonium nitrate (AN), highlighting the issue significantly. In response, stringent oversight during custody transfers in the supply chain has been emphasized as a critical priority, in line with the United Nations' recommendations for reducing the risks associated with AN (United Nations Environment Programme, 2021). For instance, Brazil has demonstrated a robust approach to managing the importation of large AN volumes through correct traceability, accountability, and adherence to strict laws and regulations over the past five decades.

These cases demonstrate how in the modern era, proper tracing and monitoring of hazardous goods is critical for identifying risks and responding appropriately to avert tragedies. Ultimately, they illustrate on polar ends that standardized identification, tracking and transparency of risky maritime cargo still presents a pressing governance priority - underlining how integrated traceability systems could play a fundamental role in advancing port safety.

Dangerous goods The traceability of dangerous goods within maritime information systems, particularly PCSs (PCS), constitutes a critical aspect in ensuring safety, compliance, and efficient

handling of hazardous cargo across global trade routes. Regulatory bodies like the International Maritime Organization (IMO) impose stringent guidelines such as the International Maritime Dangerous Goods (IMDG) Code to govern the transportation of such containers. PCS, serving as a centralized authority, integrates various stakeholders and functionalities within the maritime supply chain, fostering transparency and accountability.

Within this framework, PCS operates as the nerve centre orchestrating a comprehensive workflow. It begins with shippers and consignees submitting detailed documentation on dangerous goods, including classification, packaging, and handling instructions. This information, crucial for risk assessment and planning, undergoes scrutiny by port authorities adhering to regulatory mandates. Integration of this data into the PCS establishes a digital trail, ensuring traceability throughout the goods' journey.

The workflow encompasses multiple stages, from pre-arrival notifications to cargo manifest creation, terminal handling, and eventual delivery. Compliance checks at each juncture validate adherence to safety protocols and regulatory prerequisites. Through PCS, stakeholders access real-time updates, facilitating informed decision-making and preemptive measures in case of deviations or emergencies. This centralized architecture not only enhances operational efficiency but also augments safety by minimizing risks associated with the handling and transportation of hazardous materials.

1.1.4 PCS for dangerous goods: About Timad

Among the array of emerging PCS architectures seeking to transform supply chain visibility and coordination (Boullauazan et al., 2023), particularly regarding hazardous materials, a subset of specialized solutions aims to address the pronounced complexities of dangerous goods governance. While the centralized architectures of traditional community platforms offer vital baseline functionality, as (Doerry and Fireman, 2009) analyze, the deeply multifaceted demands of overseeing dangerous cargo necessitate purpose-built systems.

Attuned to the intricate acceleration and compression intrinsic to hazardous materials oversight, pioneering solutions like TIMAD (Traçabilité Informatisée des Matières Dangereuses) at the port of le Havre known today as HAROPA PORTsignify bespoke PCS manifestations tailored to the task with exacting precision. By consolidating diverse tracking data streams into integrated command centres focused wholly on orchestrating dangerous goods flows, such platforms catalyze new benchmarks in governance capability, compliance, and port ecosystem coordination.

1.2 Motivation

While centralized electronic data interchange platforms represented major progress for maritime logistics, limitations around interoperability, transparency, and cybersecurity have become

1.3. Problem formulation and research questions

increasingly evident. This motivates the exploration of emerging technologies with transformational potential to propel the next phase of advancement. And despite monumental technological leaps, the maritime shipping sector has often been regarded as lagging in adopting innovations that have disrupted other industries (Hoagland et al., 2010). Surveys of maritime executives affirm this perception of the industry as resistant to change, with 85% deeming it “slow to adopt” new technologies as per (Morley, 2017).

Yet amid this inertia, blockchain’s decentralized architecture signifies a breakthrough innovation with immense potential for maritime logistics governance and supply chain integration. By overcoming centralization flaws through distributed consensus and cryptographic validation principles, blockchain could enhance transparency, resilience, inclusion and sustainability across port ecosystems.

This pioneering research is motivated by a genuine interest in assessing the potential future impacts of such a disruptive innovation on an industry known for its technological conservatism. It involves a comprehensive study that evaluates technological capabilities within the sector, positions Blockchain within the industry, and conducts an extensive analysis. This analysis not only aims to enrich the maritime literature and cover the gaps but also deduces a customized implementation plan, leading to the proposed proof-of-concept targeting a particular PCS, TIMAD. This proof-of-concept offers a vital testbed for evaluating decentralized ledger adoption, addressing both general obstacles and those specific to the sector. Leveraging the technological maturity of Blockchain. This research contributes to the enhancement of the efficiency, safety, and sustainability of maritime logistics in the contemporary digital era.

In pursuit of harnessing the revolutionary capabilities of blockchain technology, our research endeavors to offer pioneering perspectives on its adoption. We aim to counteract resistance to change and redefine the technological course of the maritime shipping industry. While our focus remains on TIMAD, it’s important to note that the proof of concept (POC) could be adaptable to incorporate any other community system (CS). This initiative has also been an integral part of our implementation roadmap, as it aligns with the objectives of our project.

Our ultimate goal is to progress toward the production phase. This aspect will be elaborated upon in the forthcoming chapters, where we will detail its contextual development and provide in-depth insights.

We harness blockchain’s decentralized architecture to augment traceability, integrity and collaborative governance of dangerous goods, mitigating risks inherent to centralized platforms.

1.3 Problem formulation and research questions

Within the maritime shipping industry, there are both inter-firm information systems and intra-firm/inter-community communication that need to be addressed. Despite centralized architectures like PCS being efficient for inter-firm processes, they face typical issues of centralized systems. Meanwhile, the lack of integration in intra-firm or intra-community communication

reintroduces redundancy and manual processes globally.

This results in a lack of coordination among industry actors, poses security risks, increases workloads for authorities, reduces trust between parties, and reduces overall business process efficiency (Jensen et al., 2014). Furthermore, the variety of actors, relationships, regulations, and information costs contribute to barriers that impede global trade (World Economic Forum, 2016).

Blockchain systems could address these issues by enabling real-time document updates, automating manual tasks, improving accuracy, reducing costs, and increasing security through encryption and immutability. By providing a shared record, blockchain promotes trust and reduces intermediaries.

While researchers agree on blockchain's potential benefits, few can envision its future industry adoption (Rodriguez, 2016). However, a gap persists in envisioning and evaluating the likelihood of its adoption within the industry landscape. As blockchain's advantages become apparent, maritime IT providers looking to develop solutions need to understand its adoption likelihood and identify business opportunities and risks.

Three key needs emerge:

- Assessing the opportunities and potential of blockchain for the maritime sector.
- Providing a clear understanding of blockchain to avoid misconceptions hampering adoption.
- Determining the likelihood of industry blockchain adoption and overcoming deterrents.

This dissertation seeks to explore and articulate the multifaceted implications of blockchain technology in the maritime sector, specifically for IT service providers poised to pioneer these solutions.

We aimed, at first to address a broad research question: "How can blockchain technology be effectively implemented in the maritime sector?" This overarching inquiry has prompted several sub-questions that necessitate further refinement and exploration.

Initially, recognizing that we are not the first to approach this technology within the sector, we sought to learn from previous projects that ventured into these uncharted waters. Consequently, the first formulated question, which we addressed through an in-depth analysis in the beginning of Chapter Four, was:

Research Question 1 (RQ1): *What are the key challenges and factors influencing the success or failure of blockchain technology implementations in the maritime industry, as evidenced by case studies of specific projects?*

This question explores the complexities of adopting blockchain within the maritime sector, examining success factors, impediments, and the practical outcomes of notable initiatives. We delved into industry collaboration, commercial viability, data governance, privacy concerns,

1.3. Problem formulation and research questions

technical challenges, and the difficulty in standardizing blockchain procedures, offering insights into the nuanced interplay of technological innovation and sector-specific dynamics.

After a comprehensive analysis, we concluded that this question might require reformulation and a more nuanced approach to address the multifaceted nature of the topic comprehensively.

An oversight in the literature targeting this technology from a maritime perspective reoriented our research to fill the existing gap by answering the following research questions, allowing us in chapter four to continue and cover all aspects of the technology and position our work within a maritime context while considering maritime requirements:

Research Question 2 (RQ2): *"What are the **potential** use cases for blockchain technology in maritime logistics, shipping, and port management, and how can these drive innovation and improve operational efficiency?"*

Research Question 3 (RQ3): *"What **challenges**, including technological, regulatory, and adoption barriers, must be addressed to successfully implement blockchain in the maritime industry? Is it feasible and how this can be done? "*

These questions also introduced another consideration to be taken into account through our implementation:

Research Question 4 (RQ4): *"How likely is the **adoption** of blockchain technology by key stakeholders in the shipping industry, what are the primary barriers to its adoption, and how can these obstacles be effectively overcome? "*

This question aims to assess the readiness and obstacles within the industry towards integrating blockchain technology and to identify strategies for facilitating its successful adoption.

Through this comprehensive approach, we endeavour to provide a holistic understanding of blockchain technology's potential in the maritime sector, addressing the challenges, opportunities, and practical considerations for its effective implementation. Additionally, we embarked on a journey to provide potential solutions for the challenges that may present upon technological implementation in the sector so that we can be well-equipped to address them.

To elucidate the role and potential of blockchain in this domain, this study is structured around these pivotal research questions. We delve into the business opportunities and risks that blockchain technology may present to IT service providers in the shipping industry. This inquiry aims to dissect the technological prospects, challenges, and overarching impact of blockchain in advancing maritime operations. The approach adopted here is scholarly and analytical, encompassing a comprehensive review of existing literature and theoretical frameworks to understand the technology's potential, its historical and current applications in the maritime sector, and its position within the broader trajectory of technological evolution in this field.

Drawing from the results and insights the answers to these questions provided us, we proceeded to readdress the main question "How can blockchain technology be effectively implemented in the maritime sector?" and refine it, knowing now the added benefit and potential that this technology yields for this sector along with the challenges:

Research Question 5 (RQ5): *" How can blockchain technology be effectively and seamlessly*

integrated into the maritime ecosystem and its technology to ensure traceability, transparency and increase security?"

To answer this question, as presented in the second section of the manuscript, we utilised a case study methodology, this part of the research examines a specific application of blockchain technology: TIMAD for traceability of hazardous materials. Consequently, it elucidates the practicalities of blockchain integration in maritime operations.

This investigation aims to demonstrate how blockchain can integrate, align with and enhance ongoing digital transformation efforts in the sector, addressing both inter- and intra-organizational challenges while capitalizing on blockchain's inherent features of increased transparency and traceability. This aimed to bridge the gap between theoretical potential and practical application of blockchain in the shipping industry, offering a comprehensive, multi-dimensional analysis that integrates both academic rigour and practical insights.

Additionally, in a future work reflection, we anticipated future works in the direction of sharding. An enhancement that allows for our PoC to stay afloat with blockchain technological advancement. This embodies a commitment to continuous improvement, and innovation.

1.4 Research Scope

The maritime industry encompasses an extensive and diverse range of activities and stakeholders. Given this breadth, it is critical to delineate the specific focus of this investigation, which is confined to port segments. This delimitation is not merely a matter of narrowing the research scope but is pivotal in harnessing practical expertise from these segments to bridge theoretical concepts with innovative, pragmatic solutions.

This research operates within the framework of a CIFRE convention. A collaborative arrangement involving the University of Le Havre, the LITIS laboratory, and HAROPA PORT, one of the largest port complexes in Europe. This partnership is instrumental in providing the necessary insights from the industry combined with a strong foundation in academia.

The rationale for focusing on ports, their integral role in the maritime sector, and their potential to significantly contribute to the success of this research will be elaborated in Chapter 4. This chapter will include an overview of HAROPA Port, the ongoing digitalization trends in the sector, and other elements that fortify our research's relevance and applicability. Drawing on (Stopford, 2008) insights, we underscore the centrality of ports as operational hubs in the maritime industry, despite the dominant economic contribution of merchant shipping.

Furthermore, as elucidated in Chapter 2, the majority of blockchain applications developed to date are tailored for the shipping and port segments, further justifying our research focus.

Our thesis seeks to go beyond just assessing the benefits of isolated solutions. Instead, it seeks to explore how to draw from theoretical contributions and analysis and amalgam solutions yielding more significant advancements.

1.5 Thesis Structure and contributions

This dissertation is organized into four sections: An introductory section, a contribution section, a future works and discussions section and a conclusion. Each was meticulously explored to cover the many-sided aspects of our work.

The state-of-the-art section covers the state of the art on blockchain, maritime and technological advancements. It contains two chapters.

Chapter 2 presents an in-depth exploration of blockchain technology, tracing its evolution. It demystifies blockchain's key components. Through a scholarly lens, it elucidates how these elements converge to offer unique features like disintermediation, enhanced security, data immutability, and automation, thereby laying a conceptual groundwork for understanding blockchain's potential applications and transformative capacity beyond cryptocurrencies.

Chapter 3 has at its fulcrum the maritime industry. It scrutinized the integration of blockchain technology within the maritime ecosystem. We employed a triangulation methodology for a comprehensive state-of-the-art review. It synthesizes existing literature and web-based research to map out the current landscape and prospects of blockchain in maritime operations. The narrative captures the genesis, evolution, and functionalities of maritime information systems, including PCS and the International Maritime Organization's (IMO) efforts towards digitization and standardized data exchange through the Maritime Single Window (MSW) System.

This examination highlights the technological readiness and barriers to blockchain adoption. We also delineated the early adopters and the range of blockchain projects within the sector.

The second section presents the heart of our work and all our contributions ranging from theoretical and literary analyses to the application and implementation of a PoC within the maritime sector. We present our contributions and analyses that not only enrich the sector's understanding of this technology but also frame it within a practical use-case application. This approach targets a specific challenge in the maritime sector, showcasing the technology's potential implementation, which, while originating from this use-case, is not limited to it.

Our work in the fourth chapter focuses on the transformative potential of blockchain technology in the maritime industry. We did a comprehensive survey highlighting how blockchain can revolutionize maritime operations by enhancing transparency, efficiency, and security across various segments. We propose a systematic exploration of blockchain's applications, benefits, and challenges within the maritime sector. Contributions include identifying viable use cases, such as improving supply chain visibility, securing transactions, and facilitating regulatory compliance. We also address significant hurdles such as technical limitations, regulatory uncertainties, and the need for industry-wide standardization and collaboration. The importance of our work lies in its holistic approach, combining a theoretical foundation with practical insights to advocate for blockchain's adoption as a tool for innovation and improvement in maritime logistics and beyond covering existing literacy lacuna.

Chapters 5,6,7 and 8 of this section illustrate a holistic journey, our work and contribu-

Chapter 1. General Introduction

tions, from the theoretical exploration of blockchain technology to its practical application and evaluation in the maritime logistics sector.

Chapter 5 presents results derived from conducted analyses. We identify our wanted PoC specifications. Then we proceed to target achievability. This chapter established a strong foundation for the subsequent technical implementation, emphasizing the need for a robust and adaptable solution to the unique dynamics and requirements of maritime logistics. Consequently, we identify and justify our selection of Hyperledger Fabric (HF) as the backbone of our blockchain infrastructure for the PoC. Additionally, we implement a strategy to identify a relevant notarization use case and pertinent data, showcasing the strength of our implementation before exploring the technical aspects.

Chapter 6 outlines the technical implementation of the blockchain infrastructure, starting with an overview of the current status quo and advancing towards integration with existing systems. We highlight the smooth integration with existing PCS such as TIMAD. By adopting a phased and strategic approach, we developed a blockchain layer that improves data notarization and security, while ensuring it seamlessly fits into the existing maritime logistics workflow. Based on the specifications outlined in the previous chapter, we designed and implemented a blockchain network architecture. This architecture includes all the necessary elements that take advantage of both existing systems and blockchain capabilities to achieve desired outcomes and comply with industry standards.

Once the infrastructure is defined, implemented, and operable, Chapter 7 covers the connection between the infrastructure and its functionality. The focus shifts to the development and deployment of smart contracts specifically designed for maritime logistics operations managed by PCS. These smart contracts act as the operational bridge, enabling secure and immutable record-keeping of essential logistics information. Furthermore, the chapter details the creation of a seamless, user-centric ledger interaction, governed and implemented within TIMAD. This ensures that stakeholders can smoothly interact with data secured by blockchain, thereby enhancing the existing maritime logistics infrastructure with the critical features of blockchain technology.

Chapter 8 offers a detailed evaluation of the proposed PoC, focusing on its performance and viability within the maritime logistics sector. It highlights the systematic testing conducted to validate the architecture's viability and capacity to handle production scenarios. Additionally, the chapter introduces initiatives currently in progress and plans for future development. Our objective is to extend the blockchain network's application across the maritime industry, aiming to create a more integrated and technologically advanced maritime landscape. The chapter includes a comprehensive description of our immediate implementation of the PoC within the sector, a project that outlines concrete steps for future enhancements.

The final chapter concludes the discussion and, towards its end, presents another future prospect that ensures our project stays aligned with ongoing trends in blockchain evolution and performance enhancement. This direction is informed by the analysis conducted in Chapter

4, which identifies specific limitations of blockchain technology. It demonstrates that these limitations, along with the developments outlined in Chapter 4, can be specifically addressed and mitigated. This prospect underlines our commitment to continuously refine and adapt our project to meet emerging challenges and leverage new opportunities within the blockchain domain.

The thesis presents a compelling case for the transformative potential of blockchain technology, offering insights into its implementation strategy, the challenges encountered, and the prospects for its adoption in enhancing the operational integrity and efficiency of maritime logistics systems.

Part I

State of the art

This comprehensive introduction and detailed outline set the context for the transformative potential of blockchain in maritime logistics, tracing the sector's evolution from ancient trade routes to modern digital revolutions, and setting the stage for exploring blockchain's integration challenges and opportunities for innovation in global shipping networks.

In this section, we provide a comprehensive and detailed exploration of blockchain technology's transformative impact on various sectors, with a particular focus on the maritime industry.

This section is divided into two chapters, in addition to the general introduction.

The first chapter serves as a solid foundation for understanding blockchain's fundamental principles, applications, and features. The second one lays a scholarly foundation for comprehending the essential principles, diverse applications, and the progressive role of blockchain technology in bolstering efficiency, security, and transparency within maritime operations. Through a thorough scholarly examination of blockchain initiatives in the maritime sector, this state-of-the-art situates the technology's vast potential alongside the challenges encountered. It paves the way for a nuanced analysis aimed at optimizing blockchain technology for pragmatic applications in the industry, thereby contributing significantly to academic discourse and practical advancements.

BLOCKCHAIN TECHNOLOGY OVERVIEW

Contents

2.1	Introduction to blockchain	22
2.2	Conceptual Understanding	25
2.2.1	The evolution and distinctiveness of distributed ledgers	25
2.2.2	Key Concepts and Properties of Blockchain	26
2.2.3	Decentralization and Distribution	29
2.2.4	Consensus Mechanisms	29
2.2.5	Traceability and immutability amongst other characteristics	30
2.2.6	Smart Contracts: An evolution	31
2.2.7	Digital Wallets: The Gateway to Blockchain Interactions	33
2.2.8	Oracles	34
2.3	Blockchain topology	36
2.3.1	Centralized Architectures: A State-of-the-Art-Overview	36
2.3.2	Between distributed and decentralised	36
2.3.3	Public, permissioned and private blockchains	37

In the vanguard of technological advancements, blockchain has emerged as a paradigm-shifting innovation, garnering acclaim for its transformative potential in various sectors. Initially devised as the foundational framework for Bitcoin, blockchain technology heralds a new era of decentralized information exchange and transaction processing. Its architecture, based on distributed ledgers, leverages cryptographic validation and consensus mechanisms to foster trust in a decentralized context. This chapter delves into the quintessential elements of blockchain technology – distributed ledgers, cryptographic hash linking, the concept of shared states of truth, smart contracts, and consensus protocols. These elements collectively facilitate the technology’s unique features: disintermediation, transparency, automation, enhanced security, and data immutability.

This chapter aims to provide a high-level technical overview, demystifying the key properties and technical workings of blockchain technology. It seeks to present core concepts such as distributed consensus, the immutable nature of blockchain records, the functionality and application of smart contracts, and the various typologies of blockchain networks. The intention is

to lay a comprehensive foundation for the technology, enabling readers to grasp its intricacies within today's digitally-driven world. By exploring these fundamental aspects, the chapter sets the stage for a deeper understanding of blockchain's role and impact across diverse industry landscapes.

2.1 Introduction to blockchain

Blockchain technology, a revolutionary stride in digital innovation, emerged as a transformative solution in the realm of data management and security. Its conceptualization is primarily attributed to the 2008 whitepaper by an enigmatic figure (or group) known as Satoshi Nakamoto (Nakamoto, 2008b). This groundbreaking paper proposed a decentralized digital currency, currently known as "Bitcoin", as an alternative to traditional, centralized financial systems, highlighting a growing need for a more transparent and autonomous financial infrastructure.

The genesis of blockchain was fueled by the necessity to address a critical issue in digital transactions: the double-spending problem. In essence, this problem pertained to the potential of digital assets being duplicated and spent multiple times, undermining the trust and integrity of digital transactions. Before blockchain, centralized authorities such as banks were the primary solution to monitor and validate transactions, introducing potential risks and inefficiencies associated with centralization.

Satoshi Nakamoto combined existing technological innovations such as cryptographic time-stamping and Merkle trees to create what is now known as the "blockchain."

What is a blockchain Blockchain is a digital register. In this register we record transactions. In Nakamoto's genesis application of this technology, the transaction consisted of the digital currency amount, the digital signature of the receiving and sending address on the network and a timestamp. Each set of transactions is grouped to form a block illustrated in Figure 4.

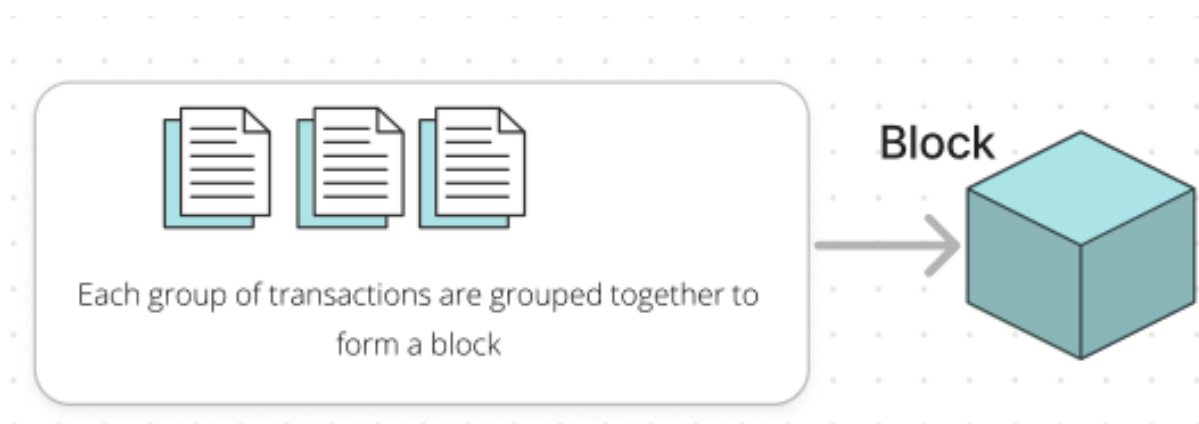


Figure 4: A block is a group of transactions : An illustration by the author

Blocks are chained together using cryptography to make a hard-to-alter information registry.

2.1. Introduction to blockchain

The first block is called the genesis block. Each block consists of a block header and a block body. It contains, in addition to its transactions, a cryptographic hash of the previous block and a block timestamp, forming a chain that is both immutable and transparent (cf. Figure 5).

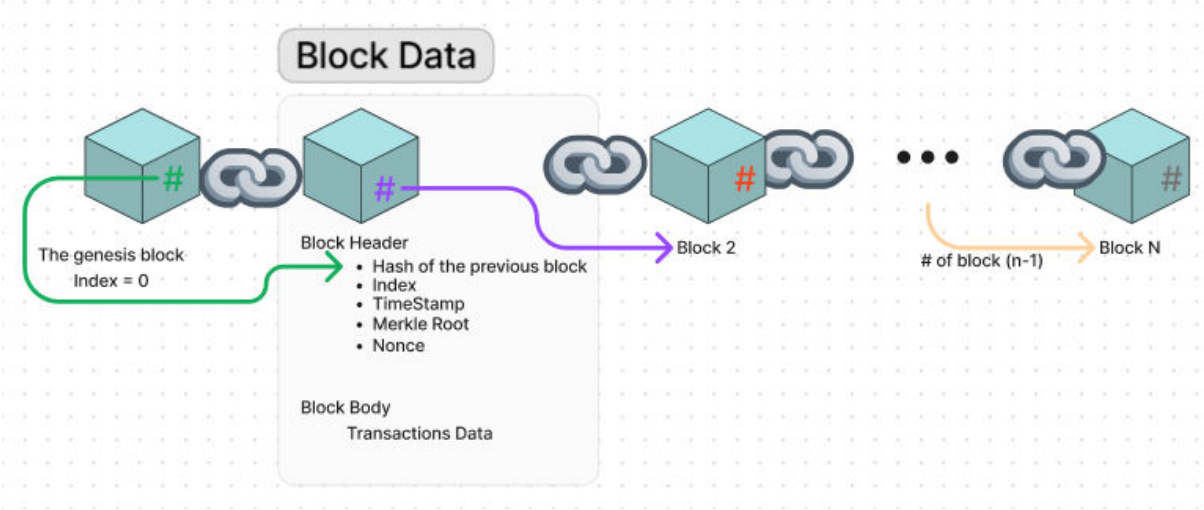


Figure 5: A chain of blocks illustrated by the author

The alteration of any data within a block requires altering the entire chain of data in a ledger. The ledger is replicated across a distributed network of machines (cf. Figure 6). Machines are called network nodes.

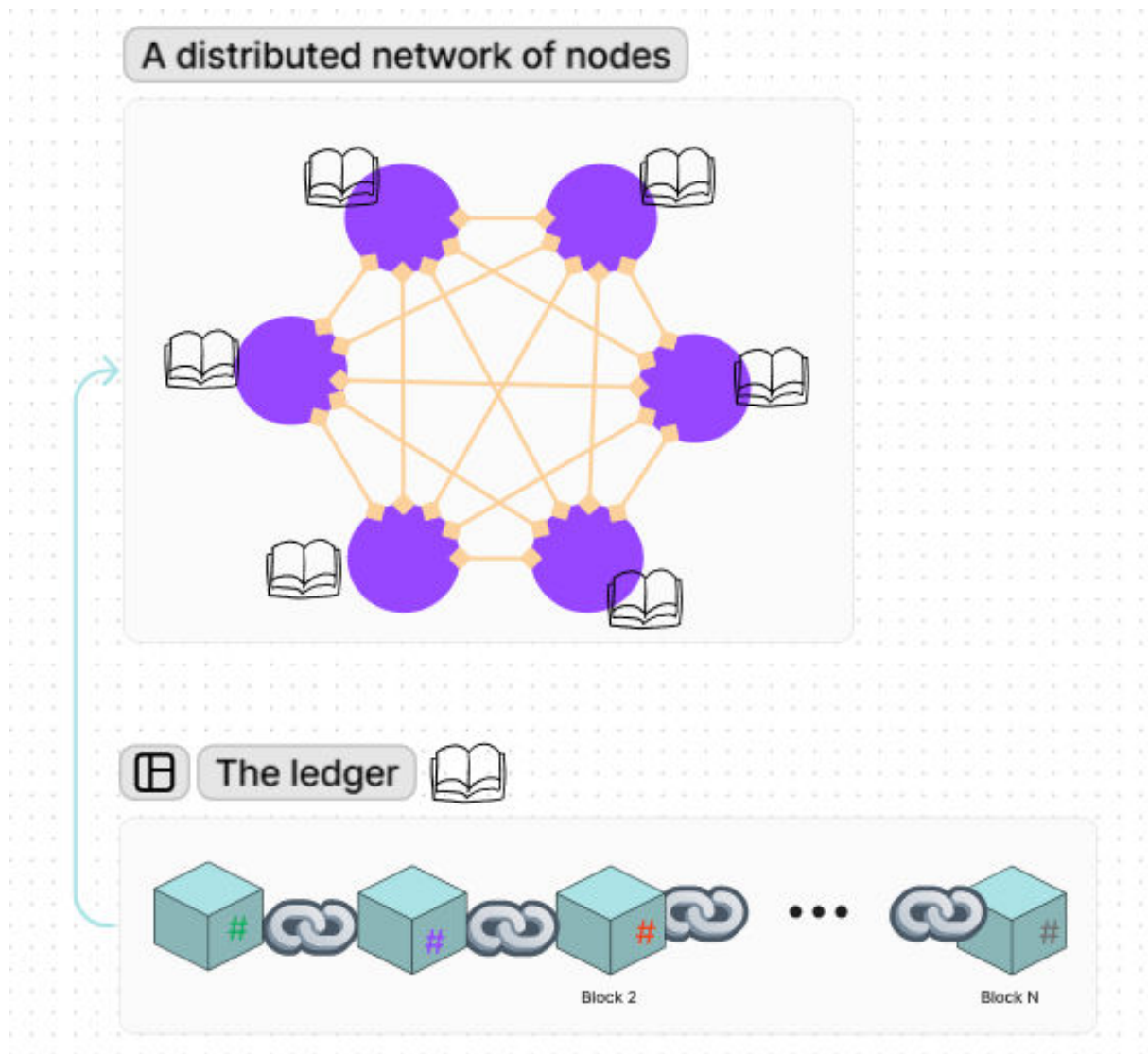


Figure 6: A network of nodes illustrated by the author

The tamper-proof nature of blockchains comes from cryptography. Altering data in a block would require first recalculating the hashes of all following blocks making it computationally hard to do. Then, the attacker would have to replicate the change amongst all or the majority of network nodes. The decentralized network ensures that any attempt to introduce a modified block would be rejected by honest nodes.

This safeguards the ledger from unauthorized modifications and ensures the chronological integrity of transactions.

Nakamoto's integration of these technologies marked a pivotal moment in digital history, extending far beyond the domain of cryptocurrencies. It paved the way for a multitude of applications across various sectors, signifying a shift towards decentralized, transparent, and secure systems for recording and managing digital interactions and transactions.

2.2 Conceptual Understanding

2.2.1 The evolution and distinctiveness of distributed ledgers

The journey of distributed ledger technology (DLT) is a fascinating saga of innovation, intertwining advances in cryptography, peer-to-peer networks, and consensus algorithms to forge a path distinctly its own in the digital world.

Tracing its embryonic stages falls back to the cryptographic pioneering of the late 1980s and 1990s. It was the conceptualization of peer-to-peer networks that added a pivotal layer, enabling decentralized information sharing without a central authority.

- In 1989, Lamport delineated a seminal method for synchronizing modifications within peer-to-peer networks (Lamport and Lynch, 1989). Tailored towards distributed computing systems its foundational principles were instrumental in facilitating consensus across distributed systems.
- In 1991, Stuart Haber and W. Scott Stornetta introduced the conceptualization of a cryptographically secure ledger (Haber and Stornetta, 1991). Their framework facilitated the verification of the origin and authenticity of digital documents independently of central authorities. It employed a pseudo-random generator seeded with the hash of the cryptographically signed document. It laid the groundwork for secure timestamping and later advancements in blockchain technology that fully embraced distributed signing
- Building upon their groundbreaking work in 1991, Haber and Stornetta continued to advance the field of cryptographically secured ledgers. Drawing inspiration from Ralph Merkle's seminal 1987 paper (Merkle, 1987), they expanded upon their initial concepts by incorporating the Merkle tree data structure. This adaptation, detailed in their subsequent publication (Bayer et al., 1993), was aimed at enhancing the efficiency of their ledger system.
- In 1997, Adam Back introduced Hashcash (Back, 1997), an early distributed ledger system devised to mitigate email spam and denial-of-service attacks. Utilizing a proof-of-work mechanism, enabled decentralized networks to collaboratively timestamp and validate transactions. While limited in scope, Hashcash was vital in demonstrating the potential of decentralized ledger management without central control, laying the groundwork for future advancements in distributed ledger technologies.

This work laid the groundwork for future advancements. Although not directly intended for blockchain, as it did not exist at the time, the principles and technologies developed played a crucial role in enabling the later emergence and growth of decentralized systems and blockchain technology.

It constituted merely the preliminary phase in the evolution of Distributed Ledger Technology (DLT). The watershed moment in this progression was heralded by the introduction of Bitcoin in 2008 (Nakamoto, 2008b). Bitcoin epitomized the core principles of DLT by integrating the secure, chain-linked frameworks proposed by Haber and Stornetta with a decentralized consensus algorithm, an approach indirectly influenced by Lamport's earlier findings. This innovative synthesis gave rise to a self-verifying ecosystem for digital transactions, characterized by its immutability, transparency, and decentralization, thereby effectuating a significant paradigm shift in the realm of digital trust (Nakamoto, 2008b).

Following this groundbreaking publication, an open-source program for implementing the Bitcoin system was released, leading to the establishment of the first Bitcoin network in early 2009. This marked the creation of the first bitcoins by Nakamoto. Despite the anonymity of Bitcoin's creator, a robust community quickly formed to support, market, and continually improve the system, addressing various issues within the code.

Bitcoin, introduced by Satoshi Nakamoto, exemplified the first successful application of blockchain, heralding a new era in decentralized and secure digital transactions.

The uniqueness of DLT is encapsulated in its capacity to generate a verifiable and immutable record of transactions. It obviates the need for centralized oversight inherently addressing many of the limitations in traditional ledgers. This attribute of DLT transcends mere technological innovation, venturing into the ideological sphere by challenging established power dynamics in finance and related domains. It represents a confluence of technological ingenuity and philosophical principles, bolstered by a community-driven ethos that prioritizes transparency, security, and the democratization of access. Blockchain, a subset of DLT, exemplifies these traits through its public ledger system, which permits unencumbered verification of transactions, thus instilling a renewed level of trust in digital interactions.

2.2.2 Key Concepts and Properties of Blockchain

Blockchain is the complex fusion of various key concepts and properties, each integral to its unique capabilities and applications. This section explores these essential elements, including timestamping, cryptography, decentralization, consensus mechanisms, traceability, immutability, and Merkle tree security features, which collectively make blockchain and adhere to its features.

Timestamping and Cryptography Each block within a blockchain is stamped with a timestamp, thereby ensuring a consistent and verifiable sequence of events, as elucidated in Bayer et al.'s exploration of blockchain's temporal aspects (Bayer et al., 1993).

Cryptography is another pillar of blockchain, providing security and privacy. Blockchain employs cryptographic hash functions to ensure data integrity.

A cryptographic hash function (cf. Figure 7) is a sophisticated mathematical algorithm that

2.2. Conceptual Understanding

maps data of arbitrary size to a fixed-size alphanumeric string, referred to as a hash value or digest. Notably, this function is unidirectional, rendering it computationally infeasible to reverse-engineer the original input from its hash output. Additionally, these hash functions are designed to be second preimage and collision-resistant, meaning it is practically impossible to find two distinct inputs that produce an identical hash output. Such attributes ensure that each hash value is a unique representation of the original data, making even minor alterations to the data readily detectable.

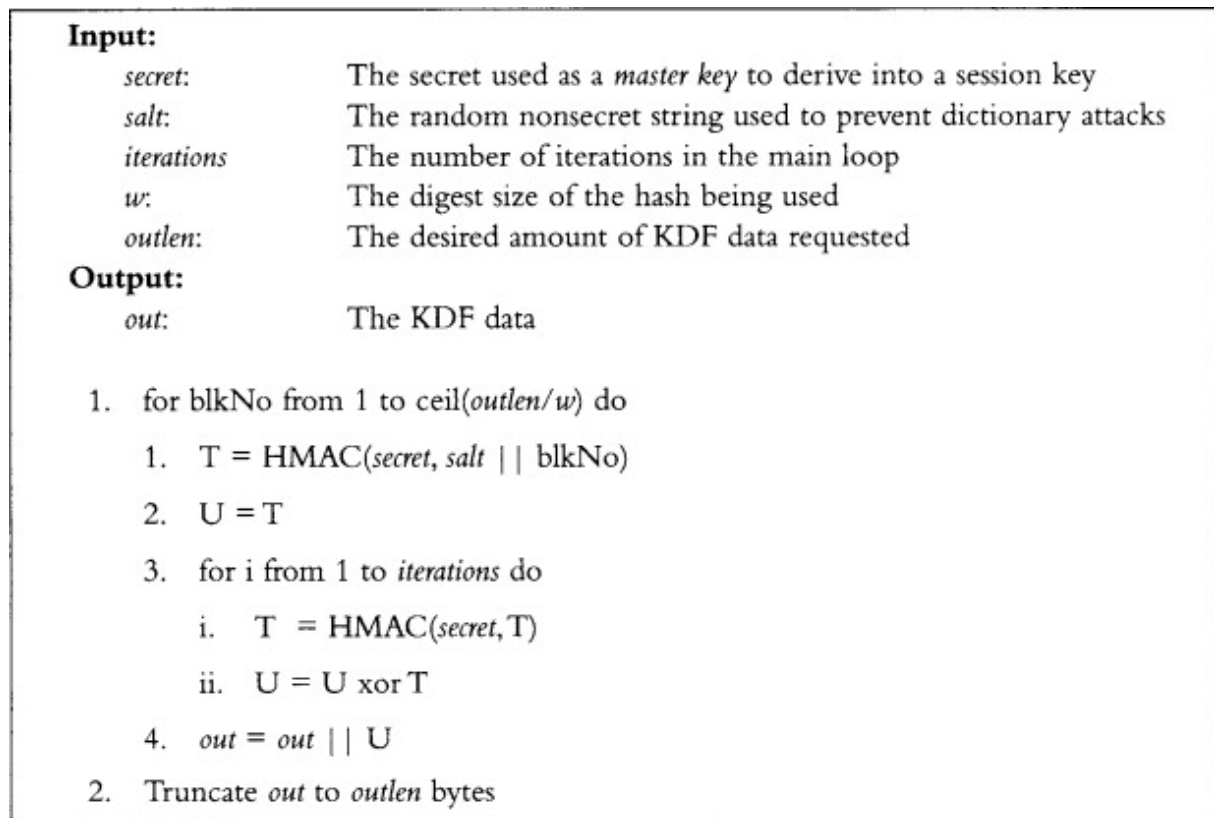


Figure 7: Hash function algorithm (St Denis and Johnson, 2007)

In blockchain technology, cryptographic hashes like SHA-256 are used extensively to generate fixed-length digests aka hashes of transactions, blocks, and other dynamic data structures. This allows efficient data integrity verification and tamper detection in an immutable ledger. Hashes act like digital fingerprints providing a compact data representation while retaining a level of unique traceability back to the source input. Each block within the ledger contains a hash of its previous.

This arrangement creates a chain of blocks, each linked cryptographically to its predecessor, thereby forming a chain that becomes increasingly resistant to alteration as it lengthens.

Merkle tree Each transaction (TX) in a block is hashed. This function generates a unique fingerprint (hash) for each transaction, like a digital summary. Transactions are then grouped in pairs. The hashes of each pair are then hashed again to create a new hash. This process continues

until there's only one hash remaining at the top, called the Merkle root (cf. Figure8).

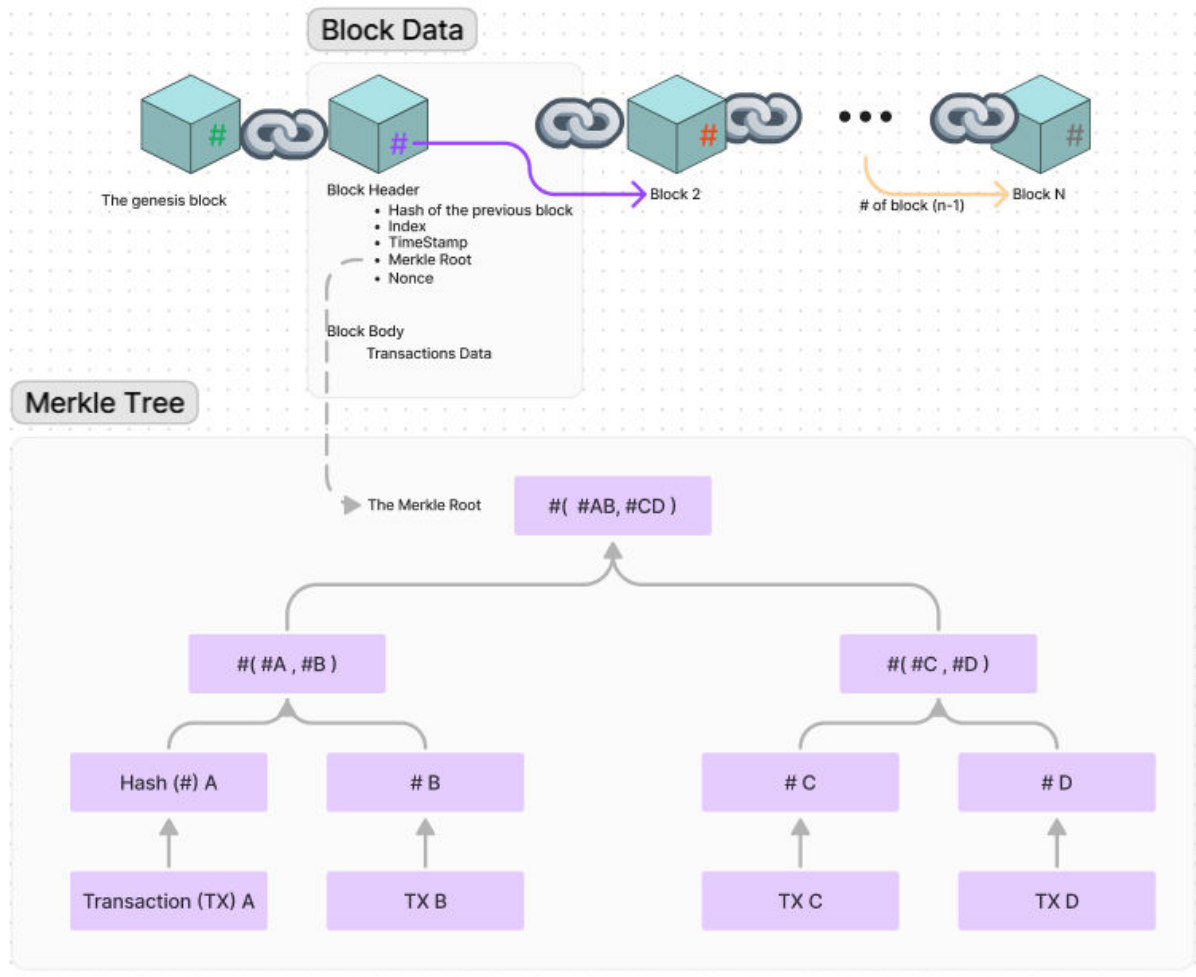


Figure 8: Merkle tree illustration by the author

Instead of verifying every transaction in a block, we can verify the integrity of the entire block by simply checking its Merkle root. This is because any change to a transaction would alter its hash, and all the subsequent hashes up the tree would be different as well. Additionally, the root acts as a compact proof of the state of the block. It allows anyone to verify that a particular transaction is indeed part of the block without downloading the entire block data (Sharad Mangrulkar and Vijay Chavan, 2024).

The robustness of Bitcoin's blockchain, especially in terms of its immutability, becomes evident when considering the computational power required to alter its ledger.

Estimating the computational power necessary to compromise Bitcoin's blockchain involves understanding its network hash rate. Throughout the year, the hash rate has shown variations. On November 19, 2023, the hash rate was recorded at about 662.42 EH/s (CoinWarz, 2023). Furthermore, as of the latest available data in December 2023, the global hash rate of Bitcoin stood at around 475.38 EH/s (CoinWarz, 2023). These figures indicate a fluctuating but generally upward-staggering level of computational effort. This means that to alter even a single block, an

adversary would need to commandeer a significant portion of this hash rate to outpace the rest of the network. This discussion segues into the next salient feature of blockchain technology: its inherent distribution.

2.2.3 Decentralization and Distribution

The term 'distribution' in blockchain refers to the decentralized structure of the network, where the ledger is not stored in a single location or controlled by a single entity. Instead, it is replicated across a wide network of nodes, each holding a copy of the ledger. This decentralization is a cornerstone of blockchain's design, contributing to its resilience and security.

The ledger is distributed across multiple nodes. Any attempt to alter the blockchain would require simultaneous modifications across a majority of these nodes. That is rendered virtually impossible by the sheer size and spread of the network. The implications of this distribution are profound. Not only does it bolster the security of the blockchain against potential attacks, but it also democratizes the control of data. As each node in the network participates in the validation process, blockchain technology embodies a shift from centralized to distributed digital trust systems.

2.2.4 Consensus Mechanisms

Building on the concept of distribution within blockchain technology, the next critical component of its architecture is the consensus algorithm. The decentralized nature of the blockchain network necessitates a robust mechanism to achieve agreement among the disparate nodes regarding the state of the ledger. This consensus algorithm is pivotal for maintaining the ledger's integrity and establishing trust within the network. Consensus mechanisms in blockchain serve as the method through which the various nodes in the network reach a common agreement on the validity of transactions and append new blocks to the ledger. In the next paragraph, we explain the intricacies of these consensus algorithms, examining how they function as the linchpin of cooperative decision-making in decentralized systems and exploring their role in upholding the principles of transparency, security, and democratic data management inherent in blockchain technology.

PoW In Proof of Work (PoW) systems like Bitcoin's (Nakamoto, 2008b), miners use powerful computers to solve complex puzzles and add new transaction blocks to the blockchain. The first miner to solve the puzzle earns a reward, an honesty incentive. To manage block creation speed and enhance security, puzzle difficulty adjusts based on the network's total computing power, making mining resource-intensive. Miners build blocks by including verified transactions broadcasted on the network, adhering to a predefined size limit. A random number (nonce) is added to the block header before hashing. This hash must meet a set network difficulty, further slowing down block creation. This design makes altering the blockchain practically impossible

due to the vast network of miners. Criticisms of PoW include its high energy use and the risk of centralization from large mining groups (Vranken, 2017).

POS Ethereum, a prominent blockchain known for introducing smart contracts and token creation capabilities (Buterin et al., 2013), transitioned from a Proof-of-Work (PoW) to a Proof-of-Stake (PoS) consensus mechanism in September 2022. This change was driven by two key factors: sustainability and scalability. PoW relies on extensive computing power, leading to high energy consumption. Instead of miners PoS relies on validators that stake tokens. The more coins (or stake) a user holds, the higher the chance of being chosen as a validator. Validators take turns proposing and validating new blocks of transactions on the blockchain. If a validator tries to tamper with the blockchain, they risk losing their stake in the cryptocurrency. This discourages malicious activity.

Raft One algorithm of particular interest is the Raft Protocol (Howard et al., 2015) that we employed in our application to be unravelled starting Chapter 5. Raft operates through leader election: servers vote amongst themselves, with the majority winner becoming the leader responsible for proposing new transactions (log entries) to others. Followers replicate these entries in their local logs. Once a majority of servers acknowledge receipt, the entry is "committed" and becomes part of the permanent record. This approach guarantees consistency across the system, even if individual servers experience failures. Raft utilizes heartbeats from the leader to maintain communication and detect failures, along with techniques to prevent conflicting leaders and ensure smooth transitions during elections. This combination offers an efficient and reliable method for achieving consensus in distributed applications, particularly in permissioned blockchains where nodes are identified and known to each other. Unlike some methods that require solving complex puzzles with massive computing power (e.g., Proof-of-Work in Bitcoin), Raft operates efficiently. It minimizes energy consumption by requiring less complex calculations on participating devices and potentially using more scalable network due to its ability to handle transactions efficiently. Additionally, Raft utilizes a designated leader to streamline communication and avoid redundant computations across the network, further reducing energy expenditure. It stands out as a more environmentally friendly alternative within the world of blockchain consensus mechanisms.

2.2.5 Traceability and immutability amongst other characteristics

Blockchain technology, characterized by its innovative approach to data management and security, encapsulates a suite of features. It differentiates it from traditional digital systems. Central to these characteristics are traceability and immutability, alongside decentralization, consensus mechanisms, all of which collectively define the essence of blockchain technology.

Traceability in blockchain is achieved through its inherent ledger system, where every transaction is recorded in a chronological chain of blocks. This allows for the transparent tracking

of any asset or data point through the blockchain. This feature renders the technology particularly advantageous where the provenance of data needs to be reliably tracked (Tian, 2016). The immutable nature of blockchain further enhances this traceability. Once data is recorded on the blockchain, it cannot be altered or deleted, which is critical for ensuring the integrity of the historical record (Crosby et al., 2016).

The decentralization of blockchain is another defining feature. Unlike centralized systems, where data is stored in a single location, blockchain distributes its ledger across multiple nodes. This fortifies it against centralized architecture limitations and provides a more democratic data management system (Swan, 2015). This distribution is maintained through consensus mechanisms that preserve the network's integrity (Nakamoto, 2008b; King and Nadal, 2012).

The principle of immutability in blockchain technology is pivotal, marking it as a fundamentally transformative tool in various sectors. Once data is added to a blockchain, altering or erasing it is extremely challenging, if not impossible. This feature assures data integrity and longevity, a cornerstone for applications where data security is critical. As noted by (Antonopoulos and Wood, 2018) in 'Mastering Ethereum', the immutability characteristic of blockchain provides an enduring and tamper-evident record, instilling a high level of trust and reliability in the data.

The relevance of immutability in blockchain has been extensively discussed in academic circles. For instance, (Tapscott and Tapscott, 2016), delves into how blockchain's unchangeable nature can drastically enhance transparency and accountability in digital transactions. They argue that this feature is precious in environments prone to fraud or where reliable record-keeping is essential.

Furthermore, (Crosby et al., 2016) emphasizes how blockchain's immutable ledger can significantly improve the efficiency and security of many systems, ranging from financial services to supply chain management. The inability to alter records without detection makes blockchain an ideal platform for secure and transparent record-keeping in various industries.

2.2.6 Smart Contracts: An evolution

Following the exploration of the fundamental characteristics of blockchain, it is crucial to address the evolution of this DLT through the advent of smart contracts. As it extended its utility beyond simple transactional records. Smart contracts are self-executing contracts with the terms of the agreement directly written into code. They are stored on the blockchain and automatically enforce and execute the terms of a contract when predetermined conditions are met. This concept, first proposed by Nick Szabo, has been revolutionary in automating contract execution and reducing the need for intermediaries (Szabo, 1996).

The emergence of smart contracts has notably expanded the scope of Distributed Ledger Technology (DLT), especially with their implementation in Ethereum, a platform developed by Vitalik Buterin (Buterin et al., 2014). Smart contracts are programmable scripts stored on the blockchain, automatically executed when predefined criteria are met. This innovative feature

guarantees that the outcomes, once the stipulated conditions are fulfilled, are executed flawlessly, without susceptibility to external interference, fraud, or errors, thus enhancing the blockchain's reliability and versatility.

Ethereum's integration of a Turing-complete programming language has been instrumental in the advancement of blockchain technology.

This development has enabled the creation of complex and varied decentralized applications (dApps) and intricate digital contracts. Through this, Ethereum has evolved blockchain from a mere transaction ledger into a platform capable of autonomously executing a diverse array of digital contracts and applications.

A smart contract is a code stored on the blockchain that users can use by sending transactions to its specific address. Smart contracts automate the execution of agreements in a decentralized manner, negating the need for intermediaries. The embedded code dictates the contract's terms, with the blockchain enforcing these terms autonomously when predefined conditions are satisfied. This ensures more efficient operations in terms of speed, costs, and transparency. The most known blockchain for its smart contract feature is the Ethereum blockchain. The Ethereum virtually distributed state machine (EVM), spread across nodes, is responsible for running the contract code. The contract code is written in a programming language such as Solidity and compiled into bytecodes to be distributed on the EVM. When someone calls the smart contract, the EVM machines run the bytecode, calculate the result, and update the blockchain's state if needed.

The automation and programmability offered by smart contracts have far-reaching implications. In finance, the genesis sector for blockchain applications, the technology enables complex operations such as decentralized exchanges, automated loans, and interest payments, all without the need for traditional financial intermediaries.

Furthermore, smart contracts facilitate the creation of entirely new types of digital assets and services. For example, non-fungible tokens (NFTs) are largely made possible through smart contracts. Similarly, decentralized autonomous organizations (DAOs) leverage smart contracts for collective decision-making and resource management without centralized control.

Non-Fungible Tokens (NFTs) Non-fungible tokens, or NFTs, are a unique type of digital asset built on blockchain technology. Unlike traditional digital assets like cryptocurrency, which are fungible (meaning one unit is interchangeable with another), NFTs are one-of-a-kind and cannot be replicated. This allows them to represent ownership of digital items like artwork, collectibles, or even virtual land within online games. Smart contracts play a crucial role in NFTs by securely recording ownership information on the blockchain and facilitating the transfer of ownership between parties.

Decentralized Autonomous Organizations (DAOs) Decentralized autonomous organizations (DAOs) are a novel form of internet-native organization that leverage smart contracts to

operate without centralized control. DAOs function through a set of pre-defined rules encoded within a smart contract, allowing members to collectively make decisions, manage resources, and achieve shared goals. Membership and voting rights within a DAO are often tied to ownership of a specific token issued by the organization itself. Smart contracts automate the execution of these decisions and ensure transparent and secure governance within the DAO.

2.2.7 Digital Wallets: The Gateway to Blockchain Interactions

Digital wallets, also known as e-wallets or cryptocurrency wallets, are software-based systems that store users' public and private keys while interfacing with various blockchains to enable users to send and receive digital currencies and monitor their balance. Unlike traditional wallets, digital wallets do not store currency in the conventional sense; rather, they provide the tools necessary to interact with the blockchain, facilitating transactions and access to digital assets.

Types and Functionalities Digital wallets can be classified into several types based on their platform and functionality: desktop wallets, mobile wallets, web wallets, hardware wallets, and paper wallets. Desktop and mobile wallets are software applications downloaded on specific devices, offering convenience and ease of use but varying in security level depending on the device's security. Web wallets operate on internet browsers, allowing users to access their funds from any device. However, they require trust in the wallet provider to manage and protect the user's private keys. Hardware wallets are physical devices that store the user's private keys offline, providing enhanced security by minimizing exposure to online vulnerabilities. Paper wallets are physical documents that contain a user's public and private keys, considered one of the most secure methods of storing keys, provided they are kept safe and free from physical damage.

Security Aspects The security of a digital wallet is paramount, given its role in managing access to digital assets. Wallets protect the private keys that authorize transactions and must safeguard against unauthorized access, cyber-attacks, and other vulnerabilities. Advanced cryptographic techniques ensure that the user's keys remain secure, yet accessible to the user. Multi-signature wallets require more than one key to authorize a transaction, adding an additional layer of security.

Interactions with Smart Contracts and dApps Digital wallets are not limited to transactions but also serve as a bridge to interact with smart contracts and decentralized applications (dApps) on blockchain networks. This interaction is fundamental to engaging with the burgeoning ecosystem of blockchain-based applications, from financial services and gaming to decentralized finance (DeFi) platforms. Wallets such as MetaMask, for instance, allow users to interact directly with Ethereum-based dApps, executing smart contracts, and managing digital identities and assets seamlessly within a single interface.

Digital wallets also play a crucial role in facilitating the economic interactions necessary for the proper functioning of the blockchain. Public blockchains rely on the activities of miners and validators, who use costly computing resources to validate transactions and secure the network. For the blockchain to remain secure and operational, it is imperative that these efforts are compensated. The remuneration of miners and validators is mainly through cryptocurrency rewards and transaction fees. Each transaction on the blockchain can incur fees, paid by the users, which are then redistributed to miners or validators. These fees are managed through digital wallets, which allow users to submit, receive, and store cryptocurrencies. Thus, wallets are indispensable not only for the daily management of digital assets but also for the overall economic functioning of blockchains. They ensure that miners and validators are properly incentivized and compensated for maintaining a secure and efficient network.

2.2.8 Oracles

The rise of smart contracts on blockchains like Ethereum introduced a fascinating challenge: how do these self-executing programs access real-world information?.

Integrating real-world data into blockchains presents several challenges. Firstly, the decentralized and secure nature of blockchains prioritizes immutability and consensus. Real-world data, on the other hand, is often dynamic and unpredictable. Introducing such data directly into the blockchain could potentially disrupt consensus mechanisms and compromise the integrity of the system.

Secondly, the deterministic nature of blockchains poses another challenge. Smart contract execution relies on a predictable outcome based on pre-defined conditions and historical data. Real-world data, by its very nature, can be unpredictable, introducing an element of uncertainty that could potentially lead to unintended consequences within smart contract execution.

Oracles bridge the gap between the isolated world of blockchains and the dynamic realm of real-world data. They act as trusted intermediaries, retrieving and delivering reliable data from external sources to smart contracts. Oracles can source data from various sources, including APIs, sensors, and IoT devices (as seen in Figure 9). This retrieved data can then be used by smart contracts to trigger pre-defined actions based on specific conditions.

Oracles are not a singular entity but rather a broader concept. Any data source capable of feeding real-world information into the blockchain can be considered an oracle. It's important to note that oracles themselves do not store data on the blockchain. Their primary function is to collect and deliver data upon request from a smart contract.

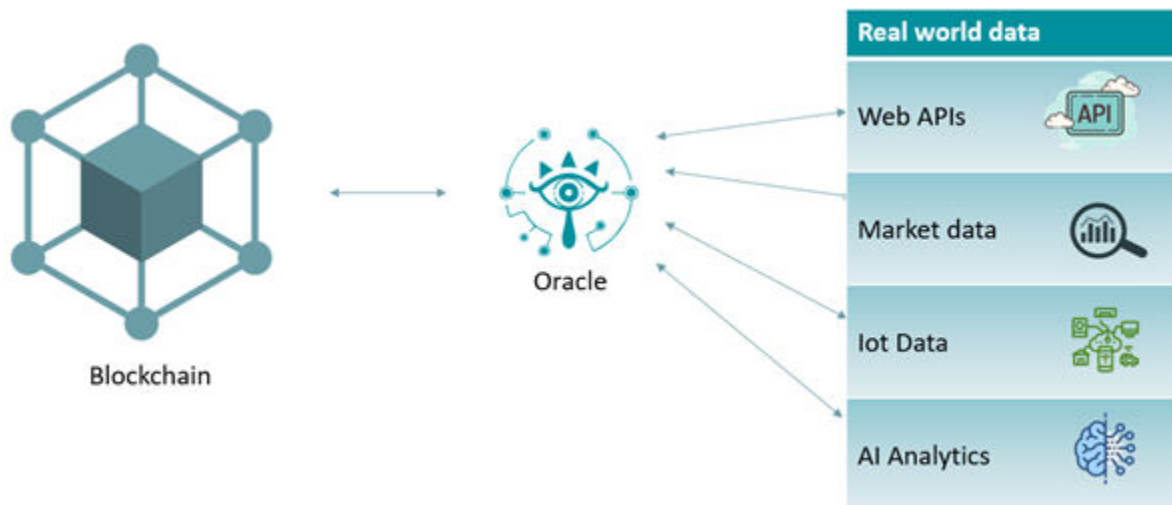


Figure 9: Oracle role representation in a blockchain environment elaborated by the author.

Oracles can be software devices, hardware devices, humans with specialized knowledge, or computational devices. Software oracles can access online information from any source of data. Hardware oracles are usually devices that have access to real-world data, such as barcode scanners, IoT or RFID devices, or sensors. Human oracles are skilled and trusted entities who can search for the needed information and authenticate it such as crypto experts or governments. All the previously mentioned oracles have a request-response role. Oracles can also use their computational power to limit on-chain gas usage. They can perform beneficial off-chain calculations. Furthermore, oracles have a two-way communication channel with blockchains. They can provide information for smart contracts but can also provide information to the outside world from a smart contract. In all of the previous data patterns, the blockchain queries the oracle for information to be provided back. There are also additional design pattern oracles such as publish–subscribe and immediate read. A publish–subscribe pattern is useful for changing data. Upon change, the oracle can broadcast the information so the provided information can always be updated with changes happening in the real world. Another type of pattern is the immediate read, where oracles store the needed information so it can be provided immediately upon request without having to query an outer source (Park et al., 2020),(Benicche, 2020).

While oracles play a critical role in enabling real-world applications for smart contracts, their integration introduces new security considerations. The reliability and trustworthiness of the oracle become paramount, as a compromised oracle could potentially feed manipulated data to the smart contract, leading to unintended consequences. Therefore, robust mechanisms for oracle selection and data validation are crucial to ensure the overall security and integrity of the system.

2.3 Blockchain topology

The topology of a blockchain network refers to its architectural structure and how nodes are interconnected. In its conceptual framework, Blockchain technology marks a distinct departure from the traditional centralized systems. This paradigm shift is crucial to understanding the evolution and topology of blockchain networks.

2.3.1 Centralized Architectures: A State-of-the-Art-Overview

Centralized architectures have dominated information systems for their efficiency in data processing and coordination. However, concerns regarding single points of failure, scalability limitations, and lack of transparency have spurred interest in decentralized alternatives.

2.3.1.1 Strengths of Centralization

- **Streamlined Operations Centralized:** servers facilitate faster decision-making and easier implementation due to efficient communication and coordination. This is crucial in sectors demanding rapid responses (e.g., healthcare (Grosman-Rimon et al., 2023)).
- **Unified Management:** Centralized data and control enable a coherent management structure, allowing for quick information dissemination and directive execution.

2.3.1.2 Vulnerabilities

Centralized systems are susceptible to single point of failures due to server breakdowns or cyberattacks (Hesarkazzazi et al., 2022). And Increased internet connectivity exacerbates this risk (Mansfield-Devine, 2018). Moreover, centralized systems struggle with managing large data volumes, hindering performance and real-time processing (Jamilov et al., 2021). Data control concentration raises concerns about data manipulation, privacy breaches, and accountability (Zimmermann et al., 2018).

2.3.1.3 Moving Forward

Multi-layered security approaches involving encryption, intrusion detection, and regular audits can mitigate centralized system risks (WatchGuard Technologies, 2023). This subtly introduces a decentralized control paradigm, enhancing security and fostering a balance between efficiency and resilience.

2.3.2 Between distributed and decentralised

In the preceding sections, the terms decentralized and distributed have been used interchangeably to characterize distributed ledger technology (DLT) and blockchain systems. However, there

exists a subtle yet significant difference between these two types of systems.

Decentralized systems are characterized by the dispersion of control and decision-making across multiple nodes, as opposed to centralization, where these functions are concentrated in a single entity. This decentralization enhances the resilience of the system by mitigating the risks associated with centralised topology. In such systems, the compromise or failure of one node does not jeopardize the entire network's integrity. The Bitcoin blockchain is a prime example of a decentralized system. As described by Tschorsch and Scheuermann, in Bitcoin (Tschorsch and Scheuermann, 2016), each node in the network maintains a copy of the ledger and partakes in the consensus process through Proof of Work (PoW), ensuring a distributed control mechanism.

Distributed systems, on the other hand, emphasize the physical dispersion of computational resources across multiple locations. While a system can be both decentralized and distributed, it is possible for distributed systems to have centralized control. The core distinction between these two concepts lies in the locus of control and decision-making processes. In distributed systems, resources and data processing are spread out, but decision-making and control might still be centralized, as discussed by Coulouris et al. (Coulouris et al., 2005).

Therefore, while the terms 'decentralized' and 'distributed' are sometimes used interchangeably in the context of blockchain, they denote different structural aspects. Decentralization refers to the dispersion of authority and decision-making, whereas distribution relates to the physical arrangement of the network's resources. Understanding this distinction is crucial for comprehending the architecture and functionality of various blockchain implementations.

In this thesis, the exploration of blockchain topology and its applicability within the maritime sector draws upon the key distinction between decentralized and distributed architectures (Abdallah and Abdallah, 2022).

This distinction is particularly relevant when considering the complex operational environments of the maritime sector, where effective coordination and information exchange are pivotal for efficiency and safety.

2.3.3 Public, permissioned and private blockchains

In light of our exploration of the distinctions between centralized, decentralized, and distributed systems, we can now explore the various types of blockchain networks. These networks exemplify the varying degrees of decentralization and distribution, crucial elements in blockchain architecture.

- **Public Blockchains** epitomize both decentralization and distribution (Bitcoin, Ethereum, Litecoin, Dash, Solana, Polkadot..). In these networks, resources are physically dispersed across multiple locations, and decision-making is collaboratively managed across the network. Nodes typically operate anonymously, bolstering consensus integrity by ensuring

Chapter 2. Blockchain technology Overview

Table 2.1: Characteristics of different types of Blockchain

Characteristic	Public	Private or Consortium
Network access	Permission less	Permissioned
Identity	Anonymous	Identified
Node Trustworthiness	Low (nodes could be malicious)	High (nodes are generally trusted)
Decentralisation	Total	Partial
Decision making	Collective	Restricted to a number of nodes
Energy consumption	Higher	Lower
Finality	Non achievable	Is achievable
Transaction validation time	Longer	Shorter
Data Visibility	Open	Restricted to authorized members

identities do not influence outcomes. However, this anonymity can increase resource consumption and pose challenges to trust, as nodes might act maliciously (Benhamouda et al., 2020). Public blockchains also face issues with finality, the assurance that completed transactions cannot be altered, due to the potential of forks, *a situation where the blockchain diverges into two potential paths forward* (da Silva et al., 2019). This absence of a central validating authority means that although finality can asymptotically approach certainty, it is never fully guaranteed.

- Permissioned (Consortium) Blockchains** These networks (Hyperledger Fabric (HF) , Quorum, Corda, R Consortium Fabric, Sawtooth Hyperledger) offer a decentralized structure, but access is restricted to identified nodes. Once a node gains access, it becomes part of the decision-making process. However, resources are not fully distributed, and in some cases, decision-making is confined to a select group of nodes, diluting the network’s decentralization. Trust levels are typically higher in permissioned blockchains due to node identification and the vetting process. The partial decentralization and distribution, along with higher trust levels, allow for lower energy consumption compared to public networks, as consensus can be reached more efficiently. This also facilitates faster transaction validation and the achievement of finality, reducing the risk of forks and enabling the network to agree on its current state (Dinh et al., 2018).
- Private Blockchains** In private blockchain networks, nodes are also identified. Decentralization is minimal, and decision-making is centralized. This centralization might seem to contradict the ethos of blockchain technology. However, the critical innovation here is the maintenance of a distributed ledger: despite central control, the ledger is replicated across all participating nodes. This approach significantly reduces the decentralization aspect but retains the benefits of distribution. (Yang et al., 2020)

This architectural choice significantly mitigates the risks inherent in fully centralized

systems—such as a single point of failure or vulnerability to tampering—by ensuring that the ledger’s integrity is maintained through its distribution across multiple nodes. Thus, while the system may reduce the aspect of decentralization traditionally associated with blockchains, it strategically retains the core benefit of a distributed system.

These typologies illustrate the nuanced interplay between decentralization and distribution in blockchain networks and their implications for trust, resource consumption, and network integrity which are summarized in the table 2.1 above drawn from one of our publications/contributions that will be developed later in the third chapter (Abdallah et al., 2022).

Blockchain technology has demonstrated significant potential across various sectors due to its unique characteristics. For instance, in the financial sector, blockchain is primarily utilized for the exchange of value units without intermediaries, exemplified by the development of cryptocurrencies. The technology also finds applications in science and academia, where it aids in mitigating issues such as the reproducibility of experimental results and enhancing trust and collaboration among researchers (Leible et al., 2019).

However, the versatility of blockchain technology extends beyond these sectors. It is adaptable for diverse use cases.

For example, a particularly innovative application of blockchain technology is in the development of Decentralized Identifiers (DIDs), which represent a paradigm shift in digital identity. DIDs are a relatively new form of digital identification that are intrinsically linked to blockchain technology, enabling autonomous digital identity. Unlike traditional identifiers such as usernames or email addresses that are governed by centralized authorities, DIDs are designed to be controlled solely by their owners. This shift facilitates individuals to own and manage their identity data independently, without the need for intermediation.

The foundation of DIDs on blockchain and key pair technologies ensures a decentralized, tamper-proof system for recording and verifying identity information (Stockburger et al., 2021). Our investigation into DIDs was driven by their potential to foster transparency and accountability in online interactions. Through the lens of Self-Sovereign Identity (SSI), DIDs exemplify how control can be redistributed from centralized systems to the individual users at the network’s edges. This approach not only challenges the conventional trust paradigms in centralized identity systems but also illustrates the utility of SSI in scenarios requiring single-sign-on (SSO) capabilities. In such contexts, DIDs can facilitate secure authentication without necessitating the disclosure of private or sensitive information. Moreover, the portability afforded by DIDs underscores their suitability in applications requiring secure, verifiable credentials across different domains.

DIDs, based on blockchain and key pair technologies, offer a decentralized and tamper-proof system for recording and verifying identity information, while their main benefit lies in enhancing transparency and accountability in online interactions (Stockburger et al., 2021). They promote self-sovereign identity (SSI) by giving users control over their own identities and addressing trust issues in centralized systems. SSI can be effectively used in single-sign-on (SSO) scenarios,

Chapter 2. Blockchain technology Overview

requiring only identity proof without sharing private data, and in authentication contexts where portability of secure verifiable credentials is advantageous.

In the maritime sector, the attributes of blockchain are crucial for addressing specific operational needs and challenges. The implementation of technology, especially with its distinct features, is crucial for deploying blockchain solutions tailored to specific operational needs and challenges. These include ensuring data integrity, efficiency, and security within complex logistical processes.

BLOCKCHAIN IN THE MARITIME SECTOR

Contents

3.1 Maritime Information Systems	42
3.1.1 The Genesis and Evolution of Community Systems	43
3.1.2 Between Port and Cargo Community Systems	43
3.1.3 Functionalities of Community Systems	44
3.1.4 IMO: Into the maritime landscape	44
3.1.5 Continuous Evolution and the Introduction of the MSW System	45
3.2 Change prospects vs Innovational Resiliency	49
3.2.1 Blockchain interest for the sector	50
3.2.2 Partial Recognition and early adopters	51

Abdallah, R., Besancenot, J., Bertelle, C., Duvallet, C. and Gilletta, F., 2022, July. Assessing Blockchain Challenges in the Maritime Sector. In International Congress on Blockchain and Applications (pp. 13-22). Cham: Springer International Publishing, (Abdallah et al., 2023d).

This dissertation investigates the integration of blockchain technology within the complex maritime shipping ecosystem. This integration is seen as a pivotal strategy to augment traceability, efficiency, security, and sustainability from end to end. To anchor this research firmly in the existing academic discourse on blockchain technology and comprehensively review the extant body of knowledge, this chapter covers the state of the art of current technological trends in the maritime sector to ensure the proper alignment of our work.

This chapter is structured around a state-of-the-art review, aimed at contextualizing the maritime landscape and the burgeoning interest in blockchain technology. We establish a robust foundation for delving into the complex and evolving field of maritime informatics. The review adopts a well-recognized methodological framework in literature, known as triangulation (Ndanu and Syombua, 2015; Thurmond, 2001; Triangulation, 2014). This approach is crucial for attaining a comprehensive understanding of the phenomenon under investigation, as reliance on a single method often falls short. Consequently, initial hypotheses are posited and subsequently validated through various methodologies, leading to deeper and more insightful findings.

The investigation commences with an exhaustive systematic literature review, alongside a state-of-the-art analysis targeting the maritime sector. We then advance, as detailed in one of our publications (Abdallah et al., 2023e), towards a state-of-the-art review that distinctly addresses blockchain initiatives within the sector, having previously delineated the genesis of technological interest.

The primary aim of this phase is to produce a cohesive and extensive corpus of research. This integration facilitates a systematic comparison between existing studies and ongoing as well as forthcoming development efforts. Such comparative analysis is crucial for formulating new hypotheses relevant to the adoption of emerging technologies. These hypotheses and their ramifications are to be further dissected in the ensuing chapters of this thesis.

3.1 Maritime Information Systems

Maritime informatics, a field that combines the study of natural and engineered computational systems, plays a vital role in leveraging digital data and technological progress within the shipping and transport community.

Recognizing the dawn of the fourth industrial revolution in the maritime sector, the Transport and Logistics Domain team at the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) emphasizes the burgeoning role of digitalization, robotics, artificial intelligence, and big data (Lind et al., 2021). Thoughtful integration of these advancements is pivotal. Not just for augmenting operational efficiencies but also for addressing critical aspects such as safety, security, and environmental impact, all while considering their influence on global trade dynamics (Lind et al., 2021).

This approach is in sync with the United Nations 2030 Agenda for Sustainable Development, underpinning a sustainable maritime transport sector that is both a propeller and beneficiary of global trade and economic activities. Maritime informatics, therefore, stands out as an indispensable field, especially in facilitating this sector's adaptation to rapidly evolving digital landscapes.

The foreseeable future of shipping is one of transformative change, echoing the shifts witnessed over the past century. These changes, primarily driven by the quest for greater efficiency, cost-effectiveness, and environmental sustainability, underscore the critical role of maritime informatics. It ensures that transitions within the industry are not only effective but also generate substantial and long-lasting benefits.

Understanding the maritime shipping sector's scale and significance is essential. For decades, maritime transport has been a cornerstone of global economic growth. It has evolved significantly since the Industrial Revolution, with milestones like massification and digitization marking its journey described in the first chapter.

Today, approximately 90% of global trade is transported by sea, underscoring the sector's role as the backbone of international trade. Known for its cost-effectiveness and safety, maritime

transport is the preferred mode for bulk cargo movements, attracting a large number of enterprises involved in shipping, port operations, and ancillary activities.

The advent of containerized freight necessitated centralized hubs to manage the complexities of mass transportation, marking a shift from traditional bulk shipping methods. Ports emerged as pivotal hubs within shipping clusters, maximizing economic benefits and anchoring digitization across global markets. This state-of-the-art overview aims to survey these systems' intricacies, evolution, and the current landscape of maritime informatics.

3.1.1 The Genesis and Evolution of Community Systems

The growth in maritime trade, alongside the need for intermediaries and digitization, led to the emergence of more evolved structures like PCSs. Originating in European ports during the late 1970s, these systems represented a unified platform that facilitated information exchange among stakeholders within the maritime community. As depicted in Figure 10, these systems marked a significant evolution in the maritime information exchange paradigm.

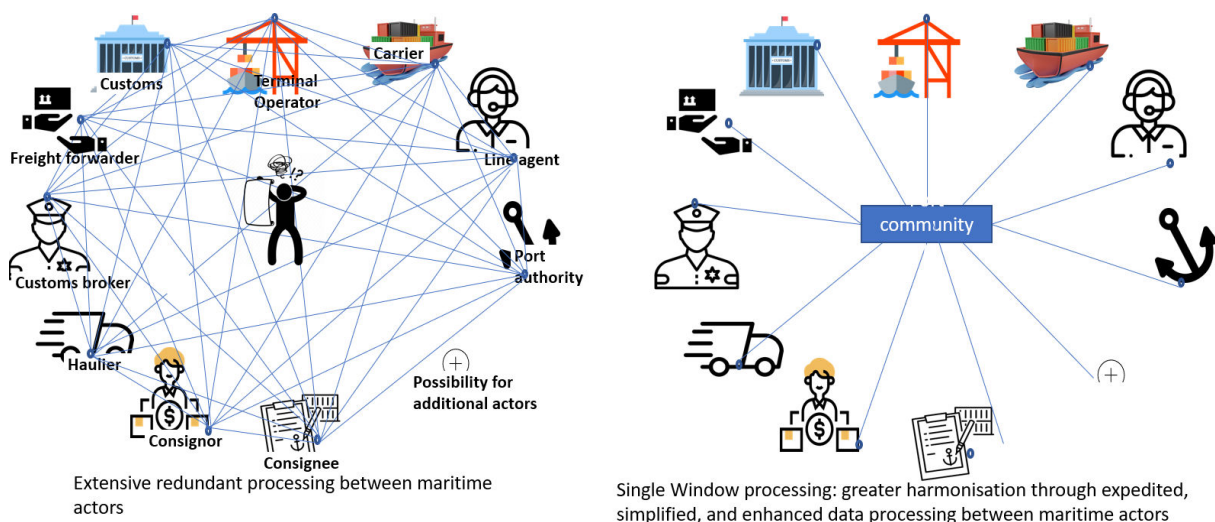


Figure 10: An exemplary representation of port community members before and after PCS: a single-window solution elaborated by the author.

3.1.2 Between Port and Cargo Community Systems

Heilig's observations (Heilig and Voß, 2017) highlight that as maritime clusters expanded and became more intricate the port milieu entities presented in chapter 1 became harder to discern. Consequently, the delineation between PCS and CCS grew less distinct. This evolution led to PCS and CCS adopting overlapping functionalities, making it challenging to clearly distinguish their specific roles within the broader maritime logistics landscape.

3.1.3 Functionalities of Community Systems

The benefits of these Community Systems quickly became evident as they spread globally, transforming the supply chain into a series of centralized nodes. Endorsed by UNCEFACT's Recommendation No. 33 (United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT), 2012), these systems have proven effective for both governmental and business entities.

Their impact goes beyond efficient resource allocation and fee collection by government entities. They have enabled better business compliance, and enhanced security measures, and contributed to a notable decrease in fraudulent activities. The advantages extend to reduced operational costs, expedited processing times, standardized procedures, clearer regulatory guidelines, and increased transparency. Collectively, these benefits foster sustainable logistics practices and contribute to reduced carbon emissions (IPCSA, 2022).

However, the specific functionalities of different maritime information systems can be elusive. Their community-centric nature means that functionalities are tailored to the needs and metrics of each community's stakeholders, leading to variations based on the specific actors within each community (Desiderio, 2011).

3.1.4 IMO: Into the maritime landscape

Building upon the foundation of maritime informatics and community systems and before presenting the current digitization trend, it's crucial to recognize the role of international organizations in shaping the global maritime landscape.

The maritime sector is a global industry spanning multiple continents. Therefore, there has long been a recognized need for international organizations that can facilitate coordination among globally dispersed maritime businesses.

Foremost among these is the International Maritime Organization (IMO). Which has been instrumental in fostering coordination, safety, and environmental responsibility in international shipping. The IMO's initiatives are aimed at creating a regulatory framework that ensures a level playing field while promoting efficient and sustainable maritime transport globally.

One of the key contributions of the IMO is the facilitation of the International Maritime Traffic (FAL) Convention. Initially, established by the International Maritime Organization (IMO) in 1965, it represents a landmark effort to boost international maritime trade by simplifying and minimizing the bureaucratic hurdles associated with maritime transport.

3.1.4.1 Genesis and adoption of the FALs

The FAL Convention was born out of a need to address the growing complexities and inefficiencies in international maritime traffic. Forming a basis upon which builds the technological development within community systems.

As global trade expanded rapidly in the post-World War II era, it became increasingly clear that the plethora of documentation and varying procedural requirements across different countries were impeding the smooth flow of maritime trade. To combat this, the IMO member states came together to formulate a convention that would standardize and facilitate maritime transport procedures, documentation, and formalities.

3.1.4.2 FALs roles and Objectives

The primary role of the FAL Convention is to streamline the formalities, documentary requirements, and procedures for ships' entry, stay, and departure in international ports. The convention includes standards and recommended practices to reduce the number and complexity of clearance formalities, thus facilitating faster, more efficient, and more predictable maritime transport.

It promotes practices aimed at reducing the bureaucratic burden on ships as well as ports, fostering more effective international maritime trade. Consequently, they have a direct impact on the development of the Maritime data exchange platforms.

Key contributions of the FAL conventions to the maritime information system include:

- **Standardization and Harmonization:** By standardizing the formalities and documentation for international maritime traffic, the FAL Convention has provided a unified framework around which PCS and CCS can be developed. This harmonization is crucial for ensuring consistency in information exchange across different ports and countries.
- **Promotion of Electronic Data exchange:** This has been a driving factor in the evolution of maritime information systems, pushing for more sophisticated, interconnected, and automated systems that can efficiently handle electronic data.
- **Enhancing Global Coordination and Compliance:** By setting global standards, the FAL Convention aids in harmonizing procedures across different countries and ports. Maritime information systems developed in accordance with these standards ensure better global coordination and compliance, leading to more efficient international maritime trade.

3.1.5 Continuous Evolution and the Introduction of the MSW System

The FAL Convention, like many international regulatory frameworks, is subject to ongoing review to ensure that it effectively meets its objectives in an ever-evolving global landscape.

This necessity for adaptation is particularly pertinent in the maritime sector, where technological advancements and changing global trade dynamics continuously reshape operational needs.

In response to these evolving requirements, the IMO has introduced significant amendments to the FAL Convention over time. One of the most notable amendments was the incorporation of the MSW System concept.

The MSW System Amendment

- In 2010, The European Union adopted directive 2010/65/EU, requiring member states to establish reporting formalities for ships entering or leaving their ports. This serves as a regional push for electronic data exchange in ports.
- In April 2016, the IMO's Facilitation Committee agreed to amend the Convention on Facilitation of International Maritime Traffic to mandate the implementation of electronic MSW globally.
- Around November 2023, the IMO announced the mandatory implementation of MSW changing the status of the directive to a regulation to become effective as of January 2024

This is considered an evolutionary approach to community systems.

This new electronic MSW encompasses the trade documentation outlined in the FAL Convention. This amendment builds upon extensive prior efforts to streamline reporting formalities and administrative procedures about maritime transport undertaken by the European Union. The electronic MSW builds upon existing practices and infrastructure used by maritime communities. It's not a completely new system, but an improvement on what's already there.

EU member states were required to establish national MSW s for receiving ship port call formalities by January 1, 2024 (International Maritime Organization, 2023). Moreover, the information furnished to the national MSW s must be submitted electronically and only once.

This amendment, adopted on 17 March 2023 (International Maritime Organization, 2022), represents a paradigm shift in the approach to handling maritime information and cargo processing. The MSW System is designed to enable all the information required about the arrival, stay, and departure of ships, cargo, and personnel. These data are to be submitted electronically through a single portal. This system streamlines processes, reducing the need for repetitive data submission and accelerating the clearance procedures in ports.

Implications for Maritime Information Systems The introduction of the MSW System is more than just a technological advancement; it signifies a strategic evolution in the management of maritime information exchange. This system brings numerous benefits:

- *Efficiency and Time-Saving:* By consolidating various reporting formalities into a single electronic submission point, the MSW System significantly reduces administrative overhead and processing time.
- *Enhanced Data Accuracy and Transparency:* Centralizing data submissions helps in maintaining data integrity and transparency, which is crucial for efficient maritime operations.
- *Global Standardization and Harmonization:* This amendment supports the global standardization of maritime data exchange, aligning different countries and ports on a common platform for information sharing.

Impact on Maritime Information Systems The FAL Convention and the MSW System are significant advancements for streamlining information exchange, but they primarily focus on mandatory reporting requirements. However, the concept of information sharing within the MSW system aligns well with the broader goals of maritime information systems. Maritime information systems cover a wide spectrum of activities given the heterogeneous nature of the business stakeholders and operations in the sector.

Maintaining safety and efficiency in maritime navigation relies on various systems. Of those are vessel traffic services, mandatory ship reporting, and automatic identification systems that allow competent authorities to monitor ship movements, particularly in congested or environmentally sensitive areas. Similar oversight occurs in ports, where vessel traffic services issuing instructions and collecting information promote safe and orderly port operations. Beyond real-time monitoring, ship clearance processes collect security, cargo, crew and passenger data to protect ports while facilitating trade. Although nautical safety and logistics have benefited from standardized electronic data exchange, other ship-port operations like supplies, services and voyage planning still employ less structured communication like email and fax. Overall, enhanced information sharing enables multiple authorities to meet safety, security and efficiency objectives in increasingly busy coastal and port waters.

As outlined in the research scope, this work focuses on a specific domain related to port activities and community systems within the taxonomy of maritime information systems. This is briefly illustrated in the Figure 11 below.

The circles in the diagram represent typical users of information management systems within the maritime sector (additional user groups may exist, this is simply a representative sample). The rounded rectangles denote classes within the taxonomy of maritime information systems. Each class describes a general set of functions that may be implemented in an information management system. This class taxonomy is a normalized representation of commonly found types of maritime information systems, which correspond to logical divisions of responsibilities across the public/private and local/international dimensions of the classification framework. Importantly, this diagram does not illustrate the governance superstructure or the distinct infrastructures of these systems. Those structures vary globally, and the heterogeneous supervisory elements specific to port systems will be detailed in subsequent chapters.

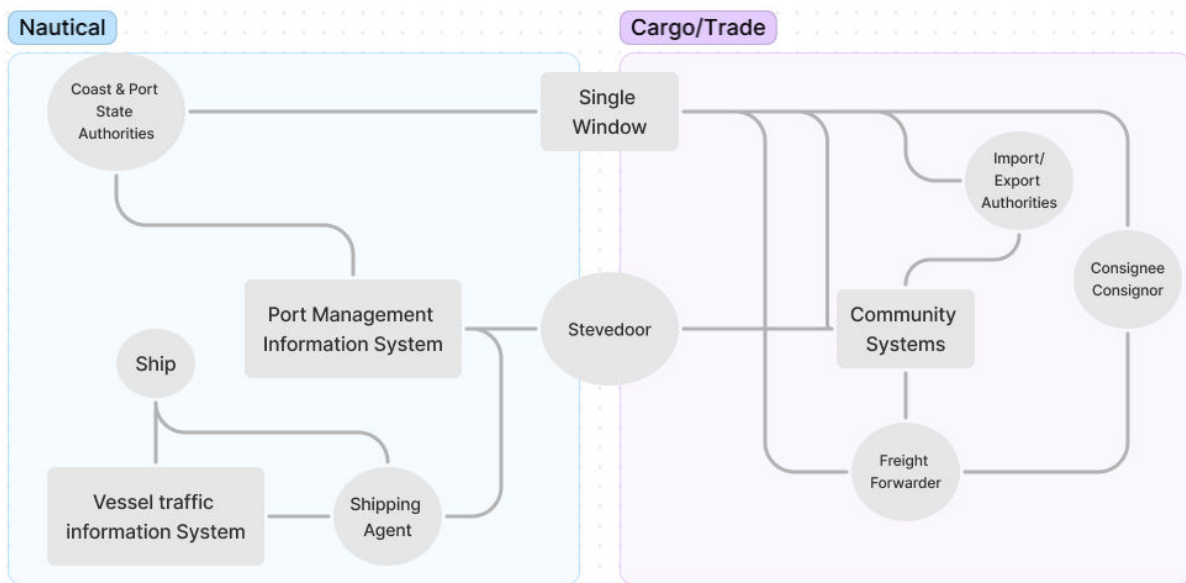


Figure 11: Maritime Information Systems taxonomy elaborated by the author.

Despite the focus of the Fals on community systems, the MSW System presents both challenges and opportunities. These systems must adapt to interface effectively with the MSW , ensuring seamless data integration and exchange. This adaptation is critical for maintaining the relevance and efficiency of PCS and CCS. Especially in the new framework set by the FAL Convention, where open data exchange could become detrimental to their competitiveness factor.

Looking Ahead The adoption and implementation of the MSW System amendment underscore the commitment of the maritime sector to embrace digital transformation. As the industry moves forward, it is essential to continually assess and refine these systems. It must be ensured that they not only comply with international standards but also effectively address the practical needs of the global maritime community.

It is also important to note that the implementation of these amendments can vary among IMO member states, depending on their readiness and capabilities to integrate these systems into their existing maritime infrastructures. Therefore, while the amendment represents a significant advancement in the FAL Convention, its impact is observed gradually as countries adopt and implement the system.

Even with global efforts made by the IPCSA and the IMO that encourage port-to-port collaboration and data exchanges, these efforts extend only to recommendations that cannot supersede the rivalries present, different governance, and ownership models of whom without their consent data exchange remains impossible.

3.2. Change prospects vs Innovational Resiliency

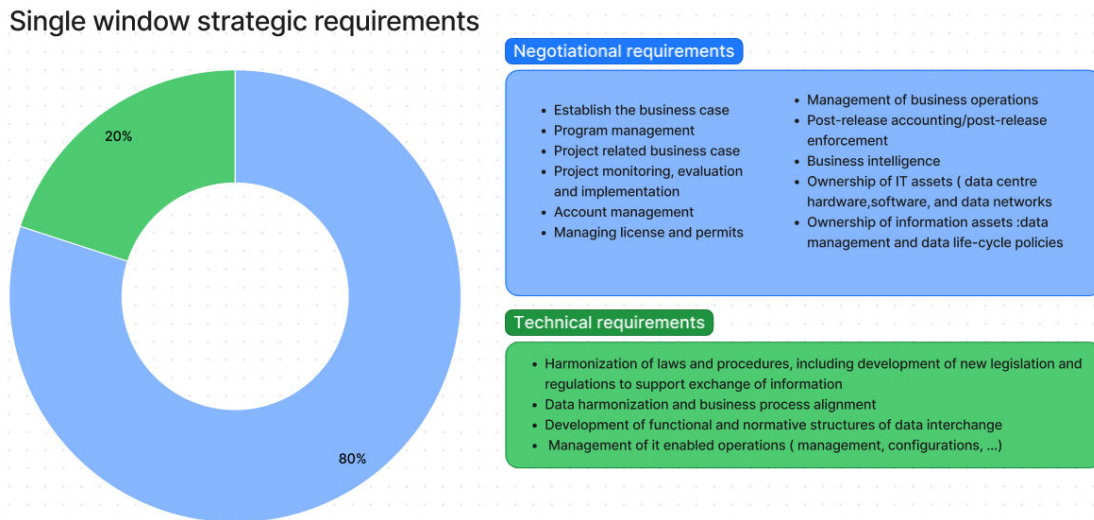


Figure 12: Actors’ strategic requirements analysis for a single-window system elaborated by the author.

Furthermore, the work requirements of establishing a single-window system mentioned in (Choi, 2011) can be divided into two main categories: negotiations and technical work. This aligns with the observation of the IPCSA, that not only do actors differ from one Community system to another but so can IT infrastructure and functionality. The analysis of the tasks and attribution to these categories clearly shows that the majority of the work is negotiating, as shown in (cf. Figure 12), which can mostly be linked to the distinct information systems of each participant. Although standardization, conventions and recommendations are crucial steps in implementation, inconsistencies exist among different community systems due to varying governance models and technological infrastructures. Consequently, integrating these systems can be very challenging. This is attributable to the evolution of these systems, which prioritized constructing an advantageous centralized data exchange platform without adequately considering the network’s architectural facets and scalability. Moreover, their emergence preceded peer-to-peer networks, which unlocked the potential for worldwide solutions.

Consequently, the global scale remained untouched, and the network remained fragmented into modular centralized systems. As a result, redundancy persisted, and automation possibilities remained limited.

3.2 Change prospects vs Innovational Resiliency

A behavioural change started appearing in the maritime sector and sustainability strategies. For example, the internationally widespread organization Maersk started searching for more effective digital solutions. These solutions are needed to overcome global inter-organizational obstacles in the supply chain, such as the multitude of actors and the complexity of regulations, while also ensuring a minimum of efficiency and digitization like the previously deployed

intra-organizational solutions (Jensen et al., 2019).

In addition, any revolutionary solution should be lucrative enough to generate sufficient interest from other maritime actors to revolutionize the industry.

This was confirmed by Knut Ørbeck-Nilssen, the Chief Operating Officer and President of DNV GL and Maritime and Director of Division Europe, Africa and Americas, in 2017. He emphasized that any technological innovation should also promote collaborative approaches to succeed because no maritime actor can act alone facing opportunities to reduce costs and facilitate exchanges (Jotun.com, 2022).

Furthermore, the introduction of new technologies to the maritime ecosystem required new technical capabilities which meant introducing additional costs in a gain-driven environment. This is why being lucrative was a key challenge in addition to a successful implementation with an infrastructure that was not designed for global digitization, and where data is vigilantly protected and very stingily shared. An optimal evolution of existing systems, in theory, grants global real-time access to shared data amongst the maritime network of participants forming a unified and trusted source of information and transforming the fragmented systems of the supply chain into a unique more evolved collectively maintained solution. This became technologically more achievable with the new and emerging technology called “Blockchain”.

The alignment between blockchain concepts and the omnipresent digitalization needs of the maritime ecosystem is **noteworthy**. These needs can be portrayed as the optimum digitized evolution for a sector with a multitude of participants. The technology has increasingly captured interest across various sectors.

3.2.1 Blockchain interest for the sector

Blockchain technology has characteristics that coherently parallel technological literary recommendations for revolutionizing the industry (Abdallah et al., 2023d).

- It facilitates the transition from globally fragmented centralized systems to a peer-to-peer network without the need to establish complete trust between actors.
- Real-time data accessibility is granted through the distributed append-only digital registry that is collectively maintained through a consensus mechanism.
- The consensus mechanism is the rule by which the ledger is extended, and additional data is recorded that guarantees nodes' honesty.
- The timestamping, encryption, and chaining of the data establish immutability that consequently elevates tracking, tracing, and certifiability for the sector.
- Additionally, several advantages result from the use of blockchains such as the alleviation of cyber burdens and data protection through cryptographic algorithms and encryption, in

3.2. Change prospects vs Innovational Resiliency

addition to the elimination of single points of failure and the need for trusted intermediaries existing in centralized systems through decentralizations and automation via smart contracts.

Hence, this technological shift might engender a colossal effect on the sector with an unprecedented estimated 15% improvement and growth in world trade (weforum, 2022) and reduction of transportation costs by 20% (Wang and Qu, 2019). Likewise, digitization and smart contracts provide increased personalized automated services. Moreover, Ref. (Jensen et al., 2019) highlights an achievable 40% decrease in delivery delays.

3.2.2 Partial Recognition and early adopters

Blockchain has successfully evolved in the financial sector with several successful projects such as Bitcoin, Ethereum, and others that have been adopted on a global scale.

This seamless exchange is not only restricted to financial assets but expands to include tangible and intangible assets. Consequently, blockchain can be used in the maritime sector for more seamless operational processing and digitization.

It has been reflected the technology has successfully sparked interest in other sectors, including the maritime industry, where multiple projects emerged. As a contribution to this thesis and a foundation for future work, we fully scanned the sector's blockchain project and grouped them into one of our contributions. (cf. Table 3.1 (Abdallah et al., 2023d).)

Chapter 3. Blockchain in the maritime sector

Usecase	Project	Owner/proposer	Blockchain used	Documentation
Fuel quality and traceability	BunkerTrace	Blockchain labs for open collaborative and Main Blockchain Labs	Ethereum	bunkertrace.co
Shipment Tracking	TradeLens	Maersk and IBM	Hyperledger Fabric	tradelens.com
	GSBN	Oracle, Microsoft, AntChain and Alibaba Cloud	AntChain	gsbn.trade
	Silsal	Abu Dhabi Port	Hyperledger Fabric	adports.ae
	Calista	PSA International, and Global eTrade Services (GeTS)	Not a blockchain an intensive API delivering end-to-end data (based on blockchain concepts)	calistalogistics.com
Track and Trace hazardous goods	(pilot project)	BLOC and Lloyd's register foundation and rainmaking consortium project	Not disclosed	lr-foundation-bloc
Smart Bill of Lading	CargoX	CargoX	Ethereum	cargox.io
	TradeLens	Maersk and IBM	Hyperledger Fabric	tradelens.com
	Bolero's digital trade platform	Bolero	Volton Corda based	bolero.net
	Easy Trading Connect	Blue Water Shipping Louis Dreyfus	Ethereum Quorum	ldc.com
	(PoC)	Pacific International Lines ,and PSA International and IBM Singapore	Hyperledger Fabric	globalpsa.com
	WAVEBL	WAVE BL	private blockchain	wavebl.com
Digitization	Tokio Marine	Tokio Marine Holdings	Corda	gtsreview.com
	(storage on blockchain)	DNV GL	Vechain Thor	dnv.com
Smart Contracts	Blockconnect	300Cubits	Ethereum	300cubits.tech
	ShipChain	ShipChain	Ethereum	freightwaves.com
Insurance and finances	(PoC: maritime insurance platform)	A.P.Møller-Maersk, Willis Towers Waston, MS Amilin, and XL Catlin	Corda	wtwco.com
	(PoC: Blockchain Insurance Industry Initiative)	B3i Services AG	Corda	b3i.tech
	(enterprise-level blockchain consortium)	RiskStream Collaborativ	Corda	theinstitutes.org
	Shipowners	Shipowner.io	Ethereum	shipowner.io
	Skuchain	Founded by Srinivasan Sriram	Hyperledger Fabric	skuchain.com
	Provenance	Owned by Morgan McKenney	Ethereum	provenance.io
VGM Portal	Tallysticks	Co-founded by Kush Patel		f6s.com
	SOLASVGM	Kuehne + Nagel Group	Hyperledger Fabric	kuehne-nagel.com

Table 3.1: Blockchain projects' use cases in the maritime sector.

However, not all projects were successful. By successful, we restrict the interpretation of the word to implying sustainability or survival. This is because we cannot judge the idea behind the project nor its implementation. as some were correctly implemented but failed to survive in the ecosystem.

These projects differ in concept and cover multiple areas of the logistical maritime operations, from storage to delivery and payments, as well as the improved transparency and security achieved. For example, the project "TradeLens" is a joint idea between two competent companies, IBM and Maersk, with the ultimate goal of cost-effective improved traceability. Another example is "CargoX" which focuses on document digitization, such as bills of lading. It aims to provide a secure, reliable, and time- and cost-effective method of processing shipping paperwork anywhere on the globe.

Other projects went further and targeted payment methods in the maritime industry with the idea of a global decentralized currency such as ShipChain or 300Cubits.

For example, ShipChain's initiative with the SHIP token exemplifies an innovative approach

3.2. Change prospects vs Innovational Resiliency

to streamlining transactions. However, this project encountered several barriers that hindered its widespread adoption. A comprehensive analysis of these challenges, including those faced by similar projects in the sector, will be presented in the subsequent chapter. This analysis will not only highlight critical pitfalls to be avoided but also provide insights into the potential obstacles anticipated within this industry.

This state-of-the-art work highlights the need for a study targeting the technology's potential and challenges to identify real and successful applications and recommendations for the technology in the maritime sector to achieve its full efficacy and avoid being substandard.

Part II

Contributions: Implementing Blockchain for the maritime: from theory to proof of concept

The maritime industry is moving towards a digital ecosystem to achieve substantial mutual profits. To achieve this, there have been attempts to combine existing, disjointed systems into more efficient, standardized platforms that can be scaled up. However, this transition has faced challenges. To address these issues, it is suggested that innovative technologies such as blockchain be utilized due to their alignment with the sector's needs. We use a triangulation approach by examining a mix of literature, web-based data, applications, and projects to showcase the contribution of blockchain and its potential use cases. We also explore its potential use cases based on other sectors using projection and parallelism. Additionally, the study delves into limitations and possible solutions. This research acts as a preliminary study for the implementation of blockchain in the maritime industry and advocates for its use as a revolutionary approach. The findings will be beneficial for scholars, policymakers, and practitioners in the maritime industry.

This thesis investigates the integration of blockchain technology into maritime logistics, a critical sector that stands to benefit significantly from enhanced security, transparency, and efficiency. By meticulously conceptualizing, implementing, and evaluating a blockchain-based infrastructure, this work navigates through the technical and operational intricacies involved in bringing this disruptive technology to the maritime domain. Through a blend of theoretical exploration and practical application, the research delves into the design and deployment of smart contracts within Port Community Systems, the development of user-centric interfaces for seamless interaction with blockchain-secured data, and the rigorous evaluation of the system's performance. Then, we proceed to set our PoC within its broader envisioned context within the sector detailing on-going effort for a futuristic approach. Culminating in a vision for the future, this thesis not only demonstrates the potential of blockchain for maritime logistics but also charts a course for ongoing and future advancements in this field, laying the groundwork for a more interconnected and technologically advanced maritime industry.

In conclusion, we offer a forward-looking perspective to address real-world challenges based on the limitations identified in our analysis of the technology's evolution and its current capabilities.

AN ANALYSIS FROM A MARITIME PERSPECTIVE ON BLOCKCHAIN

Contents

4.1 Bridging Blockchain’s Promise and Maritime Realities: A Pragmatic Approach to Sectoral Adoption	60
4.1.1 An evident based approach	60
4.1.2 key takeaways	69
4.2 A methodology reflexion	70
4.3 How can blockchain enhance the maritime industry’s performance? . . .	70
4.3.1 A global decentralized communication system	71
4.3.2 Increase operational efficiency	71
4.3.3 Reduced Data Storage	73
4.3.4 Adjoint supplementary security priviliges	73
4.3.5 Prevent and decrease pollutions	73
4.3.6 Fight Fraud and prevent corruption	75
4.3.7 Eliminate unnecessary intermediaries	76
4.3.8 An Extended Spectrum of Use Cases	76
4.4 Blockchain Challenges	78
4.4.1 Blockchain’s limited use outside of the private sector	78
4.4.2 Blockchain predates regulations	78
4.4.3 Scrutiny: The Result of Transparency	79
4.4.4 Security Challenges	79
4.4.5 Network and Technical Challenges	80
4.4.6 Data and Storage	80
4.4.7 The Nexus between Code and Logic in Business	82
4.4.8 Smart Contracts	83
4.4.9 Oracles	83

Chapter 4. An Analysis from a Maritime Perspective on Blockchain

4.4.10 Interoperability 83

4.4.11 Common Code Sense 84

4.4.12 Unquantifiable Clauses 84

4.5 Discussion 85

Abdallah, R., Bertelle, C., Duvallet, C., Besancenot, J. and Gilletta, F., 2022, August. Blockchain Potentials in the Maritime Sector: A Survey. In The International Conference on Innovations in Computing Research (pp. 293-309). Cham: Springer International Publishing, (Abdallah et al., 2022).

Abdallah, R., Besancenot, J., Bertelle, C., Duvallet, C. and Gilletta, F., 2023. An Extensive Preliminary Blockchain Survey from a Maritime Perspective. Smart Cities, 6(2), pp.846-877, (Abdallah et al., 2023e).

In the dynamic context of the maritime industry, blockchain technology represents a pivotal innovation. Prior sections of this dissertation have highlighted the industry's inclination towards blockchain adoption, as demonstrated by various initiatives and projects. Yet, the essence of this discourse extends beyond mere adoption. It critically examines the intricacies of blockchain's implementation, its successes, and the challenges encountered within the maritime domain.

The maritime industry's explorations of blockchain have highlighted that successfully harnessing this technology necessitates meticulous alignment with operational realities, stakeholder dynamics, and regulatory frameworks. While the hype surrounding blockchain often presupposes a seamless integration across sectors, a closer examination reveals a more nuanced trajectory colored by sectoral idiosyncrasies.

Early maritime blockchain pilots have paved critical success factors and impediments that demand careful navigation. Foremost is recognizing where blockchain's strengths can solve high-impact pain points within maritime workflows. Numerous exploratory projects have fallen short by deploying blockchain in a vacuum without adequately addressing entrenched legacy systems or stakeholder incentives. Conversely, initiatives that closely analyze maritime operations to pinpoint friction points are better primed for adoption.

While much excitement surrounds blockchain's potential to reshape business models, maritime applications demand prudent governance frameworks that balance innovation with pragmatism. Navigating these trade-offs will shape the trajectory of blockchain in maritime. Additionally, blockchain networks must recognize the sector's global interconnectedness, incorporating both developed and emerging economies through inclusive architecture and governance.

In light of these insights, this chapter is structured into three main sections. Firstly, an analysis of blockchain applications within the maritime sector is conducted. This involves a thorough examination of past projects, evaluating their successes and failures, and identifying how these experiences can inform future applications.

Secondly, the characteristics of blockchain technology are scrutinized and aligned with the specific needs of the maritime sector. This analysis aims to identify key blockchain features that could be leveraged in our technological implementations, targeting enhancements in efficiency, security, and transparency within maritime operations.

Finally, the chapter addresses challenges awaiting solutions that not only pave the way for

incorporating these considerations into future developments but also establish a solid foundation for substantiating the technological capabilities in overcoming these obstacles.

This exploration extends beyond a mere analysis; it contributes to the broader discourse on blockchain technology across various industries notably the maritime sector. It aims to move past the hype and provide a grounded perspective on practical implementations. By focusing on sector-specific applications and challenges, this chapter endeavors to offer a nuanced understanding of blockchain's role in maritime operations, thereby contributing to the technology's ongoing evolution in a global context.

4.1 Bridging Blockchain's Promise and Maritime Realities: A Pragmatic Approach to Sectoral Adoption

Adopting blockchain in the maritime sector goes beyond just theoretical capabilities; it calls for a realistic look at past efforts. A pragmatic lens is imperative to assess challenges in implementing blockchain maritime solutions and strategies to address them.

Obstacles range from integration with legacy infrastructure, fragmented jurisdictional environments, and varying stakeholder capabilities. Furthermore, good governance frameworks that balance decentralization with necessary oversight are pivotal for aligned regulatory outcomes. Technical architecture must account for maritime-specific data formats, interfaces, security needs, technological evolutions and global interoperability.

Many projects faced hurdles, not because of the technology itself, but due to a mismatch with maritime operations. This insight emphasizes the importance of a detailed analysis that tailors blockchain solutions to fit the sector's specific needs. This approach isn't just good for maritime; it's a guide for any field trying to mesh new tech into their operations.

By focusing on blockchain through a maritime lens, this study helps bridge the gap between academic study and real-world use, setting the stage for blockchain to move from a neat idea to a key player in making maritime logistics more transparent, efficient, safe, and green.

4.1.1 An evident based approach

We first adopt an evidence-based approach to analyze some of the previously presented specific blockchain projects, focusing on their real-world applications and outcomes. We aim to provide a critical analysis of blockchain projects that, encountered significant challenges leading to their failure. Understanding the reasons behind this failure is as crucial as recognizing the success factors in successful projects. It allows for a comprehensive learning experience, informing future endeavours in the sector and mitigating the risk of repeating similar mistakes.

4.1. Bridging Blockchain's Promise and Maritime Realities: A Pragmatic Approach to Sectoral Adoption

4.1.1.1 VGM blockchain portal

A pertinent case study in this context is the deployment of blockchain technology in the Verified Gross Mass (VGM) Portal by Kuehne + Nagel.

The VGM Portal project, last documented online in 2018 (Kuehne + Nagel, 2018) presented in Table 3.1, exemplifies a practical blockchain application in the maritime sector. This project was designed to augment the VGM solution, thereby improving business operations' efficiency and enhancing transparency regarding the VGM status of customer shipments.

Context The IMO, in its quest to bolster safety and efficiency in international maritime operations, has established several conventions, including the Safety of Life at Sea (SOLAS) convention. This treaty is pivotal for the safety of merchant ships. An accurate determination of Verified Gross Mass (VGM) (IMO, 2016) is critical in maritime logistics for ensuring safety and compliance. The VGM is the sum of the certified gross cargo weight plus the container's tare weight. It is essential for balanced ship loading and preventing risks like container collapse or ship listing. And, as of 2016, it became mandatory for all loaded containers to have a declared VGM.

Traditional methodology There are two approved methods for calculating the VGM:

- Weighing the packed and sealed container using a certified weighing bridge or device.
- Computing the VGM by adding the container's tare weight to a verified cargo weight.

The enforcement of SOLAS requirements for the VGM is the responsibility of the SOLAS Contracting Governments. According to the regulation, it is the shipper's responsibility to ensure the VGM is accurately provided to the relevant parties. There is no requirement for the carrier or terminal to recheck, verify, certify, or reweigh the VGM. The mechanisms for enforcement included:

- Documentation Verification (Line, 2024)
- Regulatory Audits and Checks (Thompson, 2018)
- Carrier and Terminal Operator Policies (SERVICE, 2022)

These practices, while effective to a degree, had limitations. The manual and semi-automated nature of these processes led to potential inaccuracies due to human error, data entry mistakes, redundancy and the possibility of fraudulent weight declarations.

4.1.1.2 Blockchain-based VGM Portal

Kuehne + Nagel's implementation of blockchain in their VGM Portal aimed to address these issues by leveraging blockchain's decentralized and immutable characteristics for real-time access, verification and certification of VGM data among stakeholders.

Chapter 4. An Analysis from a Maritime Perspective on Blockchain

The analytical examination of the Verified Gross Mass (VGM) Portal project, under the umbrella of Kuehne + Nagel and their deployment of blockchain technology, reveals a nuanced understanding of the intricacies involved in successful technological integration within the maritime logistics sector.

- **Reasonable Use Case:** *The project's cornerstone was its well-defined use case: VGM data recollection. A systematic approach to technological adoption, emphasizing relevance and applicability over mere innovation.*
- **Blockchain Maturity:** *selecting a blockchain platform capable of scaling effectively to manage the VGM data requirements without discrepancies. (Kuehne + Nagel, 2018)(Team, 2018)*
- **Privacy of Information:** *The project highlighted blockchain's strength in preserving data privacy. With Kuehne + Nagel's involvement at both ends of the transaction, the focus was on data verification, minimizing the exposure of sensitive information.*
- **Legal Clarity:** *The legal framework underpinning the VGM Portal project, particularly the International Maritime Organization (IMO) treaty established in 1960 and enforced from 1965, plays a critical role in the project's success, especially from a legal and regulatory perspective.*
 - **Responsibility and Data Management by the Shipper:** *First, the data entry point – the shipper – is clearly defined. Secondly, and perhaps more importantly, it alleviates potential legal issues related to blockchain technology. Since the shipper is responsible for data entry and initial verification, the role of blockchain is primarily to ensure the integrity and traceability of the data once entered into the system.*
 - **No ambiguities in legal and regulatory practices:** *A sufficient time has passed since the establishment of the treaty*
 - **Easing Blockchain Legal Issues:** *By positioning blockchain as a technology for enhancing transparency and verification, rather than as the primary legal record keeper, the project avoids complex legal questions that might arise if blockchain were to assume a more central role in the legal documentation process.*

Synthesis The VGM Portal project by Kuehne + Nagel offers valuable insights for the scholarly and practical exploration of blockchain in maritime logistics. Its core lessons emphasize the importance of selecting mature, scalable blockchain solutions tailored to the maritime sector's unique needs. This strategic selection is crucial, as it ensures the technology can effectively manage maritime operations' complex data requirements.

Furthermore, the project showcases how blockchain can safeguard sensitive logistical data, striking a critical balance between operational transparency and data privacy. This balance is essential in a field where confidentiality and security are paramount.

4.1. Bridging Blockchain's Promise and Maritime Realities: A Pragmatic Approach to Sectoral Adoption

Lastly, navigating the legal intricacies associated with blockchain's use in international maritime operations, the project aligns with the established IMO treaty framework. This alignment clarifies stakeholder responsibilities and uses blockchain for enhancing data integrity and transparency, sidestepping potential legal hurdles associated with data custodianship.

4.1.1.3 300Cubits

The 300 Cubits project, centered around the TEU Token, presents another compelling case study in the blockchain space within maritime logistics. This initiative was an innovative attempt to address the perennial issue of container no-shows and rolled cargo

Context : Maritime rolled Cargo The phenomenon of rolled cargo in maritime logistics reflects a significant challenge within the industry. Booked cargo is postponed to a later voyage due to overbooking by shippers. This situation, akin to airline booking practices where more tickets are sold than available seats under the expectation of no-shows, arises because container bookings traditionally don't require a deposit. This lack of financial commitment from customers leads to a scenario where, if all booked cargo arrives, there's insufficient space, necessitating the rolling of some cargo to subsequent voyages.

This practice introduces several inefficiencies and logistical hurdles. For one, it disrupts planned schedules and inventory management, leading to delays and potentially escalating costs for both shippers and receivers. Moreover, the cascading effect of rolled cargo can affect subsequent shipping schedules and broader supply chains, highlighting the need for improved management strategies in container bookings and cargo handling.

Blockchain-based solution: TEU tokens The TEU Token initiative aimed to mitigate the issue of no-shows and rolled cargo by introducing a blockchain-based deposit mechanism. This approach required carriers and shippers to use TEU tokens as a form of commitment to their cargo bookings, aiming to encourage adherence to shipping agreements and reduce inefficiencies associated with cargo rolling. Both carriers and shippers would place tokens as a form of commitment to their bookings, incentivizing adherence to agreements and reducing the likelihood of no-shows and rollings.

Project Outcome The project faced closure due to several factors that culminated in its inability to sustain operations commercially. Despite being an early innovator in applying blockchain technology to maritime logistics, the venture struggled with low transaction volume, indicating that the uptake of TEU tokens among potential users was minimal. Despite the system's live operations since July 2018, only a few hundred container bookings were processed, far from enough to maintain commercial viability (ZMUDZINSKI, 2019).

Chapter 4. An Analysis from a Maritime Perspective on Blockchain

Synthesis The analysis of the 300 Cubits: TEU Token project reveals several critical missteps that contributed to its failure. Understanding these errors is essential for developing more robust and effective blockchain solutions in the future, particularly in the complex and regulation-heavy context of maritime logistics.

- **Lack of Intrinsic Value and Price Volatility:** *The tokens were initially given for free to maritime actors, with the expectation that real value would be generated through a secondary exchange market. This approach led to significant price volatility due to varying perceptions of the token's value among different stakeholders. The volatile nature of the token's value undermined its reliability and attractiveness as a stable medium of exchange or deposit, which is crucial in the context of contractual commitments in maritime logistics.*
- **Problem Misconception:** *the project overlooked simpler, more recognized legal solutions such as edited freight contracts. These traditional contracts are already recognized and understood within the legal frameworks of maritime logistics, suggesting that an enhanced contractual approach, rather than a technological one, might have been more effective in addressing the issue.*
- **Market Adoption Challenges:** *One of the primary reasons for the failure of the TEU Token was the challenge in achieving widespread market adoption. The success of such a project heavily relies on broad acceptance and participation from industry stakeholders.*
- **Complexity in Implementation:** *The implementation of the TEU Token system was complex, involving significant changes to existing operational processes. Many companies in the maritime sector were hesitant to overhaul their established systems for an unproven solution, especially when the existing processes, despite their inefficiencies, were familiar and predictable.*
- **Technological Limitations and Integration Issues:** *The integration of blockchain with existing IT infrastructure poses significant challenges.*
- **Regulatory Ambiguities:** *The introduction of a cryptocurrency-based solution in a global industry like maritime logistics, where each jurisdiction may have different regulations regarding digital currencies and smart contracts, created a complex legal environment.*

If the 300 Cubits project were to revisit its approach revisiting the VGM blockchain portal synthesis, several key strategies could be capitalized on to mitigate rolled cargo.

By leveraging blockchain, shippers gain real-time access to data on cargo status and port activities, which is instrumental in navigating the complexities of peak seasons and avoiding potential bottlenecks.

4.1. Bridging Blockchain's Promise and Maritime Realities: A Pragmatic Approach to Sectoral Adoption

Blockchain's immutable ledger ensures that all parties have access to consistent and unalterable data, from booking to delivery milestones. This clarity allows shippers to make informed decisions well ahead of shipping deadlines, reducing the risk of last-minute rollovers due to overbooking or documentation errors. Moreover, when issues like port congestion signal tight shipping capacity, shippers can proactively secure the necessary capacity, thanks to the foresight provided by blockchain-driven insights.

Blockchain can streamline the reevaluation of shipping and documentation processes. In instances where rollovers occur, the detailed tracking and recording capabilities of blockchain provide a clear audit trail. This helps identify the root causes of rollovers, whether they stem from booking practices or documentation mishandling, enabling targeted improvements to prevent future occurrences.

By embedding blockchain within their operational framework, shippers can elevate their supply chain visibility, turning potential disruptions into manageable challenges with strategic foresight and proactive planning. This approach not only diminishes the likelihood of rollovers but also strengthens the overall resilience and efficiency of maritime logistics operations.

4.1.1.4 TradeLens

In furtherance of our examination of premortem projects, we have elected to focus our analysis on a project jointly undertaken by IBM, a preeminent global technology corporation (IBM, 2022), and Maersk, a prominent maritime carrier company. Maersk, with a storied history dating back to its founding in 1904. This company commands a substantial market share, boasting a formidable 15.3 percent underscoring their prominence and influence for the sector (Statista, 2022).

TradeLens began as distinct endeavors within these two companies. They both acknowledged the significant benefits that could be reaped from merging digital technology with the maritime sector. It was within this framework that these two entities joined forces to bring to market a solution that leveraged blockchain technology to enhance value within the container shipping industry.

Context Global supply chains, particularly those entailing maritime container shipping, constitute a complex and intricate ecosystem involving a diverse array of stakeholders. These stakeholders encompass producers, traders, importers, exporters, transport and service providers, as well as governmental entities. This multifaceted supply chain process can be delineated into three principal phases:

- **Goods Exportation:** Commencing in the originating country, this phase encompasses the packaging of goods onto pallets and their subsequent placement into containers. Subsequently, these laden containers are conveyed, typically by freight forwarders, using a combination of road or rail transport to reach the nearest seaport, designated as the port of origin. At this juncture, the goods undergo export clearance procedures mandated by

the relevant authorities before they are laden onto container ships under the supervision of the port terminal operator.

- **Maritime Conveyance:** The subsequent stage is marked by the actual maritime transportation of these goods across vast expanses of open water. Container ships serve as the conduit for the conveyance of these containers to their intended destination country, traversing diverse maritime routes en route.
- **Importation and Final Delivery:** As the containers near the port of destination, they are subjected to security clearance measures prior to their arrival. Upon reaching the designated port of destination, the containers are offloaded from the vessel under the purview of the port terminal operator. Following import clearance procedures administered by local authorities, these containers are then transferred onto various modes of transport, including trucks, trains, or barges. The concluding leg of this journey is managed by freight forwarders, culminating in the delivery of the goods to their ultimate consignees.

The fundamental objective of the proposed solution was to address the imperative issue of delivering tangible business value while concurrently mitigating the inefficiencies and security vulnerabilities inherent in global supply chains reliant on container shipping.

As a consequence, global supply chains grapple with an array of inefficiencies and impediments to seamless trade, primarily attributable to three overarching challenges: the exorbitant costs associated with administrative processes, the unpredictable arrival schedules of goods, and the rigorous security protocols imposed.

About TradeLens TradeLens endeavors to confront these challenges by offering an inclusive and impartial industry platform that facilitates the exchange of critical shipping data and pivotal trade documentation among a diverse spectrum of stakeholders, even including entities that may be in direct competition with one another.

The evolution of TradeLens diverged from the conventional trajectory of typical IT projects, which typically embark upon their journey armed with well-defined requirements and precise endpoint objectives. In contrast, the genesis of TradeLens transpired through a series of pioneering initiatives, collaborative endeavors, and pre-existing solutions, operating under various appellations. Over time, these disparate elements coalesced to form the cohesive entity now recognized as TradeLens. This transformative journey, spanning the period from 2013 to 2019, bore witness to several pivotal milestones and involved a multitude of influential participants, as elucidated within the project's comprehensive timeline.

The TradeLens initiative, born from the collaboration between Maersk and IBM, represents an innovative departure from conventional IT development practices, particularly within the domain of global trade digitization. Instead of commencing with predefined requirements and set objectives, TradeLens emerged through the fusion of two pivotal initiatives: the Shipping

4.1. Bridging Blockchain's Promise and Maritime Realities: A Pragmatic Approach to Sectoral Adoption

Information Pipeline (SIP) and the Paperless Trade (PT) blockchain network. These prototypes played an indispensable role in the digital capture and sharing of essential shipping data and the secure encryption of critical global trade documents.

The developmental process encompassed the meticulous selection of specific documents for integration into the blockchain solution, with a particular emphasis on those necessitated by importing authorities, distinguished by their original stamps and signatures, ensuring uniqueness and authenticity. This critical decision crystallized during a pivotal joint workshop held in New York in June 2016. However, as the project advanced, challenges surfaced due to the dispersed nature of the development teams spread across the globe, resulting in diverse focal points and intricacies.

A momentous breakthrough was achieved in December 2016 when a successful prototype was piloted on a trade route responsible for the transportation of fresh cut roses from Kenya to Europe. This live pilot program, involving tangible shipments and active participation from authorities on both sides of the Atlantic, effectively validated the viability of a blockchain-powered solution for global trade.

In 2017, under the stewardship of Maersk's new chairman and augmented support from top-tier management, the project continued to evolve, striving to transform into a market-ready iteration. By December 2018, the Global Trade Digitization (GTD) team declared TradeLens as commercially available, positioning it as an open, impartial, decentralized platform catering to container shipping, underpinned by the foundations of blockchain technology. This platform was meticulously designed to facilitate secure, authenticated, and auditable transactions and information exchange. Additionally, it harnessed smart contracts to automate functions such as import clearance. TradeLens thus stands as a testament to the boundless potential of collaborative innovation in the paradigm shift underway within the global supply chain ecosystem.

The rest of key events that marked milestones in the product's journey are as follows:

- *2018*: TradeLens was officially announced and launched as a collaborative venture between IBM and Maersk.
- *2019*: TradeLens received a significant boost when the Federal Maritime Commission (FMC) endorsed "The TradeLens Agreement," authorizing cooperative efforts toward a blockchain-enabled, globally digitized trade solution.
- *2021*: The electronic bill of lading (eBL) system of TradeLens garnered approval from the International Group of P&I Clubs for use by its member entities.
- *2023*: A decision was made to discontinue the TradeLens platform due to commercial viability challenges and other pertinent issues.

Synthesis The following sections will dissect the various aspects that contributed to its ultimate discontinuation, drawing from the collective wisdom of academic and industry contributions in

the field.

TradeLens Solution Deployment: A seminal study (Jensen et al., 2019) has previously outlined the principles underpinning TradeLens and its potential to deliver substantial business value. This along with the commercialization and services made available sheds light on whether the platform was able to fulfill these promises and overcome its inherent challenges.

Louw-Reimer et al. have addressed the utilization of hybrid cloud blockchain in TradeLens, emphasizing its potential to enhance containerized supply chains. This brings forward the challenges faced by various stakeholders in adopting this platform and whether these challenges proved insurmountable (Louw-Reimer et al., 2021). What were the primary challenges faced by stakeholders in adopting the TradeLens platform? Did technical limitations of hybrid cloud blockchain technology hinder TradeLens' effectiveness?

The work of Bauk presents a comprehensive framework for the deployment of blockchain in maritime, including its potential strengths and weaknesses in the context of TradeLens (Bauk, 2022). Consequently, it is important to encompass the alignment between theoretical and conceptual frameworks and whether any deviations contributed to its discontinuation. In their 2023 study, Liu et al (Liu et al., 2023) introduced a blockchain-based system designed for the scheduling and management of marine transportation flow, a concept that aligns closely with the TradeLens project. To what extent did TradeLens deviate from established theoretical frameworks for blockchain implementation in maritime logistics? How did these deviations, if any, contribute to the platform's discontinuation?

Drawing from various scholarly articles, we acknowledge the robust technological foundation of this initiative. This insight prompts further contemplation on whether the limitations encountered were solely attributable to strategic flaws.

Despite its eventual discontinuation, the TradeLens project served as a significant case study in demonstrating the applicability and potential of blockchain technology within the shipping industry. Its journey has yielded critical insights and lessons, contributing substantially to the discourse on digitalization and the application of blockchain in maritime logistics. Furthermore, TradeLens exemplified that even with technological prowess and expertise, as evidenced by the involvement of a technological behemoth like IBM, success in technological innovation is not guaranteed. This underscores the multifaceted challenges that extend beyond mere technological advancement, which must be navigated in such large-scale implementations.

- **Lack of Industry Collaboration** *Despite the advanced technological infrastructure, the project encountered significant hurdles in fostering global collaboration, a critical element for the success of such a platform in the interconnected maritime industry. Notwithstanding the challenges in collaboration, the TradeLens platform demonstrated a notable level of industry engagement prior to its shutdown (Lorenz-Meyer and Santos, 2023).*
- **Lack of Sufficient Commercial Viability** *Despite its groundbreaking and innovative approach, ultimately did not achieve the level of commercial success required for its*

4.1. Bridging Blockchain's Promise and Maritime Realities: A Pragmatic Approach to Sectoral Adoption

continued operation as an independent entity. The TradeLens experience, therefore, contributes significantly to the discourse on the commercialization of innovative technologies, emphasizing the importance of developing business strategies that are as robust and forward-thinking as the technologies they aim to promote. (Shipping and Freight Resource, 2022)

- **Challenges in Data Governance and Privacy** *The blockchain architecture of the TradeLens project, while prioritizing information privacy, inadvertently led to a perception of opacity, particularly due to the centralized data governance model involving major industry players such as Maersk. This centralized approach, while aiming to secure data, paradoxically raised concerns among stakeholders, especially when considering the competitive dynamics within the shipping industry. The involvement of Maersk, a key competitor within this sector, in the governance of sensitive data, introduced an element of apprehension among other industry participants.*
- **Centralization Concerns** *the perceived excessive control exerted by IBM and Maersk. (PierNext, 2023)*
- **Technical Challenges** *The technological infrastructure of the TradeLens platform, while boasting high levels of security, came with a significant cost implication, resulting in elevated expenses for its customers. (Blockchaining.org, 2023; PierNext, 2023) Additionally, a discontinuation contributor would be the high costs associated with its development and maintenance. (Lyon, 2022)*
- **Limited Value Proposition for Information Providers** *The lack of sufficient incentive for key stakeholders, such as terminals and freight forwarders, to contribute their data. These entities perceived little to no benefit in sharing their valuable data with TradeLens*
- **Difficulty in Standardizing Blockchain Procedures** *Difficulty in standardizing blockchain procedures across a highly diverse industry characterized by siloed data and disparate systems. (Sharkey, 2022)*

4.1.2 key takeaways

These analyses underscore the complexity of integrating blockchain within an industry characterized by entrenched legacy systems and diverse stakeholder interests. The journey of blockchain from a theoretical solution to a practical tool in maritime logistics is fraught with hurdles, yet it is ripe with opportunities for enhancing efficiency, transparency, and security. Given the insights gleaned from the analysis of blockchain technology in the maritime sector, the following recommendations are proposed to guide future research and practical applications:

- Enhance Industry Collaboration

- Develop Standards and Best Practices
- Focus on specific pain points
- Pilot projects then turn into well-scaling proven solutions
- Invest in Knowledge
- Engage with regulatory bodies
- Leverage interdisciplinary research that combines expertise from computer science, maritime logistics, legal studies and economics
- Monitor emerging technological evolutions

4.2 A methodology reflexion

The complexity of blockchain technology, coupled with an unclear path to its practical maritime applications, has often stymied its broader acceptance. The lack of detailed knowledge about where and how blockchain can be applied within maritime logistics has contributed to hesitancy and skepticism, further exacerbated by the visible failures of numerous initiatives, leading to what can be described as a "cemetery of projects."

Consequently, we altered our approach. Transitioning from the specific examination of blockchain technology within the maritime sector to a more sectorial in-depth exploration, as we did in (Abdallah et al., 2023e). It embodies a comprehensive endeavor to dissect both the potential applications and the challenges hindering blockchain's widespread adoption. This shift in focus is driven by the realization of blockchain's vast potential juxtaposed with a notable gap in sector-specific understanding and application.

To address this knowledge gap and to demystify the complexities surrounding blockchain, we wanted to create an extensive body of work that not only highlights the technology's potential but also rigorously examines the challenges it faces. By doing so, it aims to provide a clearer picture of blockchain's applicability across various facets of the maritime sector, from documentation and compliance to supply chain transparency and beyond. Importantly, this analysis does not shy away from the difficulties encountered; instead, it seeks to identify and propose solutions to these challenges, offering a pragmatic path forward.

4.3 How can blockchain enhance the maritime industry's performance?

This section draws from our publications (Abdallah and Abdallah, 2022; Abdallah et al., 2023d) and (Abdallah et al., 2023e). A comprehensive review of blockchain technology in the maritime

4.3. How can blockchain enhance the maritime industry's performance?

sector will be beneficial to filling gaps in the existing literature. Through a systematic review, assessment, and examination of the potential of this technology in the sector, the next section will aim to establish a foundation that aligns the technological characteristics of blockchain with the industry's needs.

4.3.1 A global decentralized communication system

Viewing the Global Shipping Network (GSN) from a global perspective emphasizes unconventional results in the shipping map structure, which encourages to shift from traditional studies that define ports as nodes of the shipping network towards a more innovative approach where we consider shipping areas as nodes and connections between them as its edges.

Studies show that the influence of shipping areas on the GSN has a much higher impact than any single port (Li et al., 2014) which explains the technological research shift towards decentralized border-crossing digitized solutions such as Maritime MSW s and/or blockchain.

This paradigm shift underscores the imperative to shift from traditional maritime study frameworks, advocating for a comprehensive perspective that prioritizes the interconnectedness of extensive shipping regions. The prevailing hesitation among institutional frameworks to foster trust beyond their immediate national boundaries results in a segmented approach to global shipping logistics, presenting a notable impediment to adopting cohesive systems.

Blockchain technology, however, introduces a mechanism to establish trust without the prerequisite of trusted centralized authorities. It leverages a secure infrastructure predicated on sequential data chaining, encryption, and consensus protocols. This technological foundation also obviates the need for centralized databases and trusted intermediaries. It promotes decentralization that could be tailored to adhere to the specific requirements of the maritime environment. The application of blockchain within maritime logistics does not necessitate the indiscriminate disclosure of sensitive data across public networks; instead, it allows for a strategic selection among public, private, and consortium blockchains, each offering distinct characteristics suited to varying degrees of data accessibility and security (Dib et al., 2018; Dib and Toumi, 2020a). This nuanced approach enables the maritime sector to harness blockchain's capabilities while safeguarding sensitive information and aligning with the unique operational needs of global shipping logistics (refer to Table 2.1).

4.3.2 Increase operational efficiency

Despite the technological advancement and widespread use of PCSs and centralized data-driven tools to increase operational efficiency and manage logistics in the shipping industry, goods flow across the supply chain, global transparency and poor global data management remain (Czachorowski et al., 2019a).

Moreover, none of these parties have continuous real-time access to required information throughout the whole supply chain and the accountability level for inefficiencies and fraudulent

Chapter 4. An Analysis from a Maritime Perspective on Blockchain

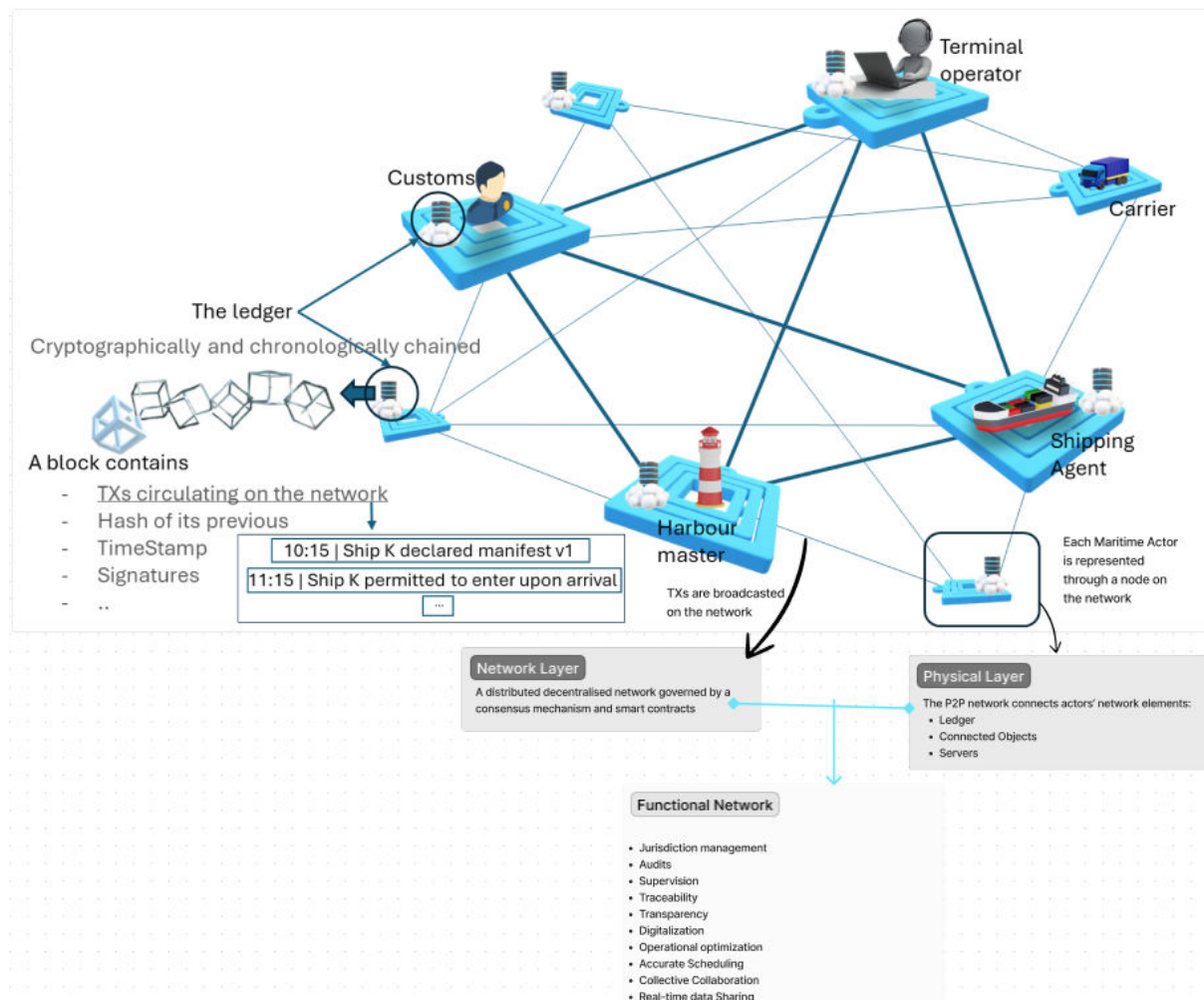


Figure 13: A Conceptual architecture for the maritime sector

activity is at its minimal (Botton, 2018). Incorporating blockchain technology into maritime operations presents a transformative opportunity to enhance efficiency and streamline processes across the board. The global dissemination of data facilitates unparalleled transparency and enables more effective traceability of cargo (Ganne, 2018).

By integrating data collection at every pertinent point, blockchain ensures that all relevant stakeholders have access to shared ledger information for review or verification. This not only bolsters transparency and traceability but also aligns with regulatory standards and safety requirements. Furthermore, the adoption of blockchain has the potential to significantly reduce transactional fees and other associated costs, such as those related to accounting and auditing, offering a more cost-effective solution for maritime logistics (Ganne, 2018).

A conceptual blockchain architecture including some maritime actors and exemplary transactions is illustrated in (Figure 13) below.

4.3. How can blockchain enhance the maritime industry's performance?

4.3.3 Reduced Data Storage

In the majority of steps across the supply chain data is not shared real-time amongst all relevant entities and data inflow can reach up to 35 zeta bytes per day (Mathews, 2017) (Czachorowski et al., 2019a).

Blockchain technology introduces a secure, decentralized platform that allows all relevant stakeholders to access real-time, authenticated information. This approach meets the widely recognized need for a secure, borderless system where data is instantaneously shared among all pertinent parties. Additionally, blockchain's use of hashing significantly reduces storage costs. By leveraging blockchain infrastructure, stakeholders can authenticate information directly, addressing current challenges such as the growing difficulty of verifying large data storage and eliminating single points of failure that can disrupt information flow.

4.3.4 Adjoint supplementary security privileges

With increased digitization rise a need for more cyber scrutiny to minimize risks. Nowadays not only ports and CS are concerned. Modern ships utilize onboard connected systems like Electronic Chart Display and Information System (ECDIS), digital navigation tools, and Automatic Identification System (AIS) for improved operational efficiency and communication. However, these systems are vulnerable to cyber-attacks, including hacking that can erase data and disrupt communications with signal jammers (DiRenzo et al., 2015).

Therefore, despite the advantages of increased digitization in the maritime sector, security attacks and accidental errors can have immense impacts on varying levels. For example, a ransomware attack on one of the largest shipping companies "Maersk" resulted in an estimated loss of 250 million dollars with an impact that reverberated to around 70 terminals globally (Mathews, 2017).

Blockchain mitigates cybersecurity risks associated with centralized systems by preventing data alteration with its encrypted, chronologically chained ledger, eliminating single points of failure. Decentralized systems, as such, offer enhanced security compared to centralized models (Di Gregorio et al., 2017). When integrated with connected devices, blockchain enables scalable infrastructure where data origin can be traced, and fraudulent devices are readily identified thanks to the ledger's immutability. This allows for direct device interaction and automation without centralized servers (Reyna et al., 2018).

4.3.5 Prevent and decrease pollutions

The shipping industry, while being one of the more energy-efficient methods of transporting large cargoes, significantly contributes to atmospheric pollution through the emission of NO_x, SO_x, carbon dioxide, and particulate matter. Notably absent from the 2015 Paris global climate change agreement (unfccc, 2015), the sector has seen the IMO intensify efforts to curb its

Chapter 4. An Analysis from a Maritime Perspective on Blockchain

environmental impact.

Since 1980, with a pronounced focus post-2013, the IMO has enacted stricter regulations, notably reducing the allowable sulfur content in ship fuel from 3.5% to 0.5% in 2020.

This shift mandates the adoption of low-sulfur fuels or the installation of scrubbers on ships. These regulatory measures amongst others are anticipated to prevent approximately half a million premature deaths within five years (Reuters, 2019) (Sofiev et al., 2018).

However, the enforcement of these rules presents a substantial challenge, with voluntary non-compliance rates in fuel consumption estimated between 10% to 30% in 2018 (Grimmer, 2018), underscoring the need for more effective monitoring and enforcement mechanisms in the maritime sector.

The maritime sector currently lacks extensive technological literature addressing pollution prevention.

A notable study in this realm explored the potential of blockchain to mitigate pollution within the maritime industry, examining the shipping sector's openness to adopting such technologies for environmental conservation. The study identified a clear link between the hesitancy towards innovation and the perceived increase in operational costs; for modern technology adoption to be viable, it must demonstrably reduce overall expenses (Czachorowski et al., 2019a).

Despite this gap in maritime-specific research, blockchain's efficacy in pollution control has been substantiated in other domains. Notably, the integration of IoT and smart sensors with blockchain and smart contracts has been employed to monitor air pollution in China, offering real-time data collection and facilitating governmental auditing processes (Dai et al., 2019). Beyond air quality management, blockchain applications have been extended to tracking various pollutants, as evidenced by the 2017 launch of Open Litter Map. This platform incentivizes users worldwide to report pollution through geospatial data, rewarding contributions with Littercoin cryptocurrency. However, the longevity of such innovative initiatives hinges on substantial global support (Lynch, 2018).

Further studies have demonstrated the feasibility of leveraging IoT and blockchain synergistically to trace water pollution sources in real-time (de Tazoult et al., 2019). Another investigation proposed a blockchain-based prototype for global, immutable air quality monitoring. This system utilized the Ethereum blockchain in conjunction with the Interplanetary File System (IPFS) and uPort for cost-effective data storage and identity management. The approach significantly reduced blockchain data storage costs (de Tazoult et al., 2019). In blockchain data storage volume is directly proportional to the cost. It made the solution economically viable, yet highlighted the need for improvements in data pre-validation and user verification.

Data storage cost The following is a simplified proportionality and doesn't account for the base transaction cost (used for a basic transfer) or potential variations in gas usage due to specific data storage operations.

4.3. How can blockchain enhance the maritime industry's performance?

$$\text{EstimatedTransactionCost}(TxCost) \propto \text{DataVolume}(DV) * \text{GasPrice}(GP)$$

- TxCost: This represents the estimated transaction cost in the same unit as the gas price (usually Gwei for Ethereum)(Marchesi et al., 2020). Gas represents the fee paid by miners (the computational effort required for processing actions on the network. The more complex the transaction the more gas it utilises (Marchesi et al., 2020).
- DV: This represents the data volume of your transaction in bytes.
- GP: This represents the current gas price on the Ethereum network in Gwei.
- (proportional to): signifies that the transaction cost is directly proportional to the data volume and the gas price

These explorations across various sectors underscore blockchain's potential in environmental monitoring and pollution prevention. They suggest a promising direction for the maritime industry to overcome innovation barriers and operational cost concerns, advocating for a more sustainable and technologically advanced approach to environmental protection.

4.3.6 Fight Fraud and prevent corruption

The exploration of secured, distributed systems offering real-time transparency and traceability paves the way for considering blockchain and smart contracts as viable tools against corruption and fraud. Evidence from various sectors supports the efficacy of such systems in enhancing real-time traceability, reducing costs, and upholding privacy and security (Sarda et al., 2018; Cai and Zhu, 2016; Kshetri and Voas, 2018; de Souza et al., 2018a).

Technological advancements have historically been leveraged to combat corruption, with numerous studies demonstrating how IT progress can curtail corrupt practices (Arayankalam et al., 2021; Lio et al., 2011; Srivastava et al., 2016). Blockchain technology, in particular, offers a robust framework for preventing fraud, streamlining transaction authentication, and validation processes. Its tamper-proof, encrypted ledger enhances the detection of malicious activities, while smart contracts automate processes, reducing human error or deliberate tampering (Santiso, 2018).

In the maritime sector, characterized by its extensive scope, complex operations, and numerous stakeholders, fraud and corruption are significant challenges, potentially inflating shipping costs by at least 10% (Di Gregorio et al., 2017). The transition from intra-organization digital systems in the 1980s to the more recent adoption of "e-government" initiatives illustrates the sector's ongoing efforts to harness technology in fighting corruption. However, these digitization efforts are often hindered by their fragmented nature and reliance on centralized systems, which

Chapter 4. An Analysis from a Maritime Perspective on Blockchain

pose risks of data breaches and cyber-attacks, ultimately facilitating fraudulent activities due to minimal transparency.

Blockchain technology proposes a comprehensive approach to unifying the digitization process within the maritime industry. Its decentralized structure enhances visibility across supply chains, promoting information sharing and reducing ambiguities in transaction validation and authentication. The immutable nature of the blockchain ledger aids in verifying transactions and identifying fraudulent patterns, while permissioned blockchains offer a balance between regulatory enforcement and the benefits of decentralization.

Yet, it's crucial to acknowledge that blockchain is not a cure-all for fraudulent issues in the maritime sector. Given the variety of fraudulent activities, expecting any single technological solution to eliminate corruption entirely is unrealistic. Instead, blockchain should be viewed as a powerful tool that, when integrated with other measures, can significantly mitigate fraud and enhance the integrity of maritime operations.

4.3.7 Eliminate unnecessary intermediaries

The Blockchain structure being a shared secure hard to alter ledger made data available to relevant parties through any device without the need for additional notaries(Finextra, 2016).

4.3.8 An Extended Spectrum of Use Cases

A crucial step in the application of blockchain in the maritime sector is the identification of the full spectrum of use cases throughout the sector. the following section aims to broaden the spectrum of potential applications and use cases for blockchain beyond the aforementioned.

Adapting proven use cases from outside the maritime sector The most straightforward approach to successful implementation involves Leveraging Established Use Cases (LEUC) from other sectors, where no entirely new functionalities are proposed. Existing successful applications from other industries can be streamlined for the shipping sector through blockchain (as shown in Table 4.1).

4.3. How can blockchain enhance the maritime industry's performance?

LEUC Domain	Brief Elaboration on beneficial aspects for the maritime sector
Security	(DiRenzo et al., 2015): Connected systems in the maritime sector can be hacked and (Mathews, 2017): Security attacks have immense consequences. Distributed approaches are more secure than centralized ones (Di Gregorio et al., 2017), hence blockchain can be deployed for adjoined security features for existing systems such as connected devices (Reyna et al., 2018)
Environmental sobriety	(unfccc, 2015; Gold, 1999a): Disastrous incidents in the maritime sector have led to stern rules. (Reuters, 2019), (Sofiev et al., 2018): Rules and standards that are enforced can be largely preventive and beneficial. (Grimmer, 2018): Currently, the enforcement of these rules remains far from an optimum where volitional infringements in 2018 are up to 30%.
Counterfeit and malicious activity	(Sarda et al., 2018) , (Cai and Zhu, 2016) (Kshetri and Voas, 2018; de Souza et al., 2018b) (Dahiya et al., 2017) , (Narayanan et al., 2016) (Sun Yin et al., 2019a), (Chanson et al., 2019) (Pu and Lam, 2021), (Jensen et al., 2019) (Sullivan and Burger, 2017a), (Köhler and Pizzol, 2020) and (Ziolkowski et al., 2020) demonstrate in literature the use of blockchain for fraud prevention and detection. The maritime sector has active concerns where counterfeit and malicious activities raise costs by at least 10% (Di Gregorio et al., 2017) and can immensely benefit from the use of technology having anti-fraud characteristics.
Reducing delays and unnecessary third parties	We reflect on the several potentials to highlight the consequent improvement in operational efficiency that aligns with our hypothesis. The prevention and easy identification of malicious activities, the simplified regulatory enforcement, and the adjoined security privileges combined with incremented transparency and traceability and the elimination of unnecessary third parties would unlock colossal benefits for the maritime sector.

Table 4.1: Extending blockchain's spectrum of domain applications.

For the technology to reach its full capabilities and revolutionize the maritime sector, it needs not only to be applied in heterogeneous use cases but also be deployed with a sense of homogeneity. These different applications should be able to interoperate to facilitate secured widespread digitization that propagates through the whole supply chain.

To elaborate on LEUC, consider the enforced shipping standards established by the International Safety Management (ISM) code and International Organization for Standards (ISO). As (Abdallah and Abdallah, 2022) suggests, regulatory quality and safety standards in shipping are likely to become stricter. This will lead to more intricate operational processes.

LEUC highlights the suitability of blockchain for simplifying documentation and ensuring safe conditions throughout the supply chain. A prime example is the transportation of vaccines. Initially, during the pandemic, air freight ensured faster delivery. However, with decreasing virulence, cost-effective options like maritime shipping become viable (<https://dfreight.org/>, 2022).

Here, efficiency remains crucial. Vaccines are susceptible to degradation under fluctuating temperatures according to the World Health Organization. LEUC proposes the use of blockchain-monitored containers with passive cooling systems. Real-time temperature recording allows for immediate intervention, minimizing degradation. Smart containers with sensors, already used in air transport (Hampstead, 2018), demonstrate the feasibility and success of LEUC. Documents

can be digitized, certified, and verified using blockchain.

Incremental innovations Furthermore, this approach can be used as a foundation for further experimentation. For instance, the Internet of Things (IoT) can be integrated for complete traceability. While currently used for real-time tracking, IoT devices alone are vulnerable to security threats. Blockchain's secure ledger system can monitor both goods and devices, facilitating the detection of malfunctioning or compromised elements.

Since the technology is still new to this sector, with limited successful applications, we must be aware of possible technological limitations and how to address them.

4.4 Blockchain Challenges

The full potential of a decentralized technology such as the blockchain cannot be exploited without efforts being made in the ecosystem to ensure total coordination and widespread adoption. Therefore, we re-address some of the challenges in (Abdallah et al., 2023d), and bring forth additional challenges with a deeper analysis using a triangulation approach (Pansiri, 2005) to confirm hypothetical challenges and probe for solutions and analyze them.

4.4.1 Blockchain's limited use outside of the private sector

Despite the large variety of pilot projects and described applications in literature, there have not been any tangible blockchain applications in the public sector (Tan, 2023; Reddick et al., 2019) (cf. table 3.1). Entities of the public sector recognize the massive potential of blockchain but are deterred from participating in this phase where there are still ambiguities and complexities tied to this technology that are yet to be solved. Therefore, this challenge can be linked with other challenges that are developed below such as security threats, network limitations, lack of regulations, and unwanted scrutiny (Abdallah et al., 2023d).

4.4.2 Blockchain predates regulations

Emerging technologies like blockchain introduce regulatory uncertainty, hindering industry adoption (Kapidani et al., 2021). The maritime sector, already grappling with complex regulations, presents a unique challenge. While the International Maritime Organization (IMO) establishes international shipping regulations (Reynolds, 2000), local and sectoral regulations further complicate the landscape. PCSs enforce regulations locally, but lack communication and global harmonization.

Blockchain aligns with the need for transparency and traceability in the maritime industry. It can function as a decentralized infrastructure for existing PCSs, fostering efficiency and communication. However, the lack of global regulations for blockchain and cryptocurrencies poses a challenge. While some governments are taking action (e.g., El Salvador adopting Bitcoin

as legal tender, The EU has also launched a crypto regulatory project, leaked to the press last September, to harmonize regulations and avoid competition across its states), others are implementing restrictive measures (e.g., China's mining ban). This inconsistency discourages adoption. And any amended regulations such as the forth anti money-laundering directive considered only exchanges between crypto and fiat currencies (Miseviciute, 2018).

Additionally, even without cryptocurrency concerns, blockchain applications must comply with data protection regulations like the EU's GDPR. The immutability of blockchain clashes with GDPR's right to rectification and erasure. Proposed solutions include a central authority for data management, distributed responsibility among multiple authorities, or pseudonymization through encryption as seen in (Rieger et al., 2019). Addressing these challenges and establishing clear regulations will incentivize industry adoption, particularly in the risk-averse shipping sector.

4.4.3 Scrutiny: The Result of Transparency

While blockchain offers demonstrably improved supply chain transparency through data sharing, origin tracking, and reduced ambiguity, this very feature presents a potential barrier to adoption. Increased visibility might disincentivize participation, particularly from shipping and global businesses wary of exposing information (Vivaldini and de Sousa, 2021).

A solution Axis Different blockchain architectures, such as public and private networks, could address these concerns by offering varying levels of transparency. However, this necessitates a critical choice between public blockchains' inherent openness and private blockchains' controlled access. Furthermore, ensuring interoperability between these disparate systems introduces unwanted technological complexities that must be carefully considered (Al-Rakhmi and Al-Mashari, 2022).

4.4.4 Security Challenges

While blockchain boasts an append-only ledger for immutability, security concerns remain. Pre-appended data integrity and 51% attack vulnerability challenge the theoretical immutability of public blockchains like Bitcoin (Reyna et al., 2018; Eyal and Sirer, 2018). Additionally, public blockchains are susceptible to forks, DoS, eclipse attacks, man in the middle, and potential future threats from quantum computing (Conti et al., 2018). Cryptocurrency hacks highlight further vulnerabilities in applications, protocols, and smart contracts (Orcutt, 2019).

These vulnerabilities necessitate a focus on security throughout the lifecycle of any blockchain application in the maritime sector. Permissioned blockchains, with controlled access and reduced attack surface, offer a potential solution (Beck et al., 2018). They incentivize information sharing within a trusted ecosystem, mitigating concerns around data privacy in the public domain.

This pragmatic approach leverages blockchain's strengths while acknowledging limitations, fostering a collaborative path for integrating the technology with existing secure systems in the maritime sector.

4.4.5 Network and Technical Challenges

The previously mentioned challenges are common to the global adoption of new technological advancement, and often after detecting them adopters will deploy solutions to overcome and flatten the fear of the adoption curve over time resulting in widespread adoption (Rogers et al., 2014). However, this cannot be said about network or technical challenges. They are more omnipresent.

4.4.5.1 Distinct technical capabilities

Current limitations hinder large-scale blockchain adoption in the maritime sector. Firstly, the technology necessitates a skilled workforce for deployment and maintenance, posing a challenge for enterprises with limited technical expertise (Botton, 2018). Secondly, the decentralized nature of blockchain requires a critical mass of participants, which can be difficult and expensive to achieve due to varying technical capabilities and upfront investment costs (Botton, 2018). This is particularly problematic when integrating participants with limited technical literacy, such as farmers in a fruit traceability system.

4.4.6 Data and Storage

4.4.6.1 Data immutability

The immutability of blockchain data amplifies the impact of human error, as demonstrated by the Ethereum DAO hack. These limitations, coupled with the potential for misuse as evidenced by illicit activities, contribute to a cautious approach towards widespread adoption (Kivo, 2018).

4.4.6.2 Data Frequency

Blockchain's inherent immutability creates challenges for storing vast amounts of data frequently generated in maritime applications, particularly when integrated with maritime technological advancements like IoT. Data frequency issues have been addressed through literature using multiple approaches that have been thoroughly explained in our publication (Abdallah et al., 2023e).

Data sharding One approach relies on limiting data redundancy through distributed storage. When a block is created, it is fractioned and then fed into a coding algorithm that will further divide these fractions of a block into sub-fractions to be distributed and stored on the network.

However, this approach might be susceptible to information inconsistency and limits our system's efficiency (Dai et al., 2018).

A compromise between simplified payment verification (SPV) and full-node pruning This can be achieved either by deleting expired transactions and keeping only block headers (Palai et al., 2018) or by introducing the idea of block summary (Gao et al., 2020). However, both these methods are targeted only to case-specific uses such as financial transactions or land agreements, and cannot be used in cases where data is sensitive to deletion such as identity management or the maritime sector.

Off-chain storage via IPFS transactions are stored in Interplanetary File System (IPFS) and the resulting hash is then stored in the block and used in the Merkle root and the block's resulting hash (Zheng et al., 2018a). (Nizamuddin et al., 2019) detailed the use of the smart contract feature of blockchain, specifically Ethereum, on top of the IPFS network. However, some problems remained: duplication, content piracy, and information availability.

Improved Off-chain storage via IPFS As duplication prevention, multiple approaches were suggested in the literature, such as SPROV (Hasan et al., 2009) which uses encryption and signatures to protect authenticity. However, this method lacks data querying, which is important, specifically in the maritime sector where data is abundant.

Improved Off-chain storage via IPFS Nonetheless, data integrity remained threatened, since all the aforementioned approaches were vulnerable to piracy. One approach to mitigate piracy risks within IPFS utilizes intermediary applications positioned between users, the IPFS network, and the blockchain. These applications act as a protection layer, encrypting files and managing access control through smart contracts (Khatal et al., 2021). While this approach offers improved security, it introduces additional complexity and potential points of failure within the system. Further research is needed to evaluate the trade-offs between enhanced security and potential drawbacks associated with intermediary applications. And these methods discard data availability problems that come with IPFS systems.

Incentivised off-chain storage via IPFS The filecoin blockchain provides an incentive layer on top of the IPFS network to guarantee data availability (Benet, 2017).

Erasure coding off-chain storage via IPFS Sia (Vorick and Champine, 2014) and Storj (Wilkinson et al., 2014), suggests the use of erasure coding (Balaji et al., 2018) to ensure data availability.

Storage type segregation via IPFS for optimized throughput A study proposes categorizing data as either "hot" for frequently used data or "cold" for far less frequently accessed data. Since the hot data has a higher availability need, it is stored and replicated multiple times through the network as opposed to using an erasure scheme for the storage of cold data. (Chen et al., 2017a)

Cloud Off-chain storage Other approaches suggested coupling cloud storage with blockchain, implementing real-time hooks for provenance events to be recorded into the ProvChain (Liang et al., 2017).

Blockchain-based storage type segregation data can be accessed in both modes (off-chain/on-chain) via two distinct types of transactions: point and data. This particular methodology allows a maximum set of participants to record data through a single compression operation lessening expense. Through internal participants, transactions of a "point" nature are made at each step. Once data reaches the terminal and is compressed, a transaction "data" is made to the ledger. This mechanism addresses the efficiency barrier of recording large bulks of data on the blockchain. Second, data can also be encrypted and only available to authorized parties addressing the privacy issue of blockchain. (Shamir, 1979).

Data Offloading unrelated block offloading filters can be used to store cold data in off-chain caches (Liu et al., 2019). Additionally, other studies that suggest improvements such as:

- A credit-based proof of work with a directed acyclic block architecture (Huang et al., 2019);
- A light chain concept with a more environmentally aware consensus mechanism (Liu et al., 2019);
- A new multi-center architecture to enhance privacy and security (Wan et al., 2019b);
- Recycling an already-deployed smart contract for space reduction (Pontiveros et al., 2018) that aligns perfectly with the compressed and private data-sharing concept and can be introduced as improvements.

4.4.7 The Nexus between Code and Logic in Business

Despite the growing interest in blockchain's potential to transform the maritime sector, a critical gap exists between technical capabilities and industry knowledge. Enterprises, even those with coding expertise, often lack domain-specific blockchain knowledge, hindering their ability to define clear expectations for blockchain applications. Furthermore, the allure of blockchain's success stories can lead to hasty adoption without a thorough analysis of its suitability for the specific problem at hand. Effective technology adoption requires not just identifying a solution,

but ensuring it is the optimal solution for the identified business challenge. This highlights the need for a deeper understanding of both blockchain technology and maritime sector logistics to ensure successful and targeted deployments : A motivation behind this in-depth research.

4.4.8 Smart Contracts

Despite the smart contract's revolutionary aspects, it also has several limitations. For one thing, the execution of a smart contract for financial purposes relies on the existence of the required funding on the blockchain. This means that any transaction involving cryptos is only executed if the crypto is native to the blockchain and the amount exists on the blockchain. Therefore, transactions cannot be enforced in the absence of these two conditions.

A third regulatory party can act as an enforcement authority, but this negates the decentralized authority concept of blockchain. Alas, stakeholders are susceptible to not being paid. For another example, most used types of transactions in the maritime sector are based on fiat currencies that blockchain cannot enforce, but only record. This means that blockchain applications in the maritime sector cannot guarantee crypto payments and cannot enforce fiat-based payments.

Furthermore, the inherent complexity of smart contracts necessitates a clear understanding of the technology's capabilities. (antonylewis2015, 2017) emphasizes the disconnect between code and real-world business logic, where a lack of clarity can lead to unrealistic expectations and wasted resources on unachievable goals.

4.4.9 Oracles

Smart contracts rely on real-world data, but blockchains themselves cannot access this information directly. Centralized oracles introduce a single point of failure and compromise the decentralized nature of blockchains. Non-deterministic data from oracles (data that can change) reintroduces trust issues (Egberts, 2017).

When choosing to work with external data sources, the chosen trust model can considerably impact the environment's nature. This is why when working with blockchain an optimum oracle model should also be trusted and/or decentralised such as Chainlink, Astrapia (Adler et al., 2018), Dia (Network, 2021), and Band protocol (Pasdar et al., 2023)

4.4.10 Interoperability

While various promising blockchain projects have emerged in the maritime sector, a significant hurdle exists their lack of interoperability. Blockchains operate on different technical frameworks, hindering communication and asset transfer across these independent systems. This fragmentation impedes the full potential of blockchain for revolutionizing maritime operations. Fortunately, solutions are on the horizon. Projects like Cosmos (Kwon and Buchman, 2019) aims to bridge the communication gap between blockchains. Upcoming IMO regulations man-

dating data exchange favor a unified approach notably with the ongoing SW efforts. Hence, alignment with global efforts by UN/CEFACT and regional regulations is crucial for successful implementation. Thus, for blockchain technology to reach its full potential within the maritime industry, interoperability solutions are paramount.

4.4.11 Common Code Sense

Smart contracts, being code-based, are inherently susceptible to vulnerabilities. These vulnerabilities can have significant consequences in the context of immutable, automated transactions. Careful validation and testing are crucial prior to deployment, as evidenced by the infamous \$50 million DAO hack that exploited a code weakness ([1]). This event, which led to a hard fork in Ethereum, underscores the importance of smart contract security assessments (Finley, 2016).

The potential for significant financial gain incentivizes attackers to exploit vulnerabilities, particularly as the number of deployed smart contracts continues to grow. Research efforts have intensified in recent years, focusing on two primary areas: ensuring correct coding practices to prevent bugs, and developing tools for vulnerability detection (etherpot, 2024; He et al., 2019).

On the prevention side, studies like (He et al., 2019) highlight common coding mistakes in smart contracts and propose best practices to mitigate them. The seemingly simple case of a "rock, paper, scissors" smart contract demonstrates the inherent complexity of this technology, as illustrated by the Etherpot lottery application's vulnerabilities (etherpot, 2024).

Despite skilled programmers, undetected bugs remain a concern. Consequently, research has also yielded advancements in automated bug-detection tools, as we further detailed in (Abdallah et al., 2023d).

4.4.12 Unquantifiable Clauses

Formal Specifications and Automated Detection : Beyond technical coding errors, smart contracts often contain unquantifiable clauses that are difficult to translate into machine-executable code. Recent research proposes a promising approach to address this challenge: formal specifications and automated detection tools.

This approach leverages the existence of commonalities across diverse smart contracts. By formally specifying a smart contract's intended behavior, the groundwork is laid for the creation of cross-platform detection tools. Traditional smart contracts lack these formal specifications, hindering automated verification.

The study (Bernardi et al., 2020) proposes a two-step approach:

- **Reusable Invariant Collection:** Collaboration with the developer community facilitates the identification and formalization of reusable invariants – properties that consistently hold true throughout a program's execution. These invariants serve as the foundation for cross-platform detection tools.

- Automated Bug Detection: Tools like Certora (Certora, 2024) integrate with existing smart contract compilers to leverage the collected invariants for automated bug detection.

This research suggests that formal specifications, coupled with automation, have the potential to surpass the limitations of manual code audits.

4.5 Discussion

The exploration of blockchain technology within the maritime sector has unveiled a spectrum of opportunities and challenges, coinciding with a nascent yet transformative phase in the industry's technological evolution.

The maritime sector has taken into consideration studies' results highlighting the impact of unhindered digitized collaboration over the global operational efficiency, security, and durability (Bank, 2020). Considerable actions have been set in motion, such as the European maritime Maritime MSW . This aims to introduce standardization for port calls. It ensures a formality in data exchanges for each national maritime Maritime MSW for better coordination and operations facility. The regulation declared to be effective starting August 2025, imposes (among other requirements) nationwide data centralization, extended standardization, and continent-wide (European) data harmonization. Before the due date, prominent efforts will be made by the European Commission Services, the member states, the national Maritime MSW s, and port operators to assure an interoperable architecture.

The global operational management in the supply chain is onerous and time-consuming, propagating among a tension-aggravated global web of port-based clustered actors. The tension can be directly linked to the lack of transparency generating skepticism and consequently processing redundancy (Nathani and Singh, 2020). Faced with such problems, and to keep pace with the technological advancements that revolutionized other sectors, IS in the sector are looking to increase collaborative efforts not only to adhere to IMO SW regulations but also to stay afoot competitively. Big companies in the shipping sector started experiencing novel technologies that averted from centralized to the novel peer-to-peer network approach.

Apart from the nomenclature analogy between blockchain and supply chain, the technology has interesting similarities between its technical and technological concepts and those targeted by the maritime ecosystem for faster and leaner logistics in global trade that the SW aims to achieve.

This chapter has navigated through the theoretical underpinnings, and practical applications, and encountered hurdles, laying a foundation for a scholarly discourse that corroborates the analogy from a technological point of and sets the foundation for our upcoming work to successfully implement this sector-novel technology.

Blockchain technology, with its inherent qualities of decentralization, transparency, and security, aligns with the maritime sector objectives. However, the journey from theoretical exploration

Chapter 4. An Analysis from a Maritime Perspective on Blockchain

to practical implementation is fraught with challenges that demand a nuanced understanding and strategic approach. The discourse herein underscores the imperative for a balanced evaluation of blockchain's capabilities against the sector's idiosyncratic demands, advocating for a paradigm shift in how data and transactions are managed across the global maritime landscape.

Therefore, this chapter takes as its fulcrum that indeed blockchain technology proffers characteristics that conform with desirable operational aspects for the sector. It sets a theoretical conceptual hypothesis for a re-imagined maritime blockchain-based ecosystem. Similarly, (Sunny et al., 2020) agree that blockchain can act as the brain of the supply-chain body. It can simplify the real-time operation handling that might involve no less than hundreds of transactions (Tsiulin et al., 2020) through a series of decisions and exchanges among various entities.

However, despite its theoretical alignment, hesitancy still reigns over the technology, and actors remain reluctant to allocate needed resources to the technology and allow it to fully demonstrate what it has to offer. It necessitates a collaborative effort among industry stakeholders, technology providers, academics and regulatory bodies to harness its full potential while mitigating inherent risks and barriers to adoption.

The literature argues that the inhibiting factor is the presence of a gap between blockchain and the existing approaches and that this gap can be reduced by adopting the unified theory of technology acceptance, and using it to converge towards widespread use.

We agree that there is a gap between the conventional approaches of the maritime domain and the innovative revolutionary methods proposed and endorsed by the use of blockchain. It falls back to the deep-rooted conventional PCS approach spread across the globe.

However, we do not argue for the efficiency of the current approaches but identify possible weaknesses that the sector has also detected, and aim to propose a possible improvement aligning with the sector's effort through blockchain. Therefore, before starting our research rationale, we anchored the defined technical aspects of blockchain in Chapter 2, studied desired outcomes, industry specifics and maritime technological trends in Chapter 3 and assimilated them in this chapter laying solid foundational prospects of our employed future implementation within the sector. This can finally achieve the wanted shift of a re-imagined ecosystem from theory to demonstration.

We also argue that the gap that has deemed blockchain unattainable for the sector is not due to a lack of technological capabilities, but to willingness that portrayed the sector as prudent and conventional. This willingness can be intensified through this extensive analysis of the technology from a sectorial point of view. We also used a triangulation approach to demonstrate the liaison between literature and tangible projects and applications.

Notwithstanding the technology's full spectrum of capabilities, we differentiate between the existing types of blockchain (Dib et al., 2018). We argue in the next chapter about the compatibility of one type of blockchain technology with the range of needs present throughout the whole supply chain. This aligns better with the data-access policies and competitiveness that characterize the heterogenous maritime ecosystem.

As for blockchain interoperability, the advancements on the subject have been well highlighted by (Belchior et al., 2021), revealing a broader context of interoperability than a cross-chain asset and crypto exchanges.

The technology faces the same challenge that the maritime sector is currently addressing: heterogeneity. The maritime sector is characterized by its distinct actors, where both private and public actors collaborate. Thus, technological adoption should be homogenous for it to succeed. Currently, despite considerable standardization efforts for both data (such as bills of lading and manifests), and regulations, systems remain fragmented with no viable noticeable blockchain application in the maritime public sector. Moreover, regulations should not only address the ecosystem but also the technology itself. Being novel, there are still controversies concerning blockchain and smart contracts to be addressed by the law for lucid accountability. Additionally, before blockchain deployment, there is a need to clearly define transparency aspects to be agreed upon by the network's actors, and to determine the types of networks needed for each operational feature. Furthermore, despite the secure reputation of the technology, any deployment should also be addressed with a clear sense of security given the sector's nature.

The main aim behind our analysis and challenges assessment was to point out that, in addition to benefits, researchers are aware of the shortcomings of the technology and can provide discernible in-depth discussions to avoid any substandard implementation. These challenges are well addressed, as proven through a triangulation approach. We bring forward, as an example, the storage challenge, where we successfully identified a series of literary and applicative projects to answer each situation's need. At the end, the deployment of blockchain with the innovatory sequel combination of these several approaches resolves the challenge. This proves that, regardless of the challenge, with enough resources and willingness a solution can be found.

Considering the potential benefits of blockchain technology, its integration with the maritime Maritime MSW framework deserves further exploration. We investigate next how existing IS like PCS can leverage blockchain for enhanced traceability and security. Consequently, it should also be viable for any cascading evolution for the maritime IS such as SW.

IMPLEMENTING BLOCKCHAIN FOR THE MARITIME: PRELIMINARY WORK

Contents

5.1 PoC Specifications	90
5.2 Theoretical and Empirical Foundations	90
5.2.1 The Diffusion of Innovations Theories (Doi)	91
5.2.2 The Port: A key link for technological advancement	91
5.3 Implementation Approach	96
5.3.1 Technology Stack	96
5.3.2 Design principles	99
5.3.3 A Solution Strategy: Blockchain-based BAT access	101
5.3.4 Simulative Environment and Role of HAROPA PORT in the PoC	105
5.4 Towards implementation	106

Abdallah, R., Bertelle, C., Besancenot, J., Duvallet, C. and Gilletta, F., 2023, July. Repositioning Blockchain Technology in the Maritime Industry for Increased Accountability. In International Congress on Blockchain and Applications (pp. 82-92). Cham: Springer Nature Switzerland, (Abdallah et al., 2023a)

In the preceding chapter, our exploration spanned the maritime sector in its entirety, setting the stage for a targeted approach based on our findings. We addressed the initial two research questions, delving into the myriad challenges and opportunities blockchain presents for this industry. This investigation unveiled a sector poised for significant transformation, underscored by a pressing need for increased transparency, accountability, and security.

However, questions regarding the "feasibility" and "adoption" of blockchain technology remain. Despite our comprehensive analysis laying the groundwork for a more focused strategy, certain aspects remained unclear. To address this and achieve the desired level of traceability within smart ports, it became evident that implementation preliminary groundwork was essential. This chapter will draw from our paper covering published work (Abdallah et al., 2023a).

We aim to clearly define our objectives and then methodically outline our approach to achieving them. Our contribution is twofold. First, we identify the port as a strategic entry point for introducing blockchain technology, recognizing its pivotal role in the maritime ecosystem and its capacity to act as a catalyst for broader sectoral transformation. This choice is informed by a rigorous review of the literature, where we identify a critical gap: the lack of comprehensive solutions that leverage the port's central role in promoting technological adoption. Second, we target a specific use case - dangerous goods traceability - to demonstrate the practical application of our conceptual framework. This targeted approach not only addresses a pressing industry challenge but also provides a scalable model for broader application across the maritime sector.

5.1 PoC Specifications

Our PoC will demonstrate the application of blockchain technology to enhance transparency and traceability across the maritime ecosystem, with an emphasis on the traceability of dangerous goods. This PoC will incorporate blockchain's core capabilities alongside the strategies identified in the previous chapters, specifically focusing on:

- **Traceability of Data:** Ensuring the seamless traceability of data related to the handling and transportation of dangerous goods within the maritime ecosystem.
- **Ease of Adoption and Integration:** Designing the blockchain solution for straightforward adoption and integration with existing maritime operational systems, minimizing disruption and facilitating widespread acceptance.
- **Consideration of Competitiveness:** Keeping in mind the competitive landscape of the maritime industry, our PoC will demonstrate how blockchain can not only enhance operational efficiencies but also potentially confer a competitive edge to adopters, particularly in terms of operational efficiency, risk mitigation, and regulatory compliance.

We'll address feasibility, adoption, and create a tangible roadmap for blockchain in maritime.

5.2 Theoretical and Empirical Foundations

The maritime industry is often characterized by its technological caution and adherence to tradition (Acciaro et al., 2018; Stopford, 2008), a theme echoed in various scholarly works and industry analyses (Rodrigue, 2010; Stopford, 2008). Innovation has been constrained by a narrow focus on localized impacts, neglecting broader implications for the interconnected ecosystem (Acciaro et al., 2018; Arduino et al., 2013). This limited perspective undermines sector-wide innovation potential and highlights an alignment gap.

In light of these challenges, a tailored strategy is required - one that respects the sector's traditions while bridging between blockchain's innovation potential and its practical, widespread

application. This strategy should facilitate technological diffusion to surpass localized impacts and have a broader transformative effect across the maritime industry.

5.2.1 The Diffusion of Innovations Theories (Doi)

To formulate a strategy, we turned to the wealth of existing literature for a grounded technological diffusion approach. We draw upon the Doi (Sahin, 2006), the Technology Adoption Model (TAM) (Sahin, 2006) and insights from mandatory adoption scenarios (Asare et al., 2016) to study technological innovation adoption in the maritime sector.

Find a technological diffusion entry point The Technology Adoption in Supply Chains (TASC) model provides a robust framework capturing organizational, external, and relational variables critical for adoption within inter-firm networks. This research synthesizes theoretical paradigms to inform viable blockchain entry points in the domain.

The decision paradigm TradeLens' head Marvin Erdly highlighted the network's indispensability: "*we do need to get the other carriers in the platform. Without that network, we don't have a product*". This echoes the TASC's 'Decision' phase significance, where adoption either succeeds or fails. A theoretically sound yet pragmatic research approach aligning theory and practice is needed to gain insights into technology adoption.

Research hypothesis Our hypothesis posits that by pinpointing the port as a critical juncture and effectively integrating blockchain with its Information Systems (IS), we can facilitate a seamless diffusion of this technology among various maritime stakeholders. This strategic approach is expected to simplify and reduce the intricacies typically associated with the decision-making phase. We will investigate this hypothesis in the subsequent section.

5.2.2 The Port: A key link for technological advancement

Synthesizing earlier insights on technological foresight with a comprehensive understanding of port infrastructure and operations reveals a symbiotic relationship. This relationship underscores how technological advancements transform ports' evolving role within the maritime industry. Understanding a location's strategic value (location intelligence) is key to effective discussions about new technologies in shipping. This will empower ports to drive innovation in the maritime industry.

This analysis positions ports as the fulcrum of the maritime industry's technological leap. Their historical role as central hubs for global shipping networks translates into a natural aptitude for technological adoption. By investigating the theoretical underpinnings of blockchain and its potential maritime applications, this study strengthens the case for PCSs as a crucial catalyst for

disseminating this transformative technology. The ubiquitous presence of PCS globally further reinforces ports' status as linchpins of technological progress in the maritime sector.

By facilitating information/service exchange within the port community, PCS lays essential groundwork for seamlessly implementing advanced technologies like blockchain. This interconnected system unifies diverse global maritime stakeholders, offering a strategically advantageous platform for integrating blockchain and fostering a more efficient, transparent maritime ecosystem.

A targetted gap Despite this strategic alignment and PCS-blockchain potential synergies, a concerning research and real-world application gap persists regarding deploying blockchain in port operations. This underscores the urgent need for a focused, systematic approach.

We hypothesize that a PCS encapsulating blockchain-based PoC can bridge theoretical promise and practical reality, drawing a new path toward significantly enhanced port operation efficiency/transparency across the wider maritime sector

5.2.2.1 Exploring the Absence of Blockchain-Based PCS

The governance models of ports are varied and complex. Despite these governance models being highly structured and seemingly irrelevant to technological advancement, they are deeply interwoven into the fabric of underlying infrastructure and information systems.

- *Public Port Authority Model:* Here, the port is typically owned by the government and managed by a public authority. This model is often seen in the United States and parts of Europe. Governance in this model tends to be bureaucratic and may be slower to adopt new technologies due to the layers of decision-making and regulatory considerations. A key reference here is (Brooks and Cullinane, 2006), which comprehensively examines port governance models across different global regions.
- *Landlord Port Model:* In this model, the public authority owns the land while the infrastructure is leased to private firms. This model is prevalent in many parts of the world, including parts of Europe, Asia, and North America. It allows for more flexibility and can potentially be more responsive to technological innovations like blockchain. (Notteboom and Winkelmanns, 2001) offer a detailed analysis of the landlord port model and its implications for port management and operations.
- *Private Service Port Model:* Here, private entities own and operate the ports like. This model is less common but can be found in some countries where the private sector partly or entirely operates maritime activities such as some oil terminals in France or the United Kingdom (de Commerce de Port-La Nouvelle, 2023) (Kyriakoulis and Botham, 2018). This model tends to be more efficient and could be more open to adopting technologies like

5.2. Theoretical and Empirical Foundations

blockchain. A reference for this model is provided by (Verhoeven, 2010), who discusses the privatization of port infrastructure and its impact on port governance.

Consequently, they play a crucial role in understanding why PCS have historically been absent from blockchain-based systems.

These detailed models shape how ports approach new technologies, ultimately affecting how they adopt and integrate blockchain into their operations. Port governance models influence not just administrative/operational structures, but also technological infrastructure and information flow.

The public Port Authority model's bureaucracy may seem resistant to rapid tech shifts, but ensures thorough vetting and potentially more sustainable new technology integration like blockchain.

The Landlord model's public oversight and private flexibility could facilitate quicker innovation adoption but pose unique multi-stakeholder consensus challenges.

The private Service Port model's perceived agility must navigate integrating blockchain into existing proprietary systems with competitive dynamics.

Integrating blockchain across these diverse models demands understanding existing infrastructures, stakeholder relationships, and regulations - not just the technology itself. These diverse models dictate distinct stakeholder roles/interactions and influence technological utilization.

Hypothesis As a unifying framework, PCS has the potential to facilitate blockchain integration across models by tailoring solutions to each model's characteristics while leveraging PCS as a common platform.

The challenge lies in navigating technological implementation alongside the complex governance structures, stakeholder interests, and existing setups - a multifaceted approach essential to realizing blockchain's transformative potential for enhancing port operation efficiency, transparency and security globally.

This can also be deduced from the analysis of the maritime literature as well. We can clearly detect two recurrent aspects.

PCS technological advancements Firstly, there is a focus on technological advancements that may involve the use of PCS, but these advancements are typically not blockchain-based (Caldeirinha et al., 2022), (Caldeirinha et al., 2020).

The nature of PCS as a centralized system comprising a complex superstructure presents certain limitations such as centralization and fragmentation (cf.14), thereby impeding the decentralizing effect that blockchain could facilitate. Consequently, hindering the potential for broader data and global sharing and transparency that blockchain technology could offer.

blockchain-based CS On the other hand, there are propositions in the literature that advocate blockchain systems. Nevertheless, they suggest entirely replacing existing CSs such as PCSs

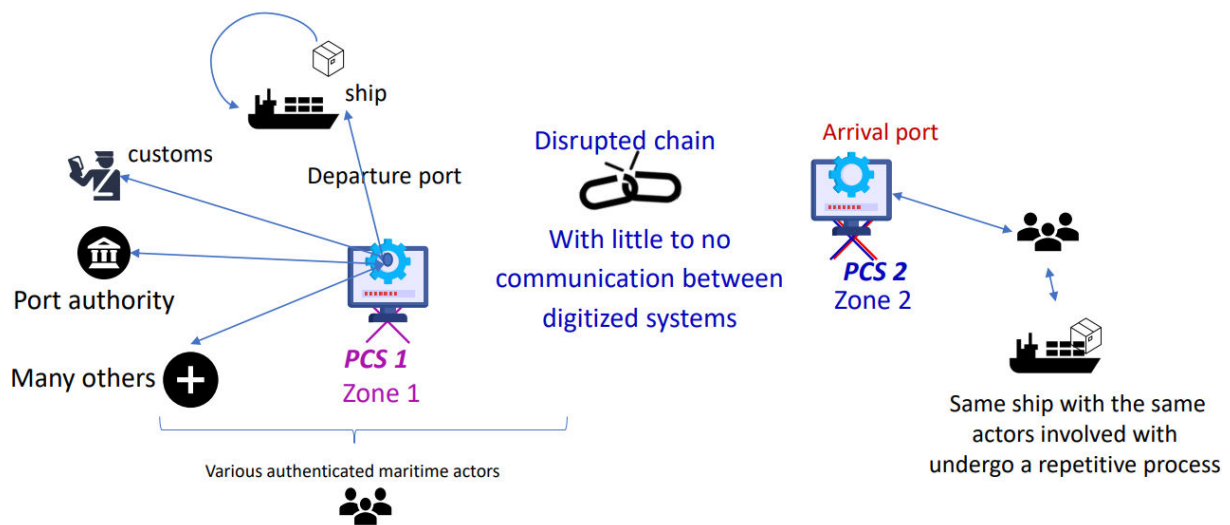


Figure 14: An illustration by the author of an example of a container's journey through PCSs across the globe

(Jović et al., 2020). This approach is also fraught with complications. Many PCS are developed and managed under the respective port governance models and represent a competitive advantage for the port. Replacing these systems with a blockchain-based alternative could disrupt established operational efficiencies and stakeholder relationships. Moreover, given that many PCS are tailored to the specific needs and governance structures of their respective ports, a one-size-fits-all blockchain solution may not be feasible or desirable.

The ideal approach therefore, seems to lie in a middle ground - integrating blockchain technology into the existing PCS framework in a manner that respects and utilizes the strengths of these systems while also addressing their limitations in terms of interoperability and data sharing. This integration requires a careful balancing act: it must acknowledge the governance models under which these PCS operate, respect the competitive dynamics at play, and yet strive towards the broader goal of enhanced efficiency, transparency, and security in maritime logistics.

5.2.2.2 Into Port IS structure

To effectively integrate blockchain into port information systems (IS), it was first necessary to understand the prevailing conditions and frameworks.

Existing research outlines a port IS taxonomy categorized as Silo, Integration, Supply-Chain, Port-Wide, and Inter-Port (Lee and Lam, 2016), encapsulating the progression from fragmented to comprehensive digitization and connectivity within and between ports.

Despite abundant literature exploring port IS evolution and desired advancements, a notable gap also persists at the inter-port level. Most research focuses on current functionalities and aspirational developments. This highlights a significant lag in achieving interconnectedness across different port operations.

5.2. Theoretical and Empirical Foundations

This observation reinforces our hypothesis and strategic approach. The absence of widespread inter-port IS enabling seamless communication and operations between ports underscores the potential impact of our proposed blockchain system. Incorporating blockchain not only aligns with the identified specifications at the beginning of the chapter but also addresses this critical gap by offering a solution to bridge disparate port systems. Our strategy aims to leverage blockchain to the transition towards more interconnected and efficient port operations aligning with the current digitization trends highlighted in Chapter 3 (SW, and interconnected PCS-CCS), substantiating our system's unique value proposition against the backdrop of the current IS taxonomy limitations.

HAROPA PORT In the quest to contextualize the implementation of blockchain technology in the maritime domain, HAROPA PORT stands as a paradigmatic example of the sector's dynamic nature and its adaptability to change. HAROPA PORT, an innovative merger of three significant ports - Paris, Le Havre, and Rouen - epitomizes the complexities and the evolving landscape of maritime logistics and port management.

Overview HAROPA PORT is not merely a physical entity but a symbol of strategic collaboration and forward-thinking in the maritime industry. The fusion of these three ports represents a significant leap in operational efficiency, economic growth, and environmental sustainability. Each port brings its unique strengths and capabilities, collectively creating a robust network that enhances the competitiveness and reach of the French maritime sector on a global scale.

- Paris: As an inland port, it contributes immensely to the hinterland connectivity, offering a vital link between maritime trade and inland transportation.
- Le Havre: Recognized as one of the largest seaports in France, it serves as a crucial gateway for international trade, particularly for transatlantic routes.
- Rouen: With its strategic location and specialized facilities, it plays a significant role in the handling of bulk cargo and agricultural products.

The Amalgamation and Its Implications It was within a few days of this thesis that the amalgamation of these three ports under the HAROPA PORT umbrella became effective. This acted as a testimony to the sector's evolving nature. This integration not only streamlines operations but also presents a unique case study for the implementation of innovative technologies, like blockchain, to embrace changes. The diverse operational dynamics and governance structures within each of these ports provide an intricate backdrop for exploring the practicalities of blockchain integration. The ever-evolving nature of the maritime sector, as exemplified by HAROPA PORT, underscores the need for adaptable and resilient technological solutions. Any proposed blockchain-based system must be flexible enough to accommodate the varying operational environments of these ports. It should be capable of addressing the specific needs of each

port while ensuring seamless interoperability and data exchange across the entire amalgamated entity.

5.3 Implementation Approach

The maritime sector, characterized by its expansive scope and intricate operations, presents a fertile ground for technological innovations. However, the sector's vast superstructure, complex infrastructure, and the sheer scale of ongoing operations pose significant challenges in implementing new technologies effectively. This complexity necessitates a focused approach, particularly when introducing transformative technologies like blockchain.

5.3.0.1 The Rationale for a Targeted Approach

Given the vast scope of the maritime industry, a proof-of-concept that comprehensively addresses all its complexities and operational scales would likely be overly ambitious and potentially infeasible within the constraints of a time-bound PhD program. To address this challenge, our strategy pivoted towards concentrating on a specific aspect of maritime operations – an approach that would allow for a more manageable and detailed exploration of blockchain's potential. This focused approach led us to the realm of dangerous goods traceability, a critical and sensitive area in maritime logistics that demands utmost precision and reliability. However, it is essential to keep in mind, while we focalise our efforts on a specific branch, the broader implications of our findings. The lessons learned and successes achieved have the potential to not only reshape the maritime industry but also to provide valuable insights for other sectors contemplating blockchain integration. This chapter, then, moves beyond a simple technology demonstration. It aims to provide a clear path towards the digital transformation of the maritime industry, with potential implications for other sectors.

5.3.1 Technology Stack

5.3.1.1 TIMAD: a digitized system in constant evolution

TIMAD, a PCS specifically designed for tracking and managing dangerous goods, presents a unique opportunity to test the efficacy of blockchain technology in a controlled yet significant aspect of maritime operations. This PCS, with its specialized focus, serves as a microcosm of the broader maritime ecosystem, allowing us to explore blockchain's applicability in a context that is both specific and relevant.

Its specialized integration capabilities and analytical functionalities set a new standard for use-case crafted digitized systems that ports globally can leverage. It harnessed increased digitalization, to address the multifaceted risks inherent in dangerous goods transportation. TIMAD's launch stems from pressing needs, intensified by heightening societal calls for accountability,

5.3. Implementation Approach

to reinforce oversight over the transit of hazardous materials within complex maritime supply chains. The solution's successful adoption at one of France's largest ports aligns with the growing strategic prioritization of technological capabilities, data harmonization, and regulatory frameworks that can aid the safe, efficient, and compliant operation of dangerous cargo flows amidst rapidly evolving regulatory landscapes.

By consolidating real-time tracking data from actors across the logistics chain, including port authorities, shipping companies, and regulators, TIMAD establishes visibility of hazardous cargo enabling stringent monitoring of compliance with rapidly evolving safety regulations while also optimizing coordination between stakeholders.

TIMAD's hazardous cargo oversight platform within HAROPA PORT reflects strategic consolidation of regional port assets under centralized governance to bolster transparency and collective risk management befitting northern France's import/export corridor (Merk et al., 2011). Initiated locally in 2008 through Le Havre's autonomous Port Authority as a basic web application labelled TIMAD V1, the system represented initial efforts unifying declarant reporting formalities promoting swift adaptations. While V1 pursued digitization for manifest documentation and liability transfers, oversight functionality remained limited without workflow integration. Governing stakeholders independently maintained responsibility across approval silos, constraining coordinated action on dynamic cargo staging and containment needs V1 firstly demonstrated potential in reconciling disparate leaseholder systems through common data requirements. But growing community concerns over environmental damage risks from industrial expansion compounded by natural occurrences such as crippling winter floods in 2010 galvanized calls for transparency enhancements (Elineau et al., 2011).

This impetus ultimately set the stage for TIMAD's full-scale overhaul through V2 featuring strengthened risk analytics, sensor integration, shipment reconciliation and collaborative messaging.

The successful 2018 rollout of TIMAD V2 delivered key promises of enhanced user experiences for declarants paired with reinforced oversight capabilities for port commanders and first responders. Digitized workflows now dictate targeted declarations based on goods characteristics, while advanced integration layering ties V2 securely into the operational systems relied upon daily by cargo handlers, emergency teams and customs units across 120km of current HAROPA waterfronts.

The evolution of TIMAD from its initial version to the sophisticated V2 iteration underscores the port's proactive role in developing and investing in its PCS. This development trajectory highlights not only the technological advancement aimed at increasing efficiency but also reflects the port's deep-seated responsibility in fostering an ecosystem where safety, transparency, and responsiveness are paramount. The case of TIMAD serves as a compelling example of how targeted technological interventions, underpinned by a commitment to continuous improvement, can significantly enhance the operational dynamics of a port.

5.3.1.2 Blockchain choice

- (Abdallah et al., 2023b,c) For our blockchain solution, we decided to employ Hyperledger Fabric as the core technology in our PoC. In chapter 2 this technology was mentioned as part of the permissioned blockchain.

The choice is underpinned by a thorough evaluation of its inherent features. based on all the findings detailed previously we headed towards our PoC to craft a meticulously studied innovatively customized solution for complex industrial applications such as maritime logistics.

- **Architectural Modularity and Customization** Hyperledger Fabric's modular architecture is a fundamental aspect that makes it particularly suitable for the maritime sector. This modularity allows for extensive customization, enabling the development of a blockchain network finely tuned to the specific operational dynamics of maritime logistics. The capacity to tailor the blockchain network to accommodate varying operational practices is pivotal in a sector characterized by diverse governance models and intricate logistic processes. The work (Androulaki et al., 2020) elucidates the benefits of such a modular architecture in industrial applications, emphasizing its adaptability and flexibility.
- **Ensuring Privacy in a Permissioned Ecosystem** The permissioned nature of Hyperledger Fabric is crucial in addressing the maritime sector's privacy and security concerns. The ability to create private networks and control access is paramount in a domain where sensitive data, such as cargo details and shipping logistics, are integral to operations. Hyperledger Fabric's architecture supports such controlled access, enabling secure and confidential data management. The research (Cachin et al., 2016) delves into the advantages of permissioned blockchains in ensuring data privacy and security, which is particularly relevant in the context of maritime logistics.
- **Scalability: A Key to Handling Vast Operations** Scalability is a critical factor in the maritime sector, given the vastness of operations and the volume of transactions involved. Hyperledger Fabric's design, particularly its efficient consensus mechanism, is adept at handling large volumes of transactions, a necessity for the smooth functioning of port operations and cargo tracking. The study by (Vukolić, 2017) highlights the importance of scalability in blockchain networks, especially in industries like maritime logistics that require high throughput and performance.

HAROPA Port, a pivotal player in this landscape, has been instrumental in shaping the work strategy. Working closely with TIMAD, HAROPA Port's PCS, we aim to infuse blockchain characteristics into the existing framework. This integration is designed not merely as an overlay of new technology but as a fundamental enhancement of TIMAD's technological capabilities. The introduction of blockchain features is poised to significantly augment the system's functionality, offering improved transparency, security, and efficiency. In the ensuing section, we will elaborate

on the intricacies of our findings, which have been developed into a comprehensive design and implementation plan. This plan is motivated by the tangible demands of the maritime industry and is sculpted to align with its actual operational requirements. Central to our approach is the recognition of the Port as an instrumental element in driving technological innovation within the maritime sector, particularly as a catalyst for the integration of blockchain technology.

5.3.2 Design principles

There is a common misconception that surrounds blockchain technologies depicting them as too complicated adding further entanglement. This is why we also focused our conceptual architectural proposition on offering a platform that can be easily integrated into the maritime sector.

In the ensuing section, we will elaborate on the intricacies of our findings, which have been developed into a comprehensive design and implementation plan. This plan is motivated by the tangible demands of the maritime industry and is sculpted to align with its actual operational requirements. We aim to showcase how blockchain technology can be seamlessly integrated into the maritime sector's existing infrastructures, specifically through PCS like TIMAD, to catalyze a new era of digital transformation in maritime logistics.

By designing blockchain solutions with user-friendliness and ease of integration in mind, stakeholders in the maritime sector can more easily understand and utilize the benefits of blockchain technology. This can help reduce the learning curve and technical barriers to entry, making it more accessible and appealing to a wider range of participants. Furthermore, it promotes collaboration among different stakeholders in the maritime sector, leading to a more streamlined and efficient supply chain. Hence, we can more effectively harness the potential benefits of blockchain technology.

Intra-maritime Operations For PoC projects, a total database transfer to blockchain appears impractical and overly complex, risking redundancy. A more judicious approach selectively concentrates on essential data aspects currently absent in existing systems (Abdallah et al., 2023a). This targeted method allows demonstrating blockchain's unique benefits like heightened security, transparency, and operational efficiency without extensive deployment. When choosing data for blockchain integration, factors like sensitivity, access frequency, stakeholder relevance, scalability potential, and compatibility with existing systems must be considered. This holistic approach to selective integration optimizes performance, reinforces security, and ensures seamless blockchain implementation alignment with strategic goals and regulations. Furthermore, determining an appropriate blockchain type and consensus mechanism, explored later, critically impacts functionality, governance framework, and organizational strategic alignment. Our study contributes a sophisticated understanding of blockchain integration in community systems by advocating a focused, informed approach underpinned by thorough blockchain literature analy-

sis tailored to organizations' specific needs and aspirations. This guides developing blockchain solutions technologically sound and strategically aligned.

A maritime insider The digitalization of the maritime industry has led to the adoption of centralized platforms for efficient data exchange (Dewulf et al., 2015). However, managing user accounts for the diverse range of actors within the network becomes challenging in a centralized system that covers the entire network. The International Maritime Organization (IMO) advocates for standardized Legal Identifiers (LIs) to authenticate organizations in these platforms, promoting security and trust. LIs are generally considered unique and secure as they are issued and approved by government authorities, adhering to various regulations and on standards to guarantee accuracy and authenticity. A widespread approach in the maritime sector is the utilization of LIs to establish a brokered authoritative transitional (BAT) access.

What is BAT access Each organization uses its legal identifiers to create an administrator account and manages its own hierarchy in the centralized system using different roles, permissions and access rights for its different users while adhering to system oversight. Through LIs, organizations represent their users on the network and satisfy legal obligations to treat other parties honestly. This approach strikes a balance between centralized control and local autonomy, enhancing efficiency and regulatory compliance. By utilizing LIs and administrative accounts, the central system is relieved of excessive administrative burdens, while LIs enhance security and trust in the network. However, limitations linked to accountability and transparency have sparked our interest. Blockchain technology offers a solution by providing decentralization, immutability, and transparency. Leveraging blockchain can overcome centralization challenges and establish a distributed network where multiple stakeholders participate in transaction validation and verification.

Blockchain background work Our research surrounding DIDs in chapter two was not primarily focused on the technical aspects of DIDs. Instead, what piqued our interest was their characteristics.

These characteristics can further elevate technological development, particularly in a global industry such as the maritime as they can enhance operational efficiency and convenience. They converge towards IMO recommendations such as the 2017 STCW amendment that necessitated identification documents' standardization and encouraged secure and verifiable electronic certificate use for enhanced security and efficiency.

A Challenge Statement The implementation of DIDs in the maritime sector faces significant challenges due to the lack of standardized governance mechanisms and a globally spread infrastructure. The decentralized and distributed trust models of DIDs conflict with existing hierarchical governance structures in the sector. Despite ongoing efforts in standardization,

regulations, and digital identity projects, the adoption of DIDs in the maritime sector is still a distant prospect. The sector must first address underlying infrastructure and superstructure challenges before embracing DIDs (Abdallah et al., 2023d). Additionally, the maritime sector is known for its technological conservatism, and resistance to DID implementation may arise due to the presence of established Legal Identifiers (LIs) that serve a similar purpose in maritime information systems.

5.3.3 A Solution Strategy: Blockchain-based BAT access

The exploration of the benefits and challenges of adopting Decentralized Identifiers (DIDs) in the maritime industry has prompted a strategic shift in our approach. Implementing a full blockchain solution in the maritime sector may be complex and face various obstacles, making it challenging to achieve widespread adoption. Therefore, we have focused on a specific use case that is more manageable and feasible, allowing us to showcase the added advantages of the technology. This specific use case involves addressing accountability and transparency concerns through the concept of brokered authoritative transitional (BAT) access. Our shift in strategy also considers the functional similarities between DIDs and Legal Identifiers (LIs). Both serve as unique digital identifiers within information systems, promoting trust and authenticating the identity of the entities involved. However, it is important to note that we do not use these identifiers interchangeably. Additionally, we have drawn inspiration from the existing balance between centralization and autonomy, aiming to innovate and address the industry's needs and challenges. We aim to build upon pre-existing technologies and criteria while introducing new and beneficial advancements in the maritime sector.

In BAT information systems, balancing operational efficiency with centralized oversight and control poses challenges for accountability. Legal Identifiers (LIs) provide administrative access, granting organizations autonomy over their users and access permissions, but this can result in a lack of transparency and accountability. Blockchain-based DIDs are promoted as a promising solution for accountability by simplifying authentication and identification processes (Maldonado-Ruiz et al., 2021). In the maritime industry, we propose the novel combination of LIs and smart contracts as a revolutionary approach. This approach maintains current operational practices while introducing blockchain technology to enhance transparency and accountability. By leveraging smart contracts, administrative access to the centralized system can be notarized in a decentralized environment, leading to increased transparency and effectiveness while improving security. The combination of LIs and smart contracts has the potential to significantly transform transparency, accountability, and overall system performance.

5.3.3.1 Enhancing Accountability through Blockchain in Maritime Operations

The focus of our PoC is centered around enhancing accountability within the maritime sector, particularly in the context of the TIMAD system, which is dedicated to the management of

dangerous goods. To this end, we have identified two key areas for blockchain implementation: stakeholder identification in TIMAD using Brokered Authoritative Transitional (BAT) access, and the securing of cargo manifests.

5.3.3.2 Notarization of Stakeholder Identifications in TIMAD

In most PCSs, including TIMAD, BAT access is commonly employed due to the administrative complexity inherent in managing a multitude of user accounts across various organizations. After an administrative account is created for an organization, it manages its own users. It handles user creations, their roles and granting and revoking rights as needed. However, in many cases, the log-keeping of these administrative actions is either minimal or non-existent, or it relies on simple log files with inadequate security measures. This lack of detailed and secure record-keeping can lead to accountability issues, which is particularly problematic in systems handling dangerous goods.

In our PoC, we propose to use blockchain technology to notarize data related to stakeholder identifications in TIMAD. By leveraging blockchain's immutable ledger, every administrative action, such as the creation of users, and granting or revoking of user permissions, will be securely recorded. This approach ensures a transparent and tamper-proof record of all changes made within the system, significantly enhancing accountability and security.

5.3.3.3 Securing Cargo Manifests on Blockchain

In transitioning from a broad exploration of blockchain's potential within the maritime sector to a focused implementation, our research strategically zeroes in also on the critical use case of securing cargo manifests. This choice is not arbitrary but is rooted in the manifest's fundamental role in maritime logistics, encapsulating the essence of cargo details and operational nuances. Cargo manifests, as pivotal documents, hold the key to enhancing operational transparency, safety, and efficiency. Their integrity and authenticity are paramount, especially when dealing with sensitive or hazardous materials. Thus, our decision to target cargo manifests for blockchain integration embodies a strategic move towards reinforcing accountability and reliability in maritime operations.

HAROPA PORT employs the Transport Information Management and Declaration (TIMAD) system to manage the traceability of hazardous materials, ensuring compliance with both local and international regulations. This system mandates that hazardous materials be declared electronically through a process that references the International Maritime Dangerous Goods (IMDG) Code before they are brought into the port. This allows port authorities to be fully informed and manage these goods safely.

The local regulations (Règlement Local pour le Transport et la Manutention des Marchandises Dangereuses) set specific conditions, such as the maximum allowable quantities of dangerous goods on docks and requirements for the storage durations and conditions on land,

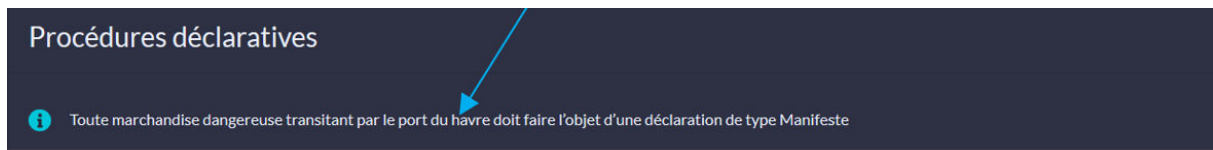


Figure 15: All hazardous materials transiting through the Port of Le Havre must be declared in the form of a 'Manifest' declaration. - TIMAD

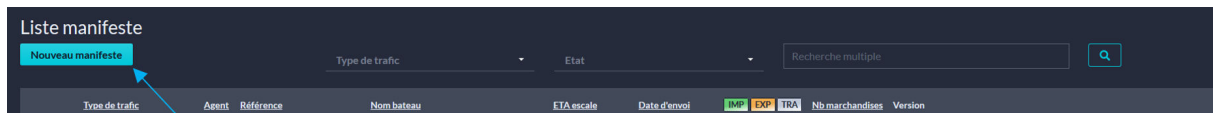


Figure 16: Add a new manifest - TIMAD

particularly for containerized goods. These detailed provisions help ensure safety and environmental protection by stipulating standards for reporting and handling dangerous goods. Through TIMAD, declarants are guided comprehensively on these procedures and are required to submit their information as part of a formal request for port entry (*demande d'entrée au port*), facilitating the efficient and secure handling of hazardous materials within maritime logistics.

The request submitted through TIMAD is then processed by the port's harbormaster (*capitaine*), who evaluates it to ensure compliance with all relevant regulations. This approval process is crucial for allowing the entry of ships carrying hazardous materials into the port, ensuring that all safety and environmental standards are met before access is granted. This systematized approach helps maintain operational efficiency and safety within the port.

There is a requirement for a formal declaration process for hazardous goods when they are going through the Port of Le Havre, which is a part of the regulatory compliance to ensure the safe and secure handling of such materials through TIMAD (cf. Figure 15).

The use of a 'Manifest' would typically detail the nature of the hazardous materials, their quantities, and any specific handling instructions necessary for the port authorities and other parties involved in the transportation process (cf. Figure 16). This applies to the different types of goods transiting through the port (cf. Figure 17).

Moreover, the choice to notarize cargo manifests on the blockchain reflects a deliberate effort to address the existing gaps in the maritime sector's information systems. By creating an immutable and auditable trail of all changes made to cargo manifests or cancellations, we introduce a layer of accountability previously absent. This move aligns with our broader objective of leveraging blockchain technology not as a disruptor but as an enhancer of existing systems, preserving the business logic while infusing an added layer of security and transparency.

This targeted approach exemplifies our commitment to pragmatic, impactful research, bridging the gap between theoretical potential and practical applicability. It also signals a nuanced understanding of the maritime sector's complexities, recognizing the need for solutions that are both technologically sound and strategically aligned with the sector's operational realities. By focusing on cargo manifests as a starting point, we set the stage for further exploration of other

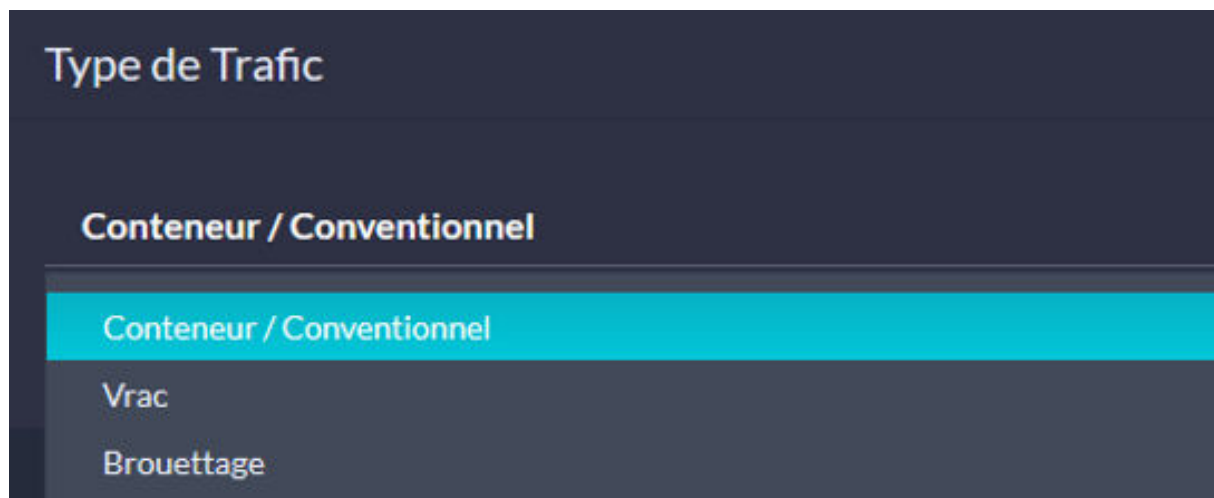


Figure 17: Add a new manifest: List of possible dangerous goods - TIMAD

critical information that can benefit from blockchain’s notarization capabilities, paving the way for a more comprehensive integration of blockchain technology in maritime logistics.

the cargo manifest is a fundamental document in maritime logistics, detailing all the cargo carried on a ship. It serves multiple purposes, including providing information for customs clearance, ensuring the safe loading and unloading of cargo, and assisting in emergency response scenarios. The manifest typically includes details such as the nature, quantity, and destination of the cargo. In current practices, cargo manifests can be subject to revisions and updates, leading to the creation of multiple versions over time.

Notarization of Entity Actions on Blockchain An important aspect of our blockchain implementation is the notarization of both the information and the entities behind each action. This means that every modification to the system by any user or administrative entity will be recorded on the blockchain. This level of detailed tracking ensures that each action and its corresponding actor are permanently logged on the immutable ledger, significantly increasing accountability within the system.

By incorporating these blockchain-based solutions into TIMAD, we aim to address the existing gaps in accountability and security, particularly concerning the management of dangerous goods. This enhanced level of transparency and accountability is not just a technological improvement but also a strategic step towards fostering a safer and more reliable maritime logistics environment.

Maintaining Business Logic and Trust in the Information System In implementing these blockchain-based solutions, it is crucial to emphasize that our approach does not alter the existing business logic within the TIMAD information system. The core operational practices and the trust relationships established among stakeholders remain intact. Our primary objective is not to challenge or revoke the trust granted to stakeholders within the system. Instead, we aim to

supplement and enhance the system with an additional layer of accountability and security.

By integrating blockchain technology, we provide a robust audit trail for all activities within the system. This audit trail is a transparent and immutable record of actions, which does not interfere with the normal operation of the system or the autonomy of stakeholders. Instead, it serves as a tool for verifying and validating actions post-facto. This approach is particularly beneficial in a context where multiple stakeholders interact and where transparency is key to maintaining trust and efficiency.

The value of this implementation lies in its ability to provide tangible benefits to all stakeholders in the system. For instance, in the event of a dispute or investigation, the blockchain ledger offers an indisputable record of actions and changes, aiding in quick resolution and maintaining operational integrity. It also serves as a deterrent against fraudulent or unauthorized activities, as all actions are permanently recorded and easily auditable.

Our approach recognizes the importance of maintaining the established trust and workflow within the maritime logistics system while introducing an innovative solution to enhance transparency and accountability. By doing so, we aim to strengthen the overall trustworthiness and reliability of the system without disrupting its fundamental operational principles. This careful balance between innovation and respect for existing practices is key to the successful integration of new technologies like blockchain in complex, multi-stakeholder environments such as maritime logistics.

5.3.4 Simulative Environment and Role of HAROPA PORT in the PoC

It is important to highlight that the initial stage of our PoC does not commence in a real operational environment but rather in a simulated setting. This approach allows for rigorous testing and refinement of the blockchain integration without impacting actual maritime operations. As previously discussed, the port plays a crucial role in driving technological advancements in the maritime sector. In line with this, our collaborative partner, HAROPA Port, will be the primary host for this PoC blockchain environment.

HAROPA Port's involvement is particularly significant given its interest in exploring and adopting innovative technologies. Since the logs of TIMAD, as well as its database, are already hosted within the port's infrastructure, the addition of a blockchain ledger in this environment is a logical extension. This integration ensures that the blockchain ledger is securely hosted on the port's infrastructure, aligning with the existing data management practices.

Importantly, hosting the blockchain ledger within the port's infrastructure does not introduce any new legal or audit challenges regarding data access and management. We are not transferring sensitive data to external parties, nor are we altering the existing access management protocols of the PCS. Access to the TIMAD system and its data remains strictly controlled within the PCS framework, ensuring compliance with existing data protection and privacy regulations.

This strategic choice of hosting the blockchain ledger at HAROPA PORT serves multiple

purposes. It allows for a controlled and secure environment to test and demonstrate the efficacy of the blockchain solution. It also ensures that the implementation is in line with legal and operational standards, maintaining the integrity and confidentiality of the data. Furthermore, by situating the PoC within the port's existing infrastructure, we leverage the port's strategic position and resources to propel the technology forward, demonstrating the potential for wider adoption in the maritime sector.

5.4 Towards implementation

The strategic approach outlined in this chapter represents a significant stride towards realizing the transformative potential of blockchain technology within the maritime sector. By identifying the port as a crucial catalyst and leveraging the pivotal role of Port Community Systems (PCS) like TIMAD, we have established a robust foundation through which we can establish seamless blockchain integration.

The decision to focus on enhancing accountability through blockchain-based notarization of stakeholder identifications and cargo manifests addresses critical pain points in the industry.

As we move forward, the next chapter will delve into the technical intricacies of our blockchain implementation. It will provide a comprehensive overview of the architectural design, smart contract development, and integration strategies employed to merge blockchain capabilities with the TIMAD system seamlessly.

TECHNICAL IMPLEMENTATION - A

BLOCKCHAIN INFRASTRUCTURE

Contents

6.1	Integrating Blockchain with Existing PCS Infrastructure	107
6.2	High-Level Conceptualization for Blockchain Integration	108
6.2.1	Current PCS State	109
6.2.2	Data Integration in Blockchain Implementation with TIMAD v2	110
6.3	Network Architecture	111
6.3.1	Envisioning the Integrated Blockchain-PCS Environment	111
6.4	Creating a Secure Blockchain environment	111
6.5	Organizational Structure	115
6.5.1	Permissions and roles	119

As we progress in our exploration of implementing blockchain technology within the maritime sector, we now enter the conception phase, where we aim to conceptualize an adequate implementation strategy. Having chosen Hyperledger Fabric (HF) as our blockchain platform and identified the key data elements for storage —particularly in relation to TIMAD— we are poised to outline a strategic implementation plan.

6.1 Integrating Blockchain with Existing PCS Infrastructure

One of our core strategies is not to replace TIMAD, but to rethink and enhance it with a new blockchain-based layer that integrates existing functionalities while introducing additional features. This approach is particularly relevant in the maritime industry, where PCS have evolved into integral components of competitive advantage, underpinned by substantial infrastructure investments.

The necessity to maintain and leverage existing PCS infrastructures while progressively introducing blockchain technology is a strategic decision. In the maritime sector, PCS has become deeply embedded in operational processes, and any abrupt replacement or overhaul could disrupt these well-established systems. This is similar to the gradual implementation

approach observed in the development of MSW Systems, which demonstrated the complexity and challenges of integrating new systems, even with broad international support.

6.2 High-Level Conceptualization for Blockchain Integration

Our high-level conceptualization for integrating blockchain with TIMAD revolves around a phased and cautious approach. This methodology acknowledges the complexities and potential resistance associated with introducing a technology as transformative and, at times, controversial as blockchain.

The envisioned integration involves several key components:

- **Data Notarization and Security** Implementing blockchain for the secure notarization of critical data, such as stakeholder identifications and cargo manifests in TIMAD, ensuring an immutable audit trail.
- **Interoperability with Existing Systems** Designing the blockchain layer to be fully interoperable with the existing TIMAD infrastructure, ensuring seamless data flow and minimal disruption to current operations.
- **Incremental Feature Integration** Gradually introducing additional blockchain-enabled features, such as enhanced data verification and smart contract functionality, to improve operational efficiency and transparency.
- **Stakeholder Collaboration and Feedback** Engaging with key stakeholders, including HAROPA Port, to gather feedback and ensure that the blockchain integration aligns with their needs and expectations.
- **Legal and Regulatory Compliance** Ensuring that the blockchain implementation complies with relevant legal and regulatory standards, particularly concerning data privacy and security.

The strategic goal is to demonstrate the added value of blockchain integration in a controlled, non-disruptive manner, thereby fostering acceptance and understanding among maritime sector stakeholders. This approach also allows for the monitoring and evaluation of blockchain's impact on PCS performance, setting the stage for more extensive adoption and potentially broader system transformations in the future.

In essence, our high-level conceptualization for blockchain integration with TIMAD aims to strike a balance between innovation and practicality, ensuring technological advancement while respecting the established dynamics of the maritime sector.

6.2. High-Level Conceptualization for Blockchain Integration

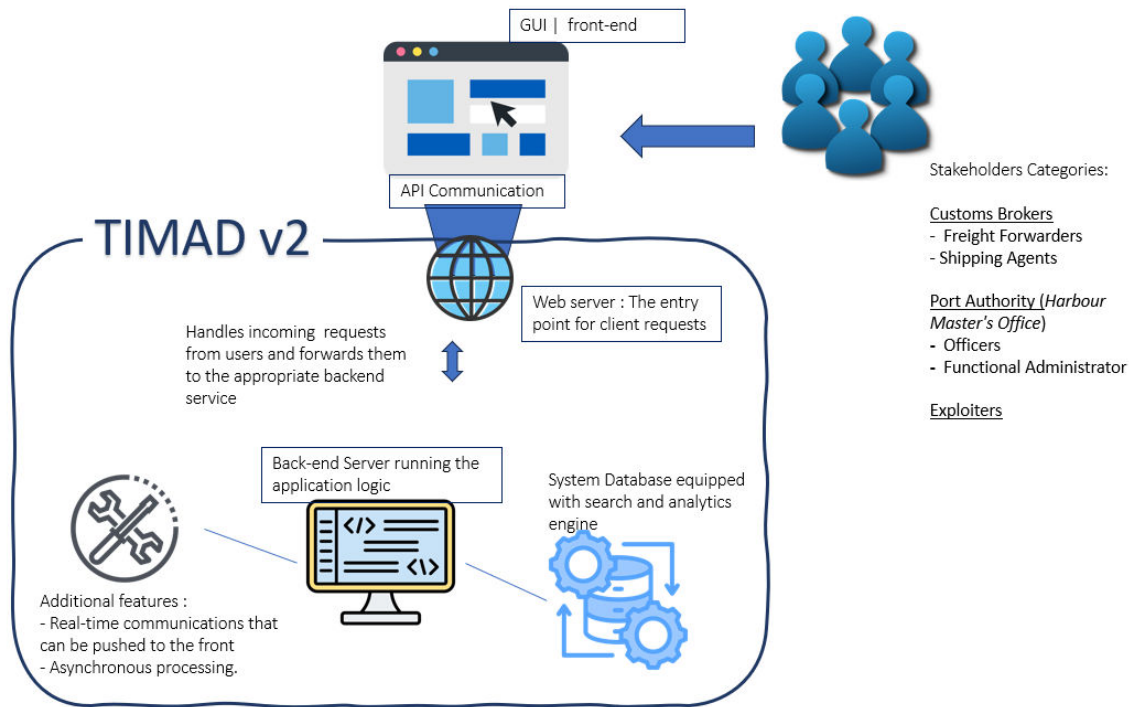


Figure 18: An illustration by the author of TIMAD v2 operational aspects

6.2.1 Current PCS State

The architecture of TIMAD is a sophisticated information system that integrates various components to facilitate the management and operational efficiency of port logistics as displayed in Figure 18. At the front end, a Graphical User Interface (GUI) allows stakeholders to interact with the system seamlessly. This interface communicates with the backend services through a robust API, ensuring that user requests are handled efficiently.

The system's architecture is designed with a web server acting as the gateway for incoming client requests, directing them to the appropriate backend services. The backend is composed of servers running the application logic, which is the core of TIMAD, responsible for processing data and executing the business rules of the system.

Additionally, TIMAD is equipped with a comprehensive centralised system database hosted within HAROPA PORT infrastructure that supports advanced search capabilities and analytics engines. This database is essential for storing, retrieving, and analyzing vast amounts of data pertinent to port operations.

The system also boasts additional features such as real-time communications, which enable immediate updates to be pushed to the front-end, and asynchronous processing, which allows the system to handle multiple operations concurrently without delays.

The stakeholders who utilize TIMAD span several categories: customs brokers (freight forwarders and shipping agents), the port authority (including officers and functional administrators), and exploitants, who oversee operational tasks. Each category of users leverages the

system's features to perform specific roles, from managing cargo documentation to administering port operations and ensuring the smooth flow of goods through the port.

6.2.2 Data Integration in Blockchain Implementation with TIMAD v2

It is imperative to clarify that data selection for blockchain recording encompasses a broad spectrum of system aspects and is not confined to any single facet or stakeholder group. This diverse selection reflects the multifaceted nature of stakeholder interactions within TIMAD v2, encompassing various categories of users, each with their distinct functional roles. Consequently, the data pertinent to each stakeholder group is inherently varied and specific to their operational needs within the system.

Given the sensitivity and the proprietary nature of the information within TIMAD v2, it is necessary to maintain confidentiality regarding the precise details of the data structure and its specific alignment with stakeholder groups. The architecture and operational dynamics of PCSs like TIMAD v2 often, reflect the heterogeneous nature of maritime logistics systems. As such, the disclosure of detailed data structuring and its specific application within TIMAD v2 may not be universally applicable or relevant to the broader context of PCS operations.

Moreover, the focus of our dissertation is not on the intricate technicalities of data within TIMAD v2, but rather on the overarching methodology and strategic implications of integrating blockchain technology into such a sophisticated system. We aim to enhance transparency, accountability, and operational efficiency through this integration while respecting the confidentiality and security requirements inherent in maritime logistics operations.

Therefore, our approach to blockchain integration is carefully tailored to complement the existing framework of TIMAD. It aims to enhance its capabilities without compromising the confidentiality and proprietary aspects of the system's data architecture. This strategy ensures that our integration efforts are both respectful of the system's operational integrity and aligned with the broader objectives of technological advancement in the maritime sector.

It's important to note that the integration will be done in a manner that respects the privacy and security of the stakeholders' information. The blockchain layer will act as an additional security and verification mechanism without disrupting the existing functionality and user experience of TIMAD. This strategic approach ensures that the integration is beneficial to all parties involved and aligns with the overall goal of improving maritime logistics operations through technological innovation.

6.3 Network Architecture

6.3.1 Envisioning the Integrated Blockchain-PCS Environment

The conceptual illustration provided as seen in Figure 19 delineates the envisioned state of the TIMAD system after blockchain integration, converging towards a cohesive network architecture that fortifies the PCS with the robustness of blockchain technology.

Seamless Integration for Enhanced Notarization We want to encapsulate a seamless interaction between the existing dangerous goods dedicated PCS - TIMAD infrastructure and the proposed blockchain layer. The goal is to connect a blockchain infrastructure that allows for the seamless notarization of data critical to the maritime logistics operations carried out by various stakeholders. They engage with the TIMAD system through a Graphical User Interface (GUI).

Maintaining Operational Flow and Security The integration aims to notarize relevant actions and data without disrupting the current business flow or compromising operational efficiency. It is designed to reinforce the PCS with a secure blockchain environment, bolstering data integrity and traceability while upholding the swift and reliable service delivery that stakeholders depend on.

Backend and API Communication At the core of the network architecture is the backend infrastructure, responsible for executing the application logic and managing the system's data processing. It communicates with the front-end GUI through a robust Application Programming Interface (API), ensuring effective handling of user interactions.

Blockchain as a Security Layer The blockchain environment acts as a foundational security layer within this architecture, enhancing the PCS's resilience against data tampering and unauthorized access. It provides an immutable ledger where notarized data is time-stamped and chronologically recorded, offering an additional layer of trust and verification for the stakeholders' transactions and interactions.

6.4 Creating a Secure Blockchain environment

We chose a permissioned blockchain environment drawing from our analysis and literary contribution previously set forth. Consequently, we need to implement network components that would allow to secure the permissioned environment.

Certificate Authorities (CAs) play a pivotal role in HF network, serving as the backbone for identity management and secure transactions. In the context of integrating the TIMAD system with a blockchain network, establishing a secure connection is paramount. CAs are instrumental

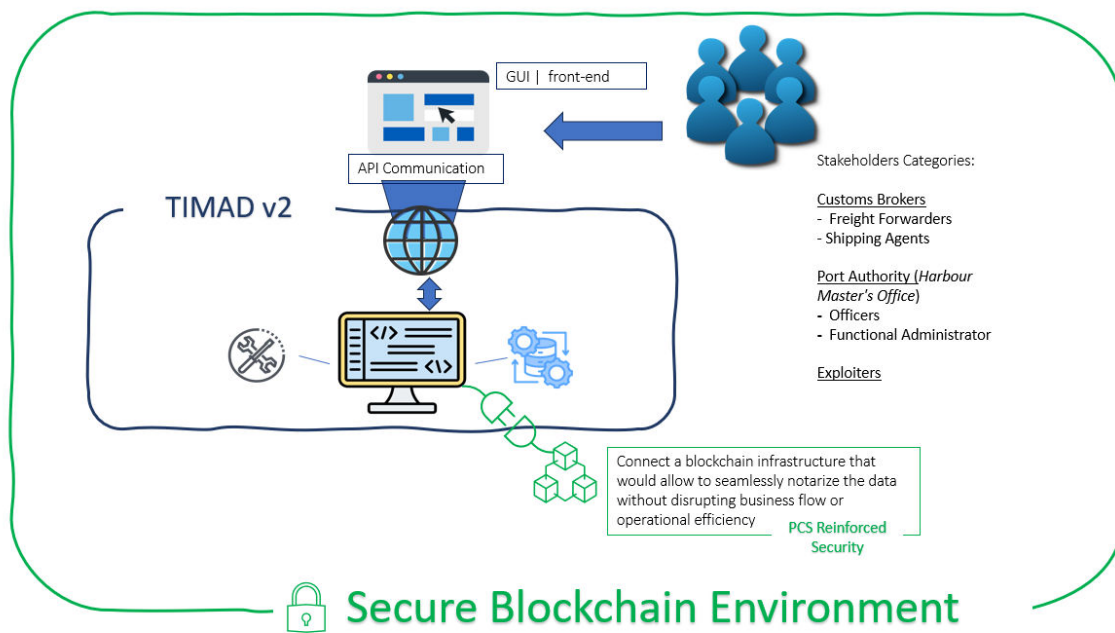


Figure 19: An illustration by the author of the envisioned wanted State

in this process, as they issue digital certificates that authenticate and verify the identities of participants within the network.

Understanding Certificate Authorities A Certificate Authority in HF is a trusted entity responsible for managing digital certificates. Digital certificates are electronic credentials that confirm the identity of network entities. These credentials are essential for creating a secure communication channel, as they ensure that the entities involved in transactions are who they claim to be. In essence, CAs act as a digital form of a notary, attesting to the identity and legitimacy of each participant in the network.

Types of Certificate Authorities in Hyperledger Fabric HF utilizes several types of CAs, each serving specific roles within the network:

- **Root Certificate Authority (Root CA):** The Root CA is the most trusted CA within the network and sits at the top of the CA hierarchy. It issues certificates to Intermediate CAs and has the ultimate signing authority. It is critical for establishing the trust anchor for the network and is typically kept offline for security purposes.
- **Intermediate Certificate Authority (Intermediate CA):** Intermediate CAs are subordinate to the Root CA and can issue certificates to other entities, such as other Intermediate CAs or end entities. They act as a bridge between the Root CA and the entities that perform transactions, helping to manage the load and streamline the certificate issuance process.
- **Orderer Certificate Authority (Orderer CA):** This CA issues certificates specifically for

6.4. Creating a Secure Blockchain environment

the nodes that maintain the ledger and order transactions (the orderers). These certificates ensure that only authorized orderers can create new blocks and maintain the network ledger.

- **Peer Certificate Authority (Peer CA):** Peer CAs issue certificates to peer nodes, which endorse transactions and maintain the ledger. Certificates from Peer CAs authenticate peer nodes when they join the network and interact with applications and other peers.

The Root CA is at the top of the certificate authority hierarchy. It is the most trusted entity in the network and is responsible for issuing certificates to Intermediate CAs. The Intermediate CAs, which are subordinate to the Root CA, further issue certificates to other entities, including the Orderer and Peer CAs. In our development environment we generate a Root CA for each organization, that will function as a RootCa within the context of that organization. Each of these CAs will then issue certificates for the respective nodes and users specified in our configuration,

In further steps, and for the production environment a more hierarchical structure with a separate, highly secure Root CA and multiple Intermediate CAs will be used based on our environment scalability for increased security.

Importance of Certificate Authorities The importance of CAs in an HF network cannot be overstated, particularly in the following areas:

- **Identity Verification:** CAs provide a mechanism for verifying the identity of participants, which is crucial for establishing trust among unknown parties in a decentralized environment.
- **Security:** Digital certificates issued by CAs encrypt the communication between network participants, ensuring confidentiality and protecting against unauthorized access.
- **Integrity:** Certificates prevent tampering with transaction data, ensuring that the information recorded on the blockchain is accurate and unaltered.
- **Permissioned Network:** In a permissioned blockchain like HF, where access control is a fundamental feature, CAs are essential for managing the permissions and roles of network participants.

By creating a network of trusted CAs, we ensure that every stakeholder interacting with the TIMAD system through the blockchain network can do so securely and reliably. These CAs form the foundation for a secure blockchain environment where transactions are transparent, auditable, and resistant to fraud. As we integrate the TIMAD system with the blockchain network, we will configure and deploy these CAs with careful consideration of their hierarchical structure and specific roles, ensuring a robust and secure network architecture.

Balancing Certificate Authority Focus with Traceability Objectives While the deployment of Certificate Authorities (CAs) is an essential component in establishing a secure blockchain environment, the primary objective of this thesis remains centred on enhancing traceability within the PCS. To maintain this focus and ensure a balanced approach, we utilized the ‘cryptogen’ tool provided by Hyperledger Fabric for the initial phase of our development.

Utilization of Cryptogen Tool The ‘cryptogen’ tool is a HF utility designed to simplify the creation of cryptographic material. It serves as a convenient means to generate the necessary key pairs and certificates for configuring the blockchain network, which is particularly useful in the developmental and testing phases.

By employing ‘cryptogen’ we develop a configuration file based on our wanted network architecture, and through the tool, we can generate all the required crypto materials needed for our environment repleted with the requisite security features, without devoting an inordinate amount of time to the manual setup of CAs.

The ‘cryptogen’ tool utilizes the configuration file, to specify the architecture of the network and the properties of the CAs and other entities.

The tool in HF uses industry-standard algorithms to generate cryptographic materials for Certificate Authorities (CAs) and other network entities. It primarily uses Elliptic Curve Digital Signature Algorithm (ECDSA) (Genç and Afacan, 2021) for generating key pairs. ECDSA is favoured for its strength and efficiency, particularly in creating shorter signatures compared to other algorithms like RSA, without compromising security. It is well-suited for systems where high security and performance are paramount.

Understanding Key Pairs and Their Function A key pair consists of a private key and a public key. The private key is a secret key that is used to sign transactions, and it must be kept confidential by the owner. The public key, derived from the private key, can be shared with others in the network. It is used to verify that a transaction was signed by the private key holder and ensures that the transaction has not been altered in transit.

Certificate Authorities and Certificate Granting

1. **CAs:** responsible for issuing digital certificates, which are electronic documents that use a digital signature to bind a public key with an identity. The digital certificate can be used to verify that a public key belongs to an individual, organization, or device (collectively known as "subjects").
2. **Certificate Issuance:** When a subject (such as a user or a peer node) joins the network, they must first register with a CA. The CA verifies the subject’s identity and then issues a certificate, signing it with the CA’s private key. The certificate contains the subject’s public key and other identifying information.

3. **Certificate Use in the Network:** Within the blockchain network, when a subject wishes to perform a transaction, they sign it with their private key. Other network participants can use the signer's public key, as provided in the certificate, to verify that the transaction is legitimate. This process ensures that only authorized entities can perform transactions and that each transaction is securely linked to the entity that initiated it.

Integration of Key Pairs and Certificates in our blockchain environment The 'cryptogen' tool generates key pairs and certificates for the network's orderers, peers, and users. The private keys are securely stored and used by the entities to sign transactions and communications within the network. The corresponding public keys are embedded within certificates that are distributed to network participants who need to verify transactions.

The generated cryptomaterials by 'cryptogen' provide the initial trust foundation that is essential for a secure and functioning permissioned blockchain network like HF. As we transition from a development to a production environment, these materials will be managed by fully operational CAs, which will handle the dynamic issuing, revoking, and renewing of certificates as the network evolves and as different entities join or leave the network.

6.5 Organizational Structure

The organizational structure of our PoC is meticulously engineered to reflect the complexities and requirements typical of a real-world blockchain network. This structure is comprehensive, encompassing the creation of CAs, organizational structures, system channels, and genesis blocks. More importantly, this foundational setup is not just a rudimentary framework but a substantive base upon which our PoC is built.

Our PoC environment includes three distinct organizations, each integral to the network's operation. Despite its simulative nature, the setup incorporates all elements necessary for a real-world application. This approach ensures that no critical components are overlooked and that each aspect of the network is thoroughly understood and aligned with maritime logistics logic. The use of tools like 'cryptogen' is employed not just for expediency but also to ensure a comprehensive understanding of the network's functioning and requirements.

Organizational Entities in Hyperledger Fabric Within HF, organizations act as entities with business interests and dedicated roles. Each organization has a unique domain, functioning as its own namespace. This domain defines the organization's identity and scope within the network. Additionally, Subject Alternative Names (SANS) are included within certificates to identify various domain names and IP addresses associated with the organization. These SANS help secure flexible and reliable communication channels across the network.

Distinct Certificate Authorities for Each Organization For each organization, a dedicated Certificate Authority (CA) is established. This distinction is essential for maintaining the integrity and security of each organization's operations within the network. The different types of organizations in our network are:

- **Orderer Organization:** This type of organization is responsible for maintaining the network's ledger and managing the consensus process. It plays a crucial role in transaction ordering and block creation.
- **Peer Organization:** Peer organizations host peer nodes, which endorse transactions, maintain the ledger, and interact with chaincodes (smart contracts). They are pivotal in processing and validating transactions.

In our PoC, we have incorporated HAROPA PORT, which maintains the TIMAD system, as a pivotal peer organization within our blockchain environment. This strategic decision not only aligns with our objective of integrating TIMAD into a blockchain framework but also sets the stage for future network expansion and broader adoption. Initiating the PoC with HAROPA PORT serves as a foundational step, demonstrating the practicality and potential scalability of our proposed solution.

Further to this, we have established an orderer organization, a critical component responsible for managing the ledger consensus, transaction ordering, and block creation within the network.

This aspect of our network architecture is distinct from other blockchain models and bears significant implications. In the maritime environment, where the presence of governmental entities and trusted authorities is paramount, our network design offers the flexibility to incorporate such entities in the future.

This approach aligns with the sector's governance structures and contrasts with the financial sector, where decentralized models are more prevalent. The use of a modular, permissioned network like HF provides a conducive framework for integrating these authoritative entities, thus reinforcing the network's credibility and aligning with the maritime sector's regulatory landscape.

Additionally, we have integrated another peer organization for simulation purposes. This organization is representative of a potential stakeholder within the maritime ecosystem, which could range from a harbour master involved in TIMAD to another entity operating a separate PCS or IS.

The inclusion of this additional peer organization, although not elaborated in detail at this juncture, is crucial for a comprehensive feasibility assessment. It serves as a prototype for potential stakeholders, illustrating the practical application of our blockchain integration and laying the groundwork for future demonstrations and onboarding efforts.

In essence, our PoC's organizational structure, encompassing HAROPA PORT as a peer organization, an orderer organization, and an additional peer entity for simulation, provides

a robust and adaptable framework. This framework is not only instrumental in validating the feasibility of our blockchain solution in the maritime domain but also positions us favorably for future expansions and collaborations, ensuring alignment with the unique operational and regulatory requirements of the maritime industry.

Orderer Organization Configuration The Orderer Organization, named Ordererharopa, is designated with the domain haropaport.com. This organization plays a critical role in the network by maintaining the ledger’s integrity and managing the consensus process.

The configuration parameter EnableNodeOUs is set to true, facilitating role-based access control within the organization through Node Organizational Units (OUs).

Ordererharopa defines specifications for its individual orderer nodes. These specifications include three distinct nodes, each with a designated hostname.

To secure communication within the network, Subject Alternative Names (SANS) are specified in the TLS certificates used by the orderer nodes. These SANS list the hostnames or IP addresses that can be used to identify the nodes, enhancing the overall security protocols.

TLS encrypts the data transmitted between nodes (such as peers, orderers, and clients), safeguarding it from eavesdropping, tampering, and message forgery. TLS uses X.509 certificates for authentication. When a node (like a peer or an orderer) connects to another node in the network, TLS certificates are used to verify the identity of the nodes communicating with each other. This verification process is essential to establish trust between nodes and to ensure that only authorized nodes can participate in the network. Also, it helps mitigating Man-in-the-Middle attacks which transcends the PoC to uphold industry standards.

Peer Organizations Configuration The network configuration includes two peer organizations: Orgharopa and Org2. Peer organizations are essential for endorsing transactions and maintaining the ledger, thus playing a pivotal role in the network’s operation. Each peer organization is associated with a unique domain delineating their distinct namespaces within the network. The EnableNodeOUs setting is activated for both peer organizations, indicating the implementation of Node OUs for streamlined and secure access control.

The template for peer nodes within each organization specifies the number of peer nodes (two for each organization) and their Subject Alternative Names (SANS), set to localhost. This setup facilitates efficient and secure local network communication. Additionally, the configuration details the number of user identities per organization, set to one for each. These user identities are integral for performing transactions and interacting with the blockchain network, representing their respective organizations in various network activities.

In the PoC for integrating blockchain technology within the maritime domain, particularly focusing on the integration with HAROPA PORT’s PCS, we have strategically configured the number of user identities within each organization. Specifically, we have limited this to one for HAROPA PORT as an initial setup, aligning with our innovative concept where the PCS itself

Chapter 6. Technical implementation - A blockchain infrastructure

acts as the primary blockchain user in the environment.

- **Leveraging Existing Business Logic** By having the PCS as the main blockchain user for the HAROPA PORT organization, we can effectively leverage the existing business logic of the PCS. This approach simplifies the integration process, allowing us to connect the PCS's operations directly to the blockchain network. It ensures that the transition to blockchain technology is seamless, requiring minimal changes to the current operational procedures within the PCS.
- **Streamlined Transaction Management** With the PCS acting as the primary user, all transactions related to HAROPA PORT's operations will be managed through the PCS. This setup not only streamlines the process of recording and endorsing transactions on the blockchain but also maintains consistency and efficiency in handling maritime logistics data.
- **Seamless Integration for Users and Stakeholders** By integrating the PCS as a blockchain user, we make the adoption of blockchain technology transparent to the end-users and stakeholders managed within the PCS. They can continue to interact with the PCS as they normally would, while the PCS handles the underlying blockchain transactions. This approach significantly reduces the learning curve and resistance to technology adoption, promoting a smoother transition to blockchain-based operations.
- **Scalability and Flexibility** While the initial configuration sets the number of users to one, the system is designed to be scalable. Additional user identities can be added as needed, allowing for more complex interactions and expanded use of the blockchain infrastructure. This flexibility ensures that the network can adapt to evolving needs and potentially integrate more stakeholders into the blockchain environment.

User vs node In HF, a user and a node represent distinct roles within the network. Users, which can be human administrators or applications (such as TIMAD), interact with the network but don't directly participate in its internal workings. They rely on valid digital certificates to submit transactions through client applications. On the other hand, nodes (of different types) are software instances running on computers that form the backbone of the network. This clear separation between users and nodes ensures a secure and well-defined workflow within the network.

By making the Port Community System (PCS) the primary user of a blockchain, we propose an innovative way to seamlessly integrate this technology into the maritime sector. This would enhance operational efficiency and transparency, extending benefits beyond localized areas to encompass the entire global supply chain. This strategic approach is both technically viable and aligns well with the maritime sector's needs, allowing us to leverage existing systems and

processes and offering the potential for future expansion and broader integration of blockchain technology.

The PCS, typically the central hub for stakeholder interactions in a port, benefits significantly from this integration. It not only preserves the existing user interaction models but also amplifies the system's capabilities by incorporating blockchain's key attributes, such as immutability, transparency, and security. This seamless integration, rooted in the existing business logic of the PCS, ensures minimal operational disruption and aligns with the principle of minimizing changes to user interfaces while upgrading backend systems. Such an approach is crucial for user acceptance and system stability.

Furthermore, the design's scalability is noteworthy. Initially positioning the PCS as the primary user is a deliberate move to validate the system's feasibility and effectiveness. As the system demonstrates its success, the network can evolve to include additional users representing varied stakeholders such as other IS (PCS, CCS, MSW, ...), thereby enhancing network interactions and capabilities. In maritime logistics, this strategy simplifies stakeholder management by allowing them to continue their usual interactions with the PCS, which, in turn, efficiently manages the complexities of blockchain interactions.

We recognize that while blockchain technology inherently promotes decentralization, the current maritime ecosystem is not yet mature enough to fully embrace this paradigm shift. In this sector, the governance role played by the PCS is crucial, and rather than eliminating their central function, it is more responsible and practical to leverage these systems to facilitate the adoption of blockchain technology and leverage its characteristics to achieve optimal traceability and accountability.

This approach echoes the challenges faced in implementing MSW systems in maritime logistics, where complexities in the system and communication barriers between different maritime entities have been evident. As long as the implementation of a MSW system remains a challenge, transitioning to a fully decentralized, trust-based communication model presents an even greater hurdle.

6.5.1 Permissions and roles

In the PoC we also leverage Membership Service Providers MSP along with the TLS responsible for identity management within our network. It issues and manages digital identities leveraging X.509 certificates for all participants, ensuring that only authorized and authenticated users can access the network and utilized in TLS communication.

Each organization within our network is assigned an MSP ID, directory and policies defining the roles and permissions and access controls. This is an important feature for the maritime sector, and its IS where not all stakeholders or actors have the same access within the network. It ensures only authorized entities can participate in certain transactions and have access to certain data on the network.

Chapter 6. Technical implementation - A blockchain infrastructure

The definition and partition within the network into different organizations with segregated components also reflect a strategy as it allows for modularity within the network and increased scalability. Each organization does not have to adhere to a common configuration used by the network but instead, it keeps its access and permissions and has them reflected within the network.

Certificates are generated by the CAs according to the MSP configuration, enrolled users will have corresponding cryptographic materials (public-private key pair and a certificate). The certificate will link the user's identity with their public key and is signed by the CA.

Additionally, this allows role-based access control where different users can have different roles.

The PCS will act as an admin and register users creating their identity on the network so that their transactions on the network can be recorded and linked with their credentials, identity and certificate. This allows the IS to assign specific roles to the users within the system at the time of registration based on the organization's access control policies.

We have implemented a strategic approach to policy assignment that effectively balances transparency, participation, and control within the network. This design is particularly tailored to the operational dynamics of the maritime sector and the role of the PCS. Here's a breakdown of the policy configuration and its implications:

- *Read and write privileges for users:* By granting users read and write privileges, we enable them to initiate and participate in transactions on the blockchain. This visibility allows all network participants to view transactional data, enhancing transparency and trust among stakeholders. This level of access ensures that stakeholders can actively engage in the network, contributing to and verifying transactions, which is essential for a collaborative and transparent blockchain environment.
- *Restricted Administrative Rights:* The administrative rights are reserved for the PCS itself, restricting the ability to perform administrative tasks such as network configuration changes, channel creation, or user enrollment within the blockchain network to the PCS. This control mechanism ensures that the PCS remains the central governing system within the network. It maintains the integrity and security of the network by limiting critical administrative functions to a trusted and centralized authority, which is crucial in a sector where regulatory compliance and operational continuity are paramount.
- *PCS as the Governing System within the organization HAROPA PORT:* The PCS, with its administrative privileges, retains the responsibility for creating and enrolling other users. This approach positions the PCS as the primary interface for stakeholders to interact with the blockchain network. Centralizing user management within the PCS simplifies the onboarding process for stakeholders and ensures that user enrollment follows established protocols and standards.

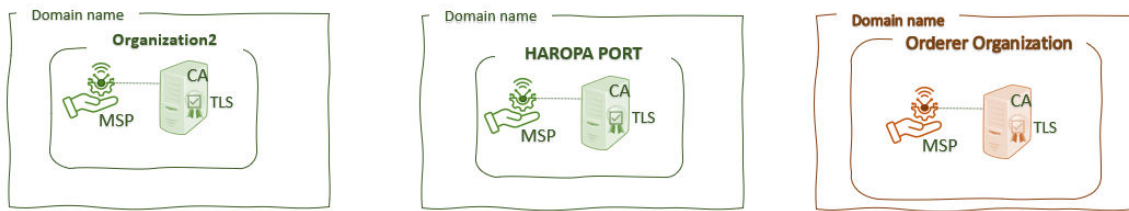


Figure 20: An illustration by the author of the created secure communication infrastructure

The resulting infrastructure at this state can be visualized in Figure 20 below presenting three distinct organizations.

This setup empowers us to leverage a unique configuration tailored for network interactions, offering the flexibility to customize according to the varying requirements of different organizations or additional environmental demands.

As we progress towards establishing the network, it is imperative to pre-define the corresponding configurations. The network capabilities are categorized into three distinct sections: Channel, Orderer, and Application.

Hyperledger Fabric's channel capabilities provide a powerful foundation for managing multiple, secure channels within a single network. Although our PoC focuses on using a single channel, the ability to create multiple channels is a key feature. Each channel functions as a separate ledger with its own set of participating organizations. This architecture allows organizations to create dedicated channels for different purposes. This enables them to control data sharing and ensure transaction privacy across a wide range of business operations and specific requirements.

And here we make a distinction between an application channel created by the organization that is part of the consortium network used for data exchange and transactions and system channels that, we the network administrator set in place to deploy the network shared ledger and add system-level components.

In the maritime sector, the deployment of a blockchain network equipped to manage multiple channels represents a significant leap forward. This technology is ideally suited to the sector's intricate and diverse nature, marked by an array of diverse stakeholders. Each of these entities has unique requirements for data sharing and privacy, which the blockchain's multi-channel architecture is adept at addressing.

The facility to create dedicated channels within the blockchain framework allows for distinct transaction types or data exchanges specific to the maritime ecosystem. For example, a channel could be uniquely configured to manage sensitive cargo information, with access restricted to authorized entities such as customs and security agencies. This level of confidentiality ensures compliance with international trade regulations while bolstering security.

The capacity to establish multiple channels within a blockchain network also directly addresses a crucial maritime sector challenge: the need for collaborative data sharing while pre-

serving organizational autonomy and maintaining data privacy. Each channel, operating independently with its own set of rules and members, enables organizations to engage in shared processes without the risk of exposing sensitive data or compromising their network integrity.

Although the base architecture of our PoC does not initially deploy this feature, the capability to create multiple channels is a fundamental aspect of our chosen blockchain technology. This feature allows for the development of separate ledgers where necessary, addressing concerns related to competition, security, and other critical factors.

Orderer Consensus - Raft In our blockchain architecture for the maritime sector, the Orderer organization plays a crucial role, particularly in the context of consensus mechanisms. We utilize a raft consensus protocol introduced in chapter two, which is a key component of our Orderer organization's functionality. To elucidate the feasibility of our PoC, we have integrated three nodes into the Orderer organization.

This algorithm is designed for distributed systems to ensure a consistent and replicated state across multiple nodes. It is employed to manage the ordering of transactions and the creation of new blocks in the blockchain. It ensures that all transaction records are consistently replicated across all nodes in the Orderer organization, maintaining the integrity and reliability of the network.

The consensus consists of electing a leader among the orderer nodes. This leader is responsible for managing the replication of transaction logs and the creation of blocks. All participating nodes in the Orderer organization communicate with each other to maintain a consistent state. If the leader node fails, a new leader is elected, ensuring the network's continuous operation. This mechanism provides fault tolerance and enhances the network's resilience, as it can continue functioning effectively even if some nodes encounter issues.

For our PoC, we chose to integrate three nodes within the Orderer organization to demonstrate the consensus mechanism's effectiveness and reliability. The integration of multiple nodes is a testament to the distributed nature of the network, showcasing how the blockchain can operate efficiently in a decentralized environment. These nodes collectively ensure that transactions are ordered correctly and that blocks are created and agreed upon democratically and reliably, reflecting the distributed and collaborative ethos of blockchain technology.

The selection of the Raft consensus mechanism for our blockchain architecture in the maritime sector is a strategic decision that aligns with the unique characteristics and requirements of this industry. The consensus in HF is pluggable and is per ordering service so if we implement different channels with different ordering services we can adjust the consensus based on the stakeholders' within the channel needs. Our choice of this particular consensus can be argued by the following:

- **Workflow Compatibility and Trusted Oversight:** In the maritime sector, operations often involve a range of stakeholders, including governmental bodies, port authorities, and private entities. The Raft consensus mechanism aligns well with this structure as it is

restricted to an organization that oversees the ordering of transactions. This organization can represent a trusted entity, possibly a governmental agency or a consortium of different nodes hosted by reputable institutions. The distributed nature of the consensus model ensures trust within the network while maintaining a centralized oversight for transaction ordering. This hybrid approach balances the benefits of decentralization with the need for trusted supervision in sensitive and regulatory-compliant maritime operations.

- **Trust and Controlled Decentralization:** Unlike the financial sector, where decentralization often aims to reduce reliance on central authorities like banks, the maritime sector operates on established trust among various stakeholders. Full decentralization might not be desirable or practical due to the complex regulatory and operational landscape. Our consensus leverages existing trust relationships while introducing distributed ledger technology. It allows for democratic participation in the network but within a framework that respects the sector's governance and trust dynamics.
- **Dynamic Leader Election:** The protocol includes a mechanism for electing a leader among the orderer nodes, responsible for transaction ordering and block creation. This leader is not static but can change, reflecting the dynamic nature of maritime operations where roles and responsibilities can shift. The ability to elect and rotate the leader node adds an extra layer of security and fairness, ensuring that no single node permanently holds control over the network. It mirrors real-world scenarios in the maritime sector where authority and responsibilities can be distributed among various parties based on expertise, jurisdiction, or other criteria.

Network nodes Following the development and establishment of cryptographic materials, configuration parameters, and organizational entities, network nodes were deployed as displayed in Figure 21. Docker containers were utilized to facilitate a streamlined deployment environment, suitable not only for the Proof-of-Concept (PoC) but also for potential production implementation, thereby simplifying onboarding maritime stakeholders. Each container encapsulated all dependencies and configurations necessary for node operation. Furthermore, docker-compose was employed within the PoC environment, enabling the execution of the entire network's container stack through a single command based on a pre-defined YAML configuration file that we wrote (a human-readable data serialization format used for configuration files and data exchange, characterized by its use of indentation to denote structure and support for complex data types). This file meticulously described the network architecture and facilitated efficient infrastructure management.

The inherent loose coupling fostered by containerization aligns seamlessly with the distributed nature of blockchain applications. Additionally, it ensures portability, consistency across versions, and isolation, thereby enhancing overall system reliability. Notably, the same docker-compose file can be readily adapted for production servers, further streamlining deployment

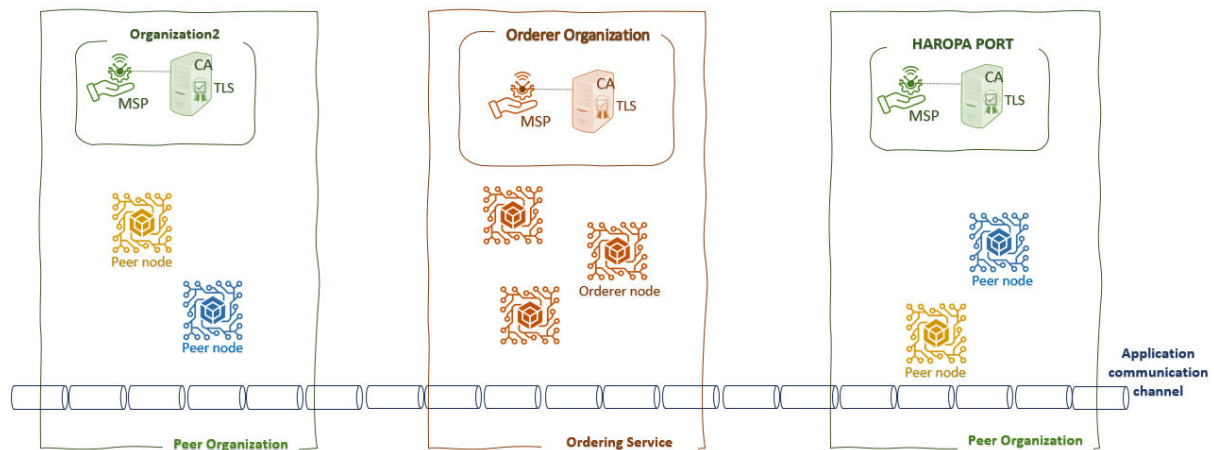


Figure 21: An illustration by the author of the created blockchain infrastructure

upon transitioning from PoC to a live environment. The containerized approach also grants the flexibility for rapid scaling of peers when necessary.

As previously delineated, the consensus mechanism leverages a Raft cluster consisting of three ordering nodes responsible for transaction ordering and block creation. Each peer organization within the network is represented by two dedicated peer nodes. These fundamental elements host ledgers and smart contracts, facilitate application interaction, and execute chaincode transactions against the ledger. The presence of multiple peers promotes redundancy and facilitates increased transaction processing capacity. Each peer is accompanied by a dedicated embedded CouchDB container serving as the state database, ensuring the continuous maintenance of the current ledger state. Peers actively query CouchDB throughout transaction validation and ledger updates.

The gossip protocol underpins peer discovery, transaction and block dissemination, and peer data synchronization. This protocol serves as the backbone for peer-to-peer communication within the decentralized network. To guarantee secure communication and verified participant identities, TLS certificates issued by designated Certificate Authorities (CAs) are employed for network entity authentication and traffic encryption. The containerized approach enables seamless scaling of peers and orderers as required, while the inherent modularity fosters flexibility, performance, and resilience - key attributes for commercially viable decentralized applications.

Into the decentralised chained data The structure of blockchain technology, particularly in the context of HF, forms the critical foundation enabling its core functionality and reliability. As described previously, the chained data structure common to any blockchain entails grouping transactions into blocks. In HF, to ensure deterministic ordering, these transactions are sequenced within blocks by an authorized set of nodes functioning as the ordering service, which we have deployed. The block structure contains a header storing essential metadata, and a body holding the transactions.

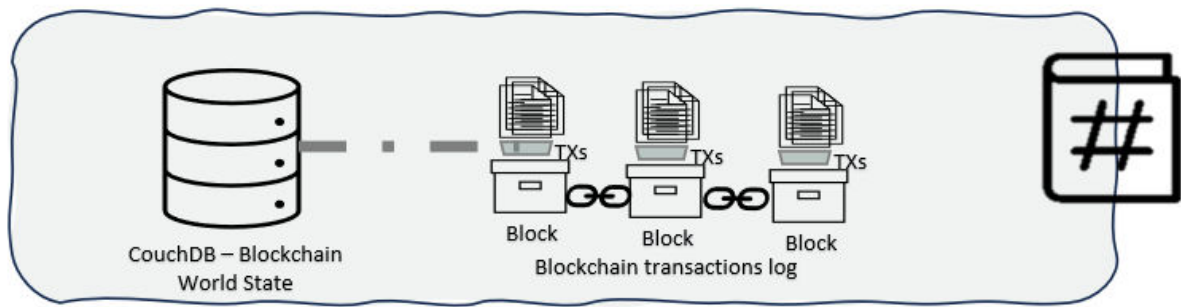


Figure 22: An illustration by the author of each peer ledger’s components

The vital block header houses reference hashes linking to previous blocks, Merkle root hashes representing the transactions, timestamps, and cryptographic signatures, chaining the blocks chronologically. However, HF utilizes a distinct decentralized approach regarding ledger distribution and peer node roles. Unlike permissions-less blockchains copying full ledgers to all nodes, HF facilitates selective data sharing aligning with privacy needs.

Each HF peer node maintains a subset of the full ledger about its authorized channels rather than the complete dataset. Transactions are disseminated between relevant peers using an efficient gossip protocol for peer-to-peer transmission. By sharing transactions and blocks within channels, peers collaboratively validate and append to their ledger subsets, avoiding unnecessary replication across the network and enabling scalability. Peers thus retain only the transaction history immediately relevant per their channel roles.

Additionally, each peer persists in the current state of its accessible transactions in a World State as elaborated in Figure 22 – an indexed ledger state database. While the immutable ledger records full history, the World State represents assets’ latest values. Chaincode applications execute transactions against this World State, generating resultant data recorded to the ledger. Efficiently partitioning historical and current states enables rich data constructs suitable for enterprise blockchains. World State updates synchronize across channels via the same gossip protocol, ensuring consistency in the decentralized network. Peers contribute to this shared ledger and World State per their authorized channels and roles. For example, endorsing peers execute chaincode transactions while committing peers append new blocks. Hence, HF’s decentralized structures governed by cryptographic consensus support extensive blockchain use cases, crucial for global industries like maritime. The complex logistics and transactions therein require integrity, traceability, and efficient state updating provided by this combination of the blockchain and World State architecture.

About peer nodes In the previous discussion, we referenced endorsing peers, one specific type of peer node in Fabric’s architecture. This leads to delineating the distinction between the various nodes. As covered previously, orderer nodes run the consensus protocol and create new blocks. However, peer nodes fulfil separate duties and consist of two main subtype conformations

- endorsing peers and validating (or "committing") peers.

Endorsing peers execute chaincode and simulation transactions against their local replica of the world state. By generating transaction endorsements that record the resultant state changes, these peers essentially "endorse" transactions as having been processed correctly. Multiple organizations may operate endorsing peers to provide decentralized endorsement for transactions within a channel or network. These peers are responsible for the execution of the smart contracts within the network which restricts the logic responsibility in the network to authorized nodes that we have configured. This is beneficial in the maritime context, particularly for our application, as we do not expose the PCS logic to unauthorized entities.

In contrast, committing peers append validated blocks irreversibly to the blockchain while updating the world state. Thus, they identify the accountable parties and authenticate signed changes, while not retaining access privileges to the smart contract logic itself. Committing peers also maintain the authoritative world state subsequently used in future chaincode executions. Like endorsing peers, multiple committing peers strengthen resilience via decentralization and redundancy.

This division of labour between node types facilitates scalability while retaining security assurances. Endorsing peers focus on transaction simulation and endorsement generation, enabling computationally intensive smart contract execution isolated from ledger maintenance and consensus duties handled respectively by committing peers and orderers. Organizations flexibly assign peer subtypes like endorsing or validating peers based on their infrastructure resources and trust roles within applicable channels. Hence, Fabric's node differentiation empowers customizable deployments suiting diverse blockchain use cases and trust models.

Endorsement policies Endorsement policies govern the number of peer endorsements required for transaction validation. These policies provide a flexible means of specifying endorsement rules for different smart contracts and channels. In our proof-of-concept, we configured a majority endorsement policy requiring endorsements from a majority of two peers per organization. However, endorsement policies can mandate more complex signing rules using "AND" and "OR" logic toward different identity classifications. For example, maritime use cases could leverage a policy demanding signature intersection across ship operators, ports, and regulators to provide multi-party transaction integrity. Alternatively, endorsement policies with "OR" clauses facilitate endorsement redundancy from identities fulfilling similar consortium roles. Hence, production systems could mandate endorsements from two of the three major shipping companies on a given channel. By customizing endorsement rules, we can support varied trust models across scenarios requiring different sign-off protocols. This reconfigurability and policy enforcement bolsters maritime solutions spanning complex supply chain interactions and multi-party information exchange.

We connected the whole thing on a channel configured as explained above and secured in its genesis block. We have also assigned to anchor peers, one per each organization.

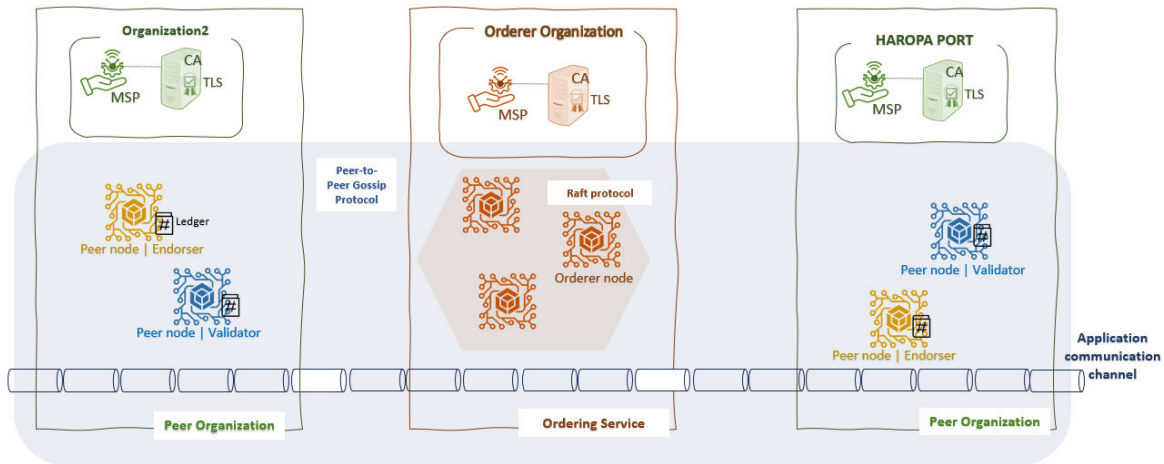


Figure 23: An illustration by the author of the full created blockchain infrastructure

When a peer needs to communicate with a peer in another organization within the same channel, it uses the anchor peer as an entry point rather than attempting to discover the entire network. The anchor peer nodes have persistent connections to other organizations' anchor peers, enabling peers to transmit transactions and blocks across organizational boundaries. We have assigned one anchor peer for each organization when configuring our network channel. These anchor peers essentially serve as communication conduits, facilitating the cross-organizational interaction necessary in multi-party blockchain networks. The gossip protocol leverages the anchor peers to disseminate transactions and ledger data to the appropriate peers across the different organizations.

Using anchor peers thus helps optimize peer discovery and communication in fabric networks with many organizations. They will play a key role in enterprise blockchain solutions for the maritime industry where transactions span numerous shipping companies, ports, customs authorities and other parties.

Now that we have established our PoC infrastructure components we can then connect the whole and create our blockchain. This configuration is elaborated in the Figure23.

we meticulously delineated the integration of blockchain technology into the maritime sector, focusing on the conception and deployment of a blockchain infrastructure that aligns with the operational dynamics of PCS like TIMAD. By leveraging HF, we established a secure, permissioned blockchain environment that respects the intricate relationships and data exchanges intrinsic to maritime logistics. We underscored the importance of data notarization for critical elements such as stakeholder identifications and cargo manifests, thereby enhancing the transparency and accountability of maritime logistics operations.

TIMAD ORIENTED BLOCKCHAIN DEVELOPMENTS

Contents

7.1	About the network’s workflow	130
7.2	PCS Blockchain liaisons	130
7.3	Blockchain functioning logic	132
7.3.1	Into Smart contracts	133
7.4	Client targeted development TIMAD	137
7.5	Seamless Integration of Blockchain Infrastructure	144
7.6	User-Centric Ledger Interaction within TIMAD	146

In the preceding section, we detailed the implementation of a network architecture conducive to the maritime sector’s requirements, integrating orderer and peer nodes with meticulous consideration for roles, permissions and security protocols. As we transition from blockchain infrastructure to leveraging it to address specific operational challenges, we pivot towards smart contracts.

The laid technical foundation allows us in this chapter to focus on the practical application of blockchain technology within the TIMAD system, a PCS, and a critical component of the maritime logistics ecosystem.

This chapter explores the development and implementation of smart contracts—programs stored on the blockchain specifically designed to address the nuanced requirements of maritime logistics operations managed by PCS like TIMAD.

At the heart of this chapter is the strategic development of smart contracts for notarizing the BAT management process and enhancing the transparency and traceability of the manifest within the PCS. These smart contracts serve as the operational link between the blockchain infrastructure and the TIMAD system, facilitating secure and immutable record-keeping of actions and data pertinent to maritime logistics operations.

Moreover, We detail the development of a user-centric interface within TIMAD that allows stakeholders to interact with the blockchain-secured data seamlessly. This interface ensures that the integration of blockchain technology enhances the user experience by providing additional layers of data verification and trust without disrupting established workflows.

Through the lens of practical application within the TIMAD system, we underscore the transformative potential of blockchain technology in the maritime sector. It highlights the meticulous approach taken to ensure that the benefits of blockchain—immutability, transparency, and enhanced security—are realized in a manner that complements and enriches the existing maritime logistics infrastructure.

7.1 About the network's workflow

While leveraging some peer-to-peer (P2P) blockchain concepts, Hyperledger Fabric's architecture introduces key differences. Transaction validation involves a unique endorsement process by peers, followed by dedicated orderer nodes achieving consensus on transaction order.

Endorsing peers execute smart contracts, simulating transactions against their local ledger state replica. They generate endorsed transaction results recording state changes, effectively validating transactions as correctly processed - ensuring integrity across the decentralized network.

Endorsed transactions are then communicated to orderer nodes, which achieve consensus on the transaction order - crucial for preserving consistency and chronology impacting data validity.

Following consensus, validator nodes validate transactions by agreed-upon rules, appending them to the blockchain to update the ledger state reflecting the latest agreed-upon network state.

Finally, a gossip protocol facilitates efficient block dissemination across the network, allowing all nodes to maintain a consistent, synchronized ledger view regardless of their role.

7.2 PCS Blockchain liaisons

The PCS as defined in our configuration will be a client within the HAROPA PORT organization as defined per the previous chapter. This client should be able to interact with the blockchain infrastructure we created. For this, we need to address two developments:

- Blockchain functioning logic | Smart contracts
- Client targeted interface | TIMAD

Identifying TIMAD as a user of the organization, aligns with the initial configuration detailed earlier. This strategic placement of TIMAD within the PoC framework is not arbitrary but is underpinned by a series of calculated decisions aimed at ensuring effective integration and functionality.

A primary objective was to achieve seamless integration of this advanced technology into the existing maritime information systems. The intention was to avoid the introduction of drastic changes or unfamiliar technologies into the established systems. To this end, a simple API request within the PCS was identified as the most suitable method for enabling communication with the

blockchain. This approach ensures that the integration is not only technically feasible but also user-friendly.

Furthermore, this method of integration offers a dual layer of security. Firstly, since the request originates from the PCS, it adheres to the PCS's stringent security standards. Secondly, the inherent security features of the blockchain are also applied, thereby providing a robust safeguard against potential vulnerabilities. This dual securitization mechanism enhances the overall security posture of the system, making it more resilient to threats and breaches.

Additionally, the implementation includes JWT (JSON Web Token) authorization on the server.

JWT a prominent mechanism for secure information exchange between parties within a distributed system. They function as self-contained units comprising three Base64 encoded parts: a header specifying the token type and signing algorithm, a payload carrying user claims or request details (not encrypted but verifiable through the signature), and a cryptographic signature ensuring data integrity and preventing tampering. The signature itself is generated using a secret key known only to the issuer (token creator) and verifier (who validates the token).

This authorization is in alignment with the certificates generated by the PCS's organization CA and MSP. This setup is instrumental in controlling who can access what information and maintaining a stringent access list. By employing JWT authorization, the system ensures that only authenticated and authorized users can interact with the blockchain, thus maintaining the integrity and confidentiality of the data and transactions within the maritime logistics ecosystem.

By using the API server we abstract the complexities of the blockchain network away from maritime stakeholders and keep only needed API request adjustments within their IT, a technology already largely common in the maritime sector. And it is the server that takes care of any blockchain intricacies.

As a result, we would need to develop the exposed API endpoints in a REST API server secured with the JWT tokens. This server interacts with the blockchain using a Fabric SDK.

REST API Servers represent a widely adopted architectural style for application programming interfaces (APIs). They adhere to a set of guidelines that promote communication standardization and interoperability between different software components. REST APIs leverage the ubiquitous HTTP protocol, utilizing familiar methods like GET, POST, PUT, and DELETE to interact with resources.

For this, we chose Node.js with Express as Node.js is known for its efficiency and scalability in handling asynchronous operations, which are commonplace in network communications and interactions with blockchain.

This choice of technology stack elaborated in Figure 24, Node.js with Express for the server-side application, coupled with JWT for security, and Fabric SDK for blockchain interaction – represents a well-considered approach. It aligns to integrate blockchain technology into the

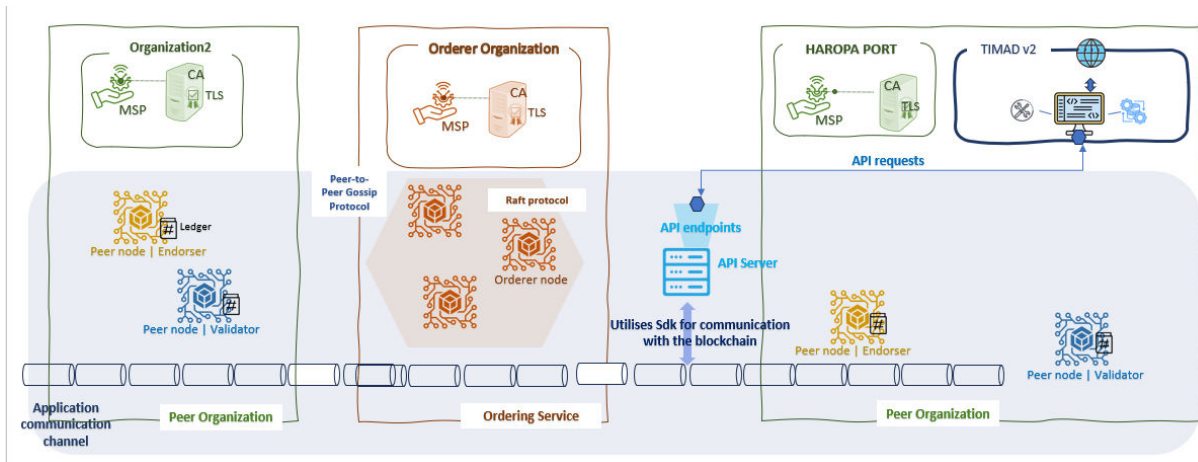


Figure 24: An illustration by the author: Timad as a client application within the secure blockchain environment

maritime sector in a manner that is both technologically advanced and user-friendly. This strategy ensures that the adoption of blockchain within the maritime logistics ecosystem is not hindered by technological complexity, but rather facilitated by the familiarity and simplicity of the API-based interaction model.

7.3 Blockchain functioning logic

The interaction between the server and the ledger is facilitated through smart contracts.

To notarize the relevant data specified in Chapter Five (BAT access data and Manifest data), the development of corresponding smart contracts is essential. These smart contracts will be coded to specifically handle the types of transactions and data exchanges that are pertinent to the maritime logistics operations managed by the PCS. Executing these contracts will rely on blockchain technology and its consensus protocol, which ensures efficient operations in terms of speed, costs, and transparency.

It is important to note that the execution of a smart contract relies on the existence of the required conditions on the blockchain. This means that the transactions are only executed if the necessary criteria, as defined in the smart contract, are met on the blockchain. Therefore, the development of these smart contracts must take into consideration the specific requirements and operational nuances of the maritime sector, particularly those related to the PCS.

The smart contracts will be designed to interact with the server, which in turn communicates with the blockchain network. This setup allows for a streamlined process where the server handles the complexities of the blockchain interactions, while the smart contracts ensure that the data related to the PCS is accurately and securely notarized on the ledger. This approach not only simplifies the integration of blockchain technology into the maritime sector but also enhances the security and efficiency of the PCS's operations.

Within the scope of this thesis, it is recognized that the distributed ledger technology lever-

aged in the blockchain network enables two-way communication capabilities. Inherent to this infrastructure is the functionality to enforce data inputs into PCS or trigger events based on predefined conditions coded into smart contracts. However, the development efforts presented herein deliberately focus primarily on the notarization functions to meet the core objective of enhancing accountability through an immutable record of maritime logistics data as it is the lacking feature.

This strategic choice to restrict the initial development scope centres on notarization functions that directly target manifest processes, contributing to the overarching goal of accountability improvements in the sector. The notarization mechanism available through blockchain technology allows for the transparent and tamper-proof recording of data, significantly bolstering traceability and answerability among stakeholders. Given that the existing PCS systems such as Timad have thoroughly integrated business logic coded by maritime partners, reinventing these established information workflows is deemed redundant and potentially counterproductive to promote adoption. Since PCS implementations vary widely across ports, custom-coding business logic would also limit interoperability and universal applicability, diminishing the effectiveness of the solution.

While the two-way communication abilities and smart contract layer of the blockchain ledger could enable valuable future capabilities like automated data feeds into the PCS or event triggers, these functions extend beyond the current scope focused on accountable notarization.

As the project matures, exploring these features could further optimize processes and confirm the full potential of blockchain technology across maritime logistics. Such development would build on the foundation established herein, integrating additional information systems and progressively working toward a decentralized infrastructure aligned with industry standards.

The customizable smart contract layer presents opportunities to code bespoke business logic and governance policies that connect stakeholders across a common blockchain network.

7.3.1 Into Smart contracts

A key contribution of our choice to use Hyperledger Fabric is the concept of chaincode, which differs subtly from the notion of smart contracts commonly used in blockchain systems. Smart contracts do not execute directly on the distributed ledger itself. Rather, they run within a secure execution environment called a chaincode container on each peer node participating in the relevant channel. This provides a security advantage for the network, as faulty smart contract code does not get directly executed on the shared ledger.

The chaincode infrastructure ensures reliability through an encapsulated execution process. It defines the general rules and processes for interacting with the ledger, setting up transaction validation, access control, and communication protocols for the network.

A smart contract, by contrast, represents a specific agreement for a given scenario, like an application on a phone. It comprises code within the chaincode that focuses on automating a

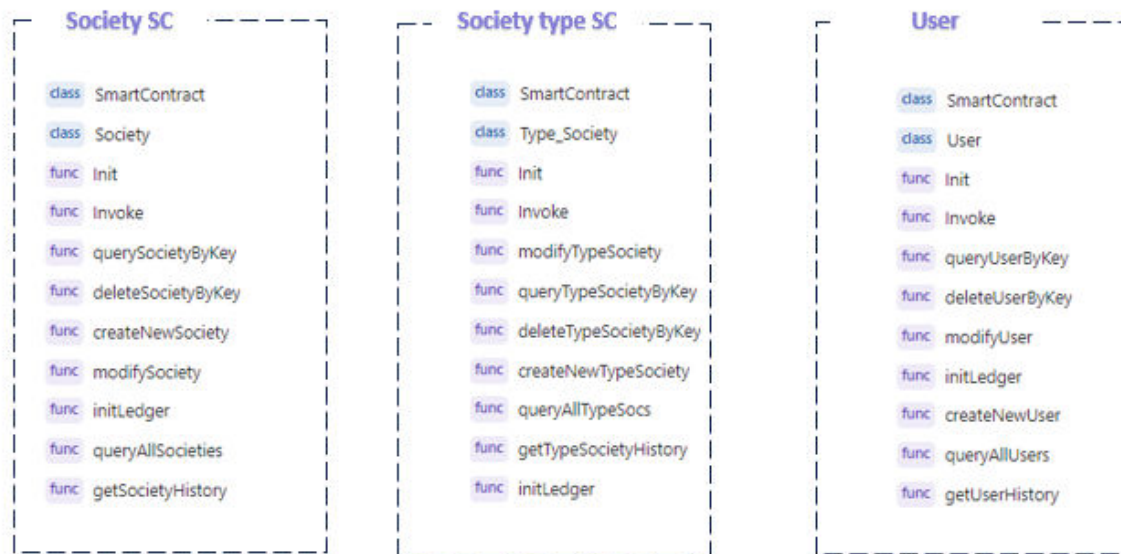


Figure 25: Bat Smart contracts

particular workflow such as PCS incoming events. The smart contract leverages the chaincode functionality to access relevant data (e.g. ship arrival), evaluate conditions (ship granted access to the port), and execute actions (notarize the manifest).

This separation of concerns into chaincode and smart contracts enables isolation and prevents malicious contract codes from affecting the integrity of the underlying ledger. The chaincode provides a secure, managed environment for smart contracts to execute business logic on the peer nodes.

In the context of enhancing traceability within TIMAD and following a thorough code review and analysis, it was determined that for the notarization of the BAT management process within PCS and manifest, four relevant chaincodes, and consequently four corresponding smart contracts, need to be implemented within the PoC .

Three of these chain codes are specifically related to the access management within the dangerous goods dedicated PCS and traceability of the BAT access (cf. Figure25). These smart contracts are designed to handle various aspects of administrative management of societies within the PCS, such as its creation, modification, and deletion and all associated actions. The implementation of these smart contracts will enable the seamless and secure handling of BAT-related transactions within the blockchain environment. This approach not only enhances the traceability and accountability of the BAT transactions but also integrates these processes more effectively into the maritime logistics workflow.

The fourth chaincode (cf. Figure 26). is dedicated to manifest control directly related to dangerous goods and their traceability within the PCS. The manifest smart contract is crucial for tracking the movement and status of goods, which is a key aspect of maritime logistics. By incorporating this smart contract into the blockchain network, the PCS can achieve a higher level of accuracy and transparency in the tracking and recording of manifest data.



Figure 26: Manifest Smart contract

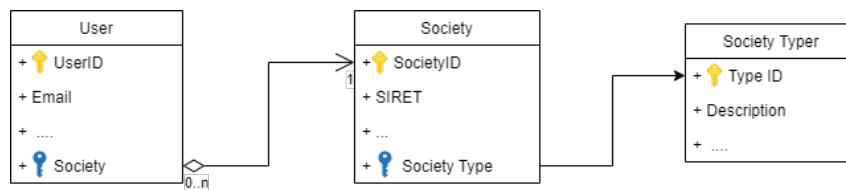


Figure 27: BAT Access logic within PCS systems

These smart contracts aim to improve accountability and traceability in maritime logistics by automating and securing critical notarization processes related to BAT and manifest handling.

Their implementation within the PoC is a strategic step towards realizing the full potential of blockchain technology.

To effectively code smart contracts that notarize PCS-related data, it is essential to have a comprehensive understanding of the relationships between different entities within the PCS. This understanding is crucial as it directly influences how the smart contracts will manage and govern interactions and transactions within the system.

In the context of the BAT access process, as outlined previously, a society or organization within the PCS obtains its credentials through the PCS portal. These credentials are necessary for the society to be created and gain access within the PCS framework. Once these credentials are obtained and the society is integrated into the PCS, it is then accorded an administrative account.

This administrative account plays a pivotal role in managing the internal hierarchy and operations of the society within the PCS. It enables the entity to manage its users, each with specific roles, access rights, and permissions (cf. Figure 27). The smart contracts must be designed to recognize and enforce these varying levels of access and authority. This includes ensuring that transactions and interactions within the PCS are executed on the predefined roles

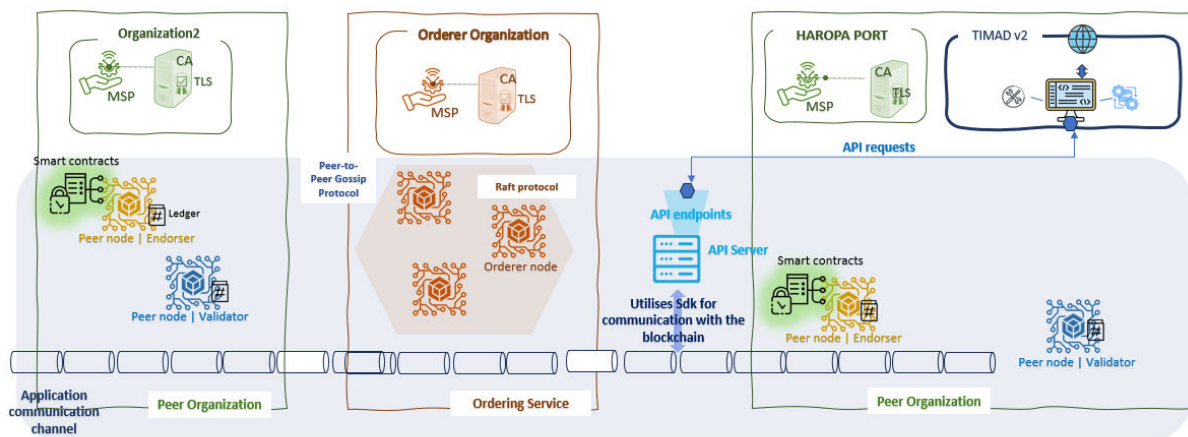


Figure 28: Manifest Smart contract

and permissions associated with each user or entity.

The smart contracts in the blockchain framework are not directly responsible for managing roles and permissions. Instead, these roles and permissions are outlined by the chaincode to ensure coherence with the PCS. It's up to the PCS to enforce these roles and permissions, while the chaincode mirrors them within the blockchain framework.

This approach indicates that the primary objective of smart contracts is to fill a gap in the current PCS functionalities, focusing specifically on ensuring the notarization of actions. For example, this includes recording actions such as the creation, modification, or deletion of users by the admin of a particular society within the PCS. By notarizing these actions on the blockchain, the system can maintain a record of accountability that is currently lacking in the PCS.

These smart contracts, once coded, are deployed within the blockchain network. The specific algorithms used for these processes can be referenced in (AppendixA), providing a detailed view of the underlying logic and structure of these smart contracts. They are deployed on the endorsing peers within the blockchain network. This ensures that they are executed according to the network configuration and the related endorsement policies. Endorsing peers are responsible for executing these smart contracts, simulating the transactions, and generating the necessary endorsements that validate the transactions as being processed correctly (Figure 28).

The decentralization aspect of the blockchain ensures that the governance of these records is in the hands of trusted entities, which in turn enhances transparency and reliability. The decentralized nature of blockchain technology offers a robust solution for maintaining an immutable and transparent record of actions within the PCS, thereby significantly improving governance and trust in the system.

Consequently, we highlight a novel application of blockchain technology in maritime logistics utilizing the above-developed smart contracts. This strategic implementation leverages the

strengths of blockchain technology to address specific challenges in the PCS, showcasing the potential of blockchain in enhancing the operational integrity of maritime logistics systems.

7.4 Client targeted development | TIMAD

Now that the infrastructural liaison between the blockchain and the server is all set, we leverage an HF software development kit (SDK). It is utilized to establish a connection with the infrastructure based on the network connection profiles that delineate the peer's organisational structure and their anchor peers.

We have developed the exposed API points within our server that provide the interface for our PCS to interact with the underlying smart contracts.

The server handles responses from the network, returning them to the clients in a JSON format. By employing Express as the web framework and body-parser for JSON parsing, the server offers a robust and efficient communication layer for exploiting the distributed ledger capabilities of HF.

The server implementation demonstrates the seamless integration of a blockchain with application logic, paving the way for diverse blockchain-based applications and functionalities. Where it only suffices to include these API calls asynchronously within the existing IS.

To first participate in Timad's network you will have to Sign up if you don't already have an account ([Inscrivez-vous ici](#)) (Figure 29).

This will redirect you to a page that notifies the stakeholder about the BAT access. The stakeholder is prompted that he is about to create a company manager account and you will be responsible for your society hierarchy within the system. The request, if accepted, will add your company to the TIMAD v2 system and make you the manager. You will need to add your employees yourself (Figure 30).

By agreeing to the creation of your society within TIMAD and having a manager account you will be redirected to a page to fill in your society data and legitimate credentials to be verified by the system and authorized parties (Figure 31).

When the society is successfully approved and created, through an API call to "Register user" the PCS will register the manager with his email address as username, organization, and organization domain.

Upon the successful creation of a society within the TIMAD network, the PCS initiates an asynchronous call to the blockchain via the API endpoint on our Node server (cf. Figure 32), to facilitate the registration of the new manager. This process is pivotal in establishing the manager's identity and authority within the system. The asynchronous nature of this function is

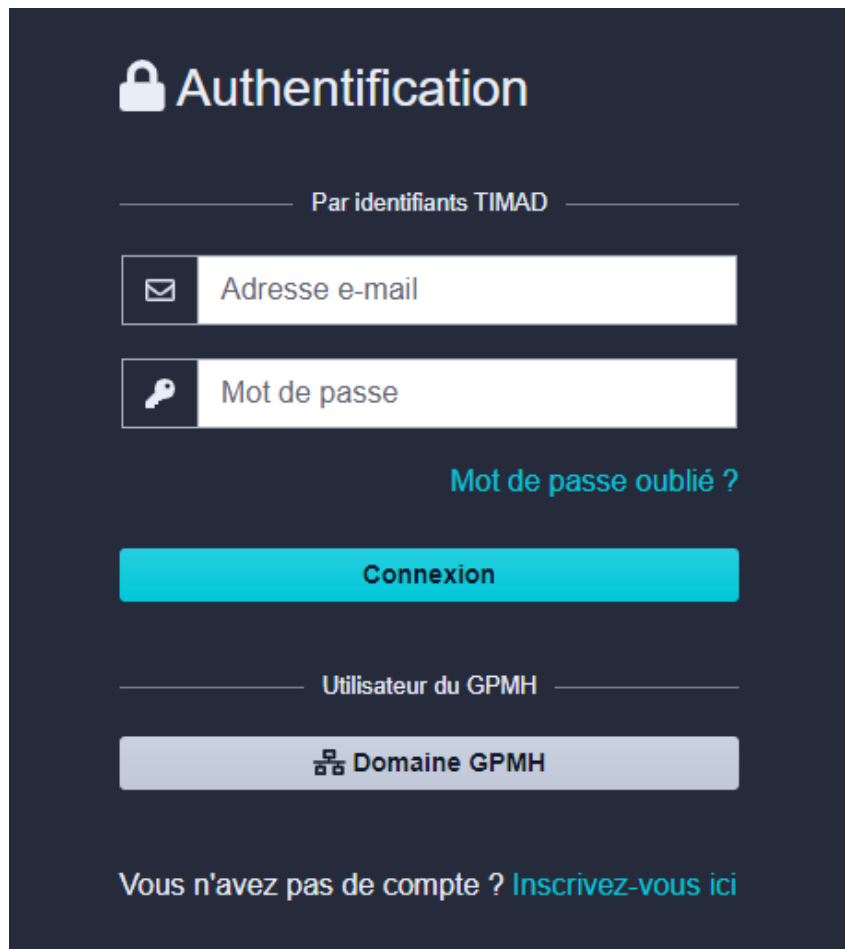


Figure 29: First Time Connecting to TIMAD - Default connection page



Figure 30: First Time Connecting to TIMAD - BAT access prompt

The image shows a dark-themed web form titled "Création de compte". The form contains the following fields from top to bottom:

- Société
- Numéro de SIRET
- Numéro EORI
- Type de société (dropdown menu)
- Adresse
- Code Postal
- Ville
- Complément d'adresse
- Téléphone (with a dropdown menu showing the French flag)
- Prénom
- Nom
- Adresse Email

At the bottom of the form is a red button labeled "S'enregistrer".

Figure 31: First Time Connecting to TIMAD - Society creation

Chapter 7. Timad Oriented blockchain developments

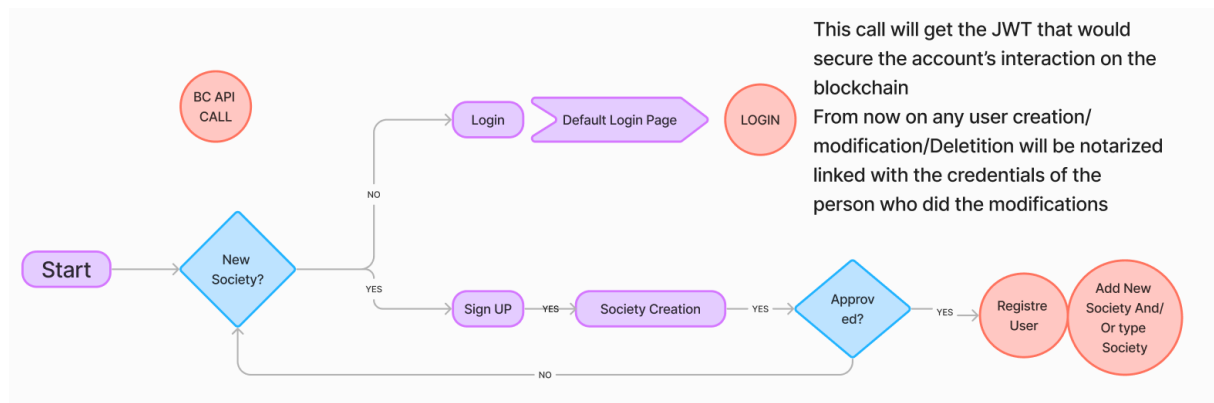


Figure 32: Society creation : A Seamless blockchain workflow integration woven into the fabric of the PCS

crucial, as it allows for the operation to be executed without blocking other system processes, thereby maintaining the efficiency and responsiveness of the overall system.

During the registration phase, a critical interaction occurs with HAROPA Port's Certificate Authority (CA). This interaction is essential for generating a digital certificate for the manager account, aligning with the specified permissions and roles required for the manager's activities within the PCS. The certificate creation process is a fundamental step in ensuring that the manager's actions within the system are securely authenticated and authorized.

Subsequently, a wallet is created for this new manager. The wallet serves as a secure repository for the manager's cryptographic materials and the X.509 identity object. The X.509 standard is a crucial component in this context, as it provides a framework for public key certificates and a robust method for validating the manager's identity. The wallet's integration with the manager's digital certificate and cryptographic materials ensures that all subsequent actions made by the manager within the PCS are securely signed, thereby maintaining the integrity and authenticity of these actions.

Furthermore, the system proceeds to generate corresponding JWT for the manager. JWTs are an integral part of the security mechanism, providing a compact and self-contained method for securely transmitting information between parties as a JSON object. This token will be used to authenticate and authorize the manager's interactions with the PCS, ensuring that each action is not only traceable but also compliant with the established security protocols.

Other than the login using the credentials and the first registration all the rest of the API endpoints that interact with the blockchain are secured with the JWT-certificate combination.

The rest of the endpoints are associated with the smart contracts logic. When the manager account through the PCS login a temporary JWT token is sent back to the PCS by the server that would allow for the manager account to interact through the PCS with the underlying blockchain infrastructure. We intercept the incoming request and filter any unauthorized, restricted allow to notarize the manager's actions within the PCS: Any user creation deletion, and modification

is recorded on the blockchain utilizing the smart contracts with the identity of the person who made the notification extracted from the JWT token and authenticated and authorized according to the account wallet.

The initiation of a society within the TIMAD network, facilitated by the PCS, constitutes a significant action that is meticulously recorded on the blockchain ledger. This recording process is a testament to the system's commitment to transparency and accountability. The creation of a society is not merely an administrative entry; it represents the establishment of a new entity within the maritime logistics ecosystem, with its own unique set of users and operational dynamics.

Following the society's creation, a manager account is generated by the PCS. This account plays a pivotal role in overseeing and managing the society's users. It is equipped with functionalities that enable the manager to administer user roles, permissions, and activities within the society. The actions taken by the manager, ranging from user management to operational decisions, are transparently recorded on the blockchain ledger. This unalterable ledger serves as an immutable record of all transactions and activities, ensuring that every action is traceable and verifiable.

These recorded actions are endorsed by the PCS organizations on the blockchain since it's through the PCS these changes are made and authorized parties. It involves the verification and validation of the actions by entities that have been granted the authority to do so within the network. This endorsement process upholds the integrity of the data and actions recorded on the ledger.

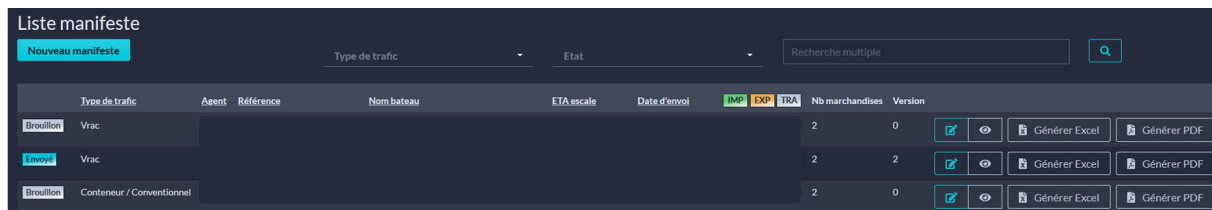
Once endorsed, the actions are subjected to the ordering service. The ordering service is responsible for sequencing the transactions and ensuring that they are consistently ordered across all nodes in the network. This service plays a critical role in maintaining the chronological integrity of the ledger, a feature essential for the accuracy and reliability of the recorded data.

Finally, the validated transactions are committed to the nodes of the blockchain network. This step marks the completion of the transaction process, as the actions are now indelibly recorded on the ledger. The nodes, in this context, serve as the custodians of the blockchain's history, maintaining a complete and accurate record of all activities and transactions.

We reiterate the primary objective of notarization in this integration, as the process, for the time being, remains asynchronous with the PCS's existing operations. This approach is deliberate; it does not interfere with the core business logic of the PCS. Instead, it adds an accountability layer, anchoring the transformative features of blockchain technology. By doing so, we augment the existing system with an additional dimension of security and traceability, enhancing the overall governance and integrity of maritime logistics operations without disrupting their established workflows.

Similar to the previously described notarization logic, the management of the manifest within the PCS is facilitated through the TIMAD system. Users interact with TIMAD to perform the range of operations described in Chapter 5 on the manifest, including adding, modifying, or

Chapter 7. Timad Oriented blockchain developments



Type de trafic	Agent	Référence	Nom bateau	ETA escale	Date d'envoi	IMP	EXP	TRA	Nb marchandises	Version		
Brouillon	Vrac								2	0		
Envoies	Vrac								2	2		
Brouillon	Conteneur / Conventionnel								2	0		

Figure 33: Manifest related Operations via TIMAD - Manifests List

deleting manifest data submitted for approval port authority agent through TIMAD (cf. Figure33). This interaction is a crucial aspect of maritime logistics operations, enabling stakeholders to maintain accurate and up-to-date records of cargo and shipments.

To ensure these operations are securely and efficiently managed, TIMAD employs restricted API calls. These calls are the conduits through which users interact with the underlying blockchain infrastructure. The restricted nature of these APIs is a deliberate design choice, ensuring that access to manifest-related functionalities is controlled and secure. This approach aligns with the overarching need for security and data integrity in maritime logistics.

Additionally, when a user, through the PCS, initiates an action related to the manifest—be it addition, modification, or deletion—TIMAD processes this request and interacts with the corresponding chaincode on the blockchain. The chaincode, in this scenario, is responsible for creating and maintaining a trace of these manifest-related actions along with the identity of the doer within the secure blockchain environment. This trace serves as an immutable record of all changes made to the manifest, providing a transparent and tamper-proof history of transactions.

This integration of PCS and TIMAD with blockchain technology for manifest management exemplifies the application of blockchain for enhancing operational efficiency and accountability in maritime logistics. By leveraging chaincodes to record manifest changes on the blockchain, the system ensures that all manifest-related actions are not only traceable but also securely stored within a decentralized framework. This approach enhances the reliability and integrity of the data within the PCS, reinforcing the system's capability to manage complex logistics operations in a transparent and accountable manner.

These API calls can be categorized into four types:

- Authentication APIs (cf. Figure 34): The Register user API allows the PCS to create a trace of the society manager creation and approval within the system. It creates a wallet storing its cryptographic materials according to the PCS's (HAROPA PORT) configured access rights for this type of account on the blockchain. The login API will extract the user's information, check its legitimacy and grant him through the PCS a JWT token that allow him to interact with the chaincodes.
- API responsible for appending data on the ledger (cf. Figure 35): These API will create

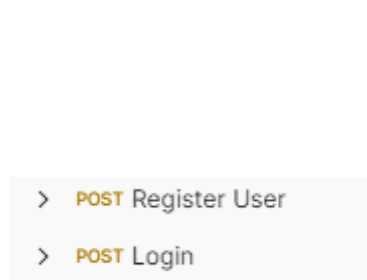


Figure 34: Auth API

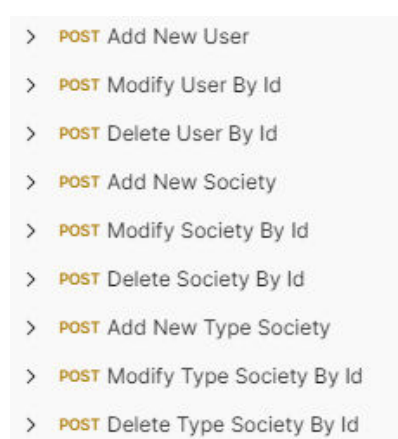


Figure 35: POST API

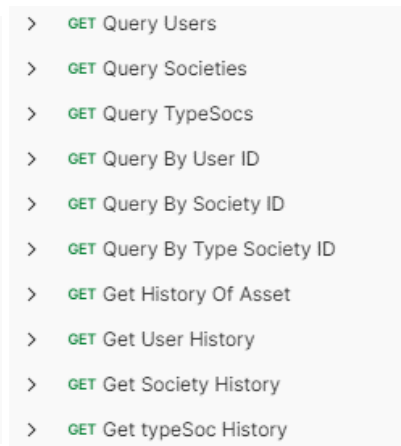


Figure 36: Get API



Figure 37: Blockchain related requests

a trace of the society manager's action on the ledger. The PCS will call the add new society once its request is approved and register the manager's account. Afterwards all the action related to user management within the society (creating new user, modifying roles and permissions, changing the society information) are recorded on the ledger. The PCS will utilise these API calls, along with the identity of the person responsible for these changes. This will create a transparent ledger of these changes that holds both the PCS and the society accountable in case of any dispute and allow the two to operate freely with reassurance and security.

- API responsible for querying data on the ledger (cf. Figure 36)
- API responsible for querying ledger info (cf. Figure 37), that is not pertinent to the current PCS state directly but allows blockchain users once the new state is passed to production to verify data on the ledger. When a society is created, the response returns a success message and a transaction ID, this ID through the Query Tx by ID will allow us to verify the TX data on the ledger, such as the info, creator, timestamp, and block number. For the block we can verify its hash, the number of transactions (cf. Figure 38).

A simplified workflow of how this works is represented in the figure 39) below. the DEMO COMPANY sends various requests to TIMAD, including creating a new society, creating new users with specified roles, deleting a user, and updating a user's role. TIMAD is responsible for the authentication and verification of data, which ensures that requests are genuine and the data is accurate before they are processed.

```
1  {
2    "numberOftransactions": 1,
3    "block": {
4      "header": {
5        "number": "2",
6        "previous_hash": "twGRUjrbwIzim3AOMXwF0iZ6eGCor5eSuNVSorq79xM=",
7        "data_hash": "p5nfjV+yS+MHI1hLXyNstY9PXH/hqStAJDAFfHlYwNg="
8      },
9    > "data": { ...
13     },
14 > "metadata": { ...
22     }
23   }
24 }
```

Figure 38: Block queried data

These requests are then forwarded to a Node.js server which performs the actual transactions (TX) for society creation, user creation, user deletion, and user update. The Node.js server handles each of these transactions and the outcomes are recorded as events on the blockchain infrastructure. For instance, the creation of a new society tx lifecycle is logged as per its associated smart contract (SC).

Additionally, the blockchain keeps a verifiable record of all user-related changes. A user's history, such as Mary's role update, can be requested which provides a timestamped record of the role change along with the identification of the person responsible for the change. This ensures traceability and accountability for actions taken within the system.

7.5 Seamless Integration of Blockchain Infrastructure

The integration of blockchain technology within the maritime logistics infrastructure represents a paradigm shift towards enhanced security and transparency without imposing significant modifications to the existing IS. This integration is designed to be non-disruptive, respecting the operational context of the maritime environment while providing the immutable assurance of blockchain technology.

As (Figure 40) elucidates, our blockchain infrastructure operates within a secure environment, encapsulating the complex mechanisms of blockchain technology behind intuitive interfaces and familiar operational processes. The established Information Systems require only minimal adjustments to interact with this new layer of technology. Stakeholders continue to engage with systems like TIMAD v2 through conventional graphical user interfaces (GUIs) and API calls, which now act as gateways to blockchain functionalities.

Behind these user-friendly interfaces, the API server, that serves as the bridge between traditional applications and the blockchain network. The server handles all blockchain intricacies, including smart contract invocation and transaction validation, while stakeholders interact with

7.5. Seamless Integration of Blockchain Infrastructure

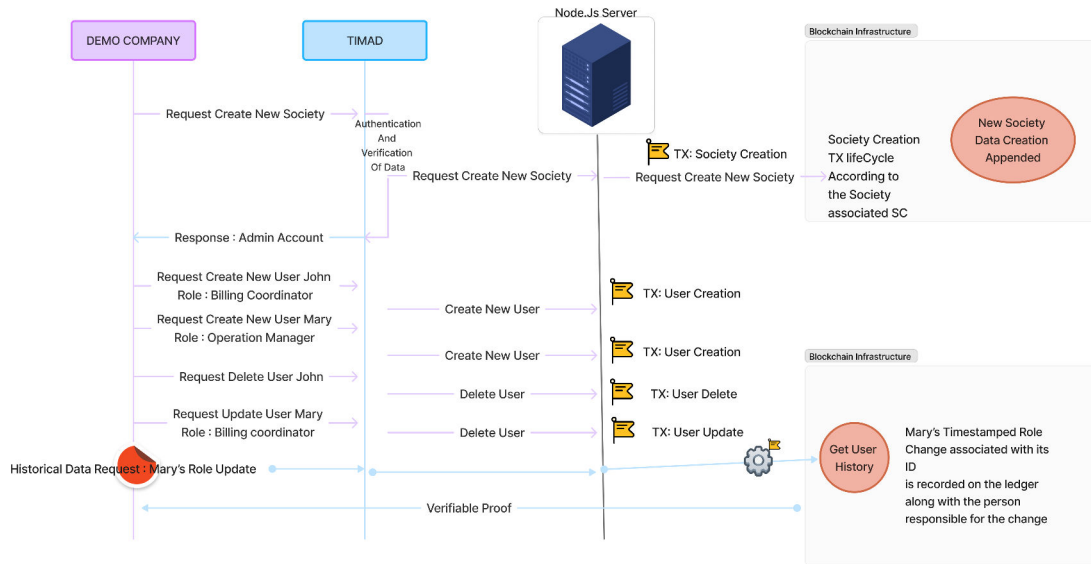


Figure 39: A simplified TIMAD-Blockchain interaction scheme

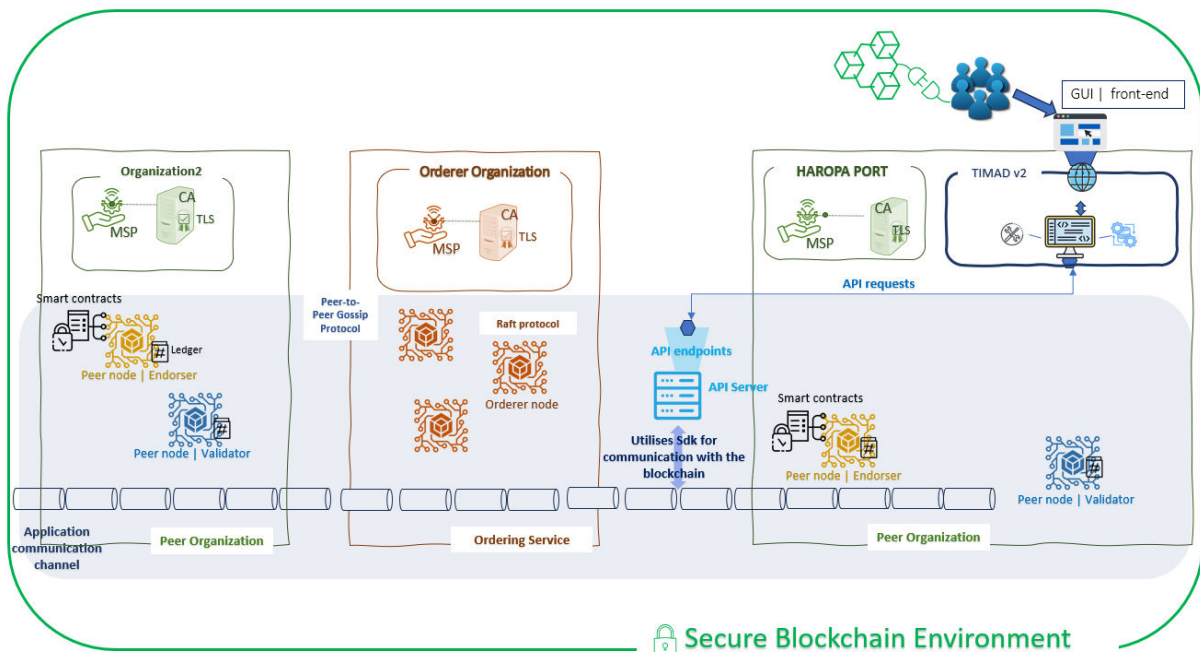


Figure 40: A diagrammatic representation of the seamless integration of blockchain within the maritime logistics ecosystem, illustrating minimal impact on existing infrastructure and IS.

the system as they normally would. This abstraction layer ensures that maritime stakeholders are insulated from the complexities typically associated with blockchain technology.

The implementation strategy has been deliberately designed to accommodate organizations with minimal technical capabilities. Organizations interested in leveraging the added value of blockchain—such as increased transparency and a universal source of truth for information—can participate in the network without extensive blockchain-specific knowledge. By requiring only a fundamental understanding of widely-used technologies like Docker and server setups akin to those already hosting maritime IS, the barrier to entry is significantly lowered.

Moreover, the strategic configuration of peer nodes as endorsers and validators, anchored by MSPs and TLS, establishes a governance framework that is both robust and familiar to entities within the maritime domain. The application communication channels and the ordering service, managed through the consensus protocol Raft, further exemplify the network's democratic and fault-tolerant nature.

In essence, this integration approach not only fortifies the maritime logistics ecosystem with blockchain's key attributes—immutability, transparency, and security—but also ensures operational continuity and stability. It is a testament to the viability of blockchain technology as a complementary layer to existing maritime logistics systems, promising an evolution of the sector that is both innovative and considerate of its heritage and current operational landscape.

7.6 User-Centric Ledger Interaction within TIMAD

The PoC for integrating blockchain into maritime logistics systems places significant emphasis on user experience and the seamless presentation of ledger information. Within the TIMAD system, users are provided with a familiar interface, which now includes additional functionalities for viewing blockchain-secured data. This integration is designed to be non-intrusive, maintaining the user interface's consistency while simultaneously enhancing data security and trust.

Intuitive Access to Secured Data A snapshot of the PoC, as shown in the subsequent figure, exemplifies the intuitive access to blockchain ledger information. Users of TIMAD are presented with ledger data in a format that is both accessible and coherent, ensuring that the transition to blockchain-augmented systems is smooth and free from unnecessary complexity.

(Figure 41) captures the essence of our design philosophy, where the underlying blockchain technology enriches the user experience by providing additional layers of verification and trust without disrupting established workflows. The Figure lists the societies within the system TIMAD that also have their data referenced on the blockchain.

Enhanced Trust without Disruption The key to this seamless integration is the deliberate avoidance of overt changes to the user interface that could otherwise be disruptive. Users

7.6. User-Centric Ledger Interaction within TIMAD

#	Désignation	Code	Code transco	Type	Numéro de SIRET	Numéro EORI	Actif	Alerte collaborateur	Actions
19	GRAND PORT MARITIME DU HAVRE	GPMH		PORT			✓	✓	
20	AGENCE DE MARCHANDISE	AGM1		Agent Marchandise			✓	✓	
21	AGENCE DE MARCHANDISE LA DEUXIEME	AGM2		Agent Marchandise			✓	✓	
22	AGENCE DE TRANSIT	TRANS1		Transitaire			✓	✓	
23	AGENCE DE MANUTENTION	MANUT1		Manutentionnaire			✓	✓	
24	SOGET	SOGET		Partenaire CCS			✓	✓	
26	FLORENT VAL COMPANY	FLODEMO	-	PORT	15151515151515	15151515151515	✓	✓	

Figure 41: Snapshot of the TIMAD interface displaying all societies created within the system

Administration des référentiels

Historique de la société

Informations #5a728ce65ff15221089e2fc9dc4069ba8d25657795124bf653ebee8335fdfe6c

2
désignation FLORENT VAL COMPANY
Code FLODEMO
codetransco -
adresse! Mon adresse
Adresse plus -
adressescomplément -
codepostal 76600
Ville Le Havre
Pays -
Téléphone +33600000000
Email florent@demo.timad.fr
siret 15151515151515
eori 15151515151515
alertecollaborateur 1
deleted ✕
Timestamp 2024-03-11 12:16:28.168 +0000 UTC

Figure 42: Snapshot of the TIMAD interface displaying ledger information seamlessly integrated within the user's workflow - All Societies view

Chapter 7. Timad Oriented blockchain developments

are not required to navigate through unfamiliar blockchain terminologies or processes. Instead, they are subtly made aware that their data is now secured on a blockchain (cf. Figure 43), providing them with peace of mind and an assurance of integrity, which is paramount in the maritime sector. The displayed ledger information includes critical data such as transaction IDs (#5a728ce65ff15221089e2fc9dc4069ba8d25657795124bf653ebee8335fdfeéc) that reinforce the credibility and traceability of operations within TIMAD and allow the user to refer to the transaction on the blockchain.

For example, if we proceed and delete the society from TIMAD. The society will no longer show up on the list nor in TIMAD's database. However, through blockchain we will keep a record of this interaction with the attribute `isDelete` turned to `true`.

```
"result": {
  "message": "Success",
  "result": [
    {
      "TxId": "651e70a97cae4bf2a310ec0938f369ad24f3e4bb760d407ab987d242d20a325e",
      "Value": null,
      "Timestamp": "2024-04-01 02:01:57.223 +0000 UTC",
      "IsDelete": "true"
    },
    {
      "TxId": "5a728ce65ff15221089e2fc9dc4069ba8d25657795124bf653ebee8335fdfeéc",
      "Value": {
        "Timestamp": "2024-04-01 01:27:07.444 +0000 UTC",
        "IsDelete": "false"
      }
    }
  ],
  "error": null,
  "errorData": null
}
```

Figure 43: Ledger information - A deleted Society

Safeguarding User Experience As stakeholders interact with TIMAD, the blockchain operates quietly in the background, recording transactions and ensuring the immutability of records. This silent vigilance of blockchain technology is crucial for stakeholders who rely on the veracity of data for their operational decisions. While users benefit from the robust security features of blockchain, their day-to-day interactions remain.

This chapter elucidated the development and implementation of blockchain technology within the TIMAD system, underscoring a pivotal transition from theoretical blockchain infrastructure to practical application in the maritime sector, specifically through smart contracts. These contracts, tailored for the TIMAD system—a PCS vital for maritime logistics operations—serve as the cornerstone for notarizing and enhancing the transparency of the Bill BAT access management and manifest within the PCS. This integration fosters a secure and immutable ledger for maritime logistics operations, ensuring a seamless user experience through a well-designed interface that bridges users with blockchain-secured data.

Further, the chapter delved into the workflow of the network, highlighting the roles of endorsing peers, orderer nodes, and validator nodes in the transaction process. This setup ensures the integrity and reliability of transactions within the network, fostering a robust and

7.6. User-Centric Ledger Interaction within TIMAD

efficient distributed ledger.

It outlined the liaison between PCS and the blockchain, detailing the development of blockchain functionality and the client-targeted interface. This interface, tailored for TIMAD, allows stakeholders to interact with the blockchain infrastructure, ensuring that the integration of blockchain technology enhances the maritime sector without disrupting established workflows.

The strategic deployment of smart contracts is detailed, focusing on notarizing relevant data and enhancing traceability within the PCS. This approach leverages the blockchain network for two-way communication capabilities, though the initial focus remains on notarization functions to improve accountability within the maritime logistics ecosystem.

PoC EVALUATION AND FUTURE PROSPECTS

Contents

8.1	Evaluation of the Proposed PoC	151
8.1.1	Evaluation Environment	152
8.1.2	Network Communication Validation	153
8.1.3	Hyperledger Fabric Implementation	154
8.1.4	Performance Definition	155
8.2	On-going Future works	158
8.3	Inter-maritime Operations	159
8.3.1	A maritime implementation	162
8.4	Conclusion	165

Abdallah, R., Besancenot, J., Bertelle, C., Duvallet, C. and Gilletta, F., 2023. Seamless Seas Leveraging Blockchain. Presented in CCSET2023 to be published in the IET conference proceedings. (Abdallah et al., 2023f)

In order to complete our exploration of blockchain technology and follow up with our new innovative approach, we now transition to a pivotal step. The following chapter will cover a performance evaluation of our system before we venture into the prospects of future developments. It offers a critical assessment of the viability performance and practical applicability of the proposed integration tailored for maritime logistics.

8.1 Evaluation of the Proposed PoC

The evaluation phase of the PoC is crucial for assessing the viability and performance of the proposed blockchain integration within the maritime logistics domain. This section delves into the systematic testing conducted to validate the applicability of our architecture and its capacity to handle production scenarios.

To ensure a rigorous and controlled evaluation of the PoC, testing was conducted within a carefully curated environment. The setup was designed to mimic the technical conditions

under which the blockchain-infused maritime logistics system would operate. The evaluation was carried out using two primary machines—one hosting the TIMAD application and the other dedicated to the blockchain infrastructure, which was deployed within a VirtualBox environment. The infrastructure setup—spanning from the deployment of the TIMAD application to the intricate network configurations enabling seamless communication between various components—lays the groundwork for a comprehensive performance assessment. By delineating acceptable response times and throughput capacities, it provides a comprehensive framework for assessing the PoC’s operational efficacy under simulated load conditions. This evaluation not only validates the architectural design but also highlights areas for potential optimization, paving the way for future enhancements.

With the deployment utilizing state-of-the-art technology and orchestrated within a Virtual-Box environment, this chapter not only reassures the technical feasibility but also exemplifies the innovative approach towards a scalable and efficient maritime logistics system. By ensuring interoperability and data exchange between the TIMAD application and the blockchain infrastructure, the PoC stands as a testament to the potential transformative impact of blockchain technology in this sector.

Furthermore, we offer through this chapter a broader perspective, looking beyond the current state of the PoC. We outline ongoing and future works aimed at broadening the blockchain network’s reach within the maritime sector. By engaging additional stakeholders and leveraging collaborative efforts, the vision extends towards a more interconnected and technologically advanced maritime domain. The chapter paints a picture of a future where blockchain technology not only enhances the operational integrity of maritime logistics systems but also fosters a new era of transparency, efficiency, and security across the global maritime logistics landscape.

8.1.1 Evaluation Environment

The machines utilized for the evaluation were provisioned with the following specifications to adequately support the deployment and execution of all necessary components:

TIMAD Deployment Machine (cf. table 8.1): This machine was configured to run the TIMAD application. Blockchain Infrastructure Machine (cf. table 8.2): The second machine was set up

Hardware Specs	Description
Processor	Intel(R) Core(TM) i5-10210U CPU @ 1.60GHz 2.11 GHz
RAM	8.00 GB
System	64-bit operating system, x64-based processor

Table 8.1: PCS host machine characteristics

within a virtualized environment using VirtualBox. This virtual machine (VM) hosted the entire blockchain infrastructure, deployed using Docker containers to simulate a production-like environment. To facilitate seamless communication between the TIMAD deployment machine

Hardware Specs	Description
Processor	Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz 2.81 GHz
RAM	16.0 GB (15.9 GB usable)
System	64-bit operating system, x64-based processor
Virtual Machine	OS: kali-linux 2023.1 amd 64

Table 8.2: Blockchain host machine characteristics

and the VM hosting the Hyperledger Fabric (HF) components, careful attention was given to the network setup. It was imperative that both systems operate within the same network domain to enable interoperability and data exchange critical for the PoC's success. To consolidate the network architecture and ensure a secure communication channel, a Virtual Private Network (VPN) is established. This VPN connected all elements of the PoC's network, encapsulating the data transfer within a secure tunnel. The implementation of the VPN is pivotal in maintaining the confidentiality and integrity of the data being exchanged within the PoC environment.

Virtual Machine Network Adapters The network adapters of the VM containing the HF components were configured with both NAT (Network Address Translation) and bridged connections. The NAT configuration allowed the VM to communicate with external networks, while the bridged adapter ensured that the VM appeared as a separate entity on the same physical network as the host machine.

Windows Subsystem for Linux (WSL) Network Configuration For the WSL environment, which is integral to the blockchain infrastructure, a bridged network configuration was employed to ensure that the subsystem was on the same network as the blockchain machine and its host machine thereby streamlining the communication pathways with the HF machine.

Implications for System Communication The network configuration was designed to support the distributed nature of the blockchain while maintaining the ease of use characteristic of traditional maritime logistics IS. By utilizing a combination of NAT, bridged connections, and a VPN, we ensured that all network elements of the PoC could communicate effectively, regardless of their physical or logical separation. This configuration not only reflects a robust approach to network security but also exemplifies the adaptability of the system to integrate within existing maritime infrastructure.

8.1.2 Network Communication Validation

Subsequent to the network setup, a series of tests were conducted to validate the efficacy of the communication channels. These tests confirmed that: - The TIMAD application could reliably transmit data to the blockchain infrastructure without any loss or significant latency. - The HF components on the VM could access the TIMAD deployment machine's resources as if they

were part of the same local network. This was not implemented in the PoC at this stage but was tested for later steps were events triggered within the blockchain network can reflect changes in the PCS. - The VPN provided a stable and secure conduit for all data exchanges within the PoC's network, ensuring that communication was consistent with the security standards required for maritime logistics operations.

8.1.3 Hyperledger Fabric Implementation

In our project, we implemented Hyperledger Fabric (HF), a permissioned blockchain framework specifically designed for enterprise applications. Hyperledger Fabric is distinguished by its role-based node architecture, modularity, and clear separation of duties, which align well with organizational structures. These characteristics were pivotal in developing our PoC that leverages blockchain technology to establish a trust model tailored to the maritime industry's unique requirements. For the PoC, we utilized bash scripts for orchestration, the Go programming language for coding smart contracts, and a Node.js server with JavaScript for developing the API. This API facilitates communication with the PHP-based Timad system. In conventional blockchain implementations, a transaction order-execute architecture is typically employed, where transactions are first ordered using the network's consensus mechanism and subsequently executed in the same sequence across all network peers. This approach, as explored in scholarly works such as (Androulaki et al., 2018), emphasizes transaction throughput, ensuring deterministic transactions and reliable smart contract execution. Hyperledger Fabric, however, adopts an alternative workflow known as execute-order-validate. In this model, endorsers execute transactions within isolated environments of individual peers and transmit the signed, endorsed transactions across the network. The transactions are then sequenced by the ordering service before being committed to the ledger by validator nodes. This process allows for the sequential execution of interdependent transactions, while others can be executed in parallel, significantly enhancing transaction throughput. It is noteworthy that smart contracts in HF are primarily written in Go, a decision influenced by the fact that HF's core is also developed in Go. However, HF supports other general-purpose programming languages like Java and JavaScript, adding to the PoC's versatility and suitability for broader, global deployment in the maritime sector. In HF, validator nodes, among others, maintain the shared state of the blockchain. The combination of isolated smart contract execution and a shared ledger augments both the security and reliability of the system, crucial aspects in the context of blockchain-based solutions in the maritime industry.

The software versions that have been used for the development are:

The Hyperledger Fabric (HF) network has undergone extensive evaluation in academic and industry literature, demonstrating notable efficiency and performance. This is evident in studies such as (Thakkar et al., 2018) which provide comprehensive insights into the performance metrics of HF. These evaluations typically focus on various aspects such as transaction throughput, latency, and scalability, crucial factors for enterprise blockchain applications.

Software	Version
Hyperledger Fabric Docker Images Tag	2.1
Hyperledger Fabric COUCH Docker Images Tag	Latest
Hyperledger Fabric Go Chaincode	go1.20.4
Hyperledger Fabric Gateway Node.js	2.2.15
Docker	20.10.24

Table 8.3: Software versions

Further, the modular and customizable nature of HF, as discussed by (Cachin et al., 2016) allows organizations to tailor the network to fit specific needs, thereby optimizing performance for various use cases, including those in the maritime sector.

In the context of implementing blockchain solutions within the maritime sector, particularly using Hyperledger Fabric, specific configuration parameters of the ordering service play a pivotal role in optimizing transaction processing and block creation. One such critical configuration is the `BatchTimeout`, set at 2 seconds, which dictates the maximum duration for accumulating transactions before a block is finalized. This setting ensures a balance between timely block creation and adequate transaction inclusion. Complementing this, the `BatchSize` configuration is meticulously defined to cater to the operational demands of the maritime industry. It includes a `MaxMessageCount` of 10, allowing up to ten transactions per block, thus ensuring efficient processing while avoiding overload. The `AbsoluteMaxBytes` is configured at 99 MB, a threshold that represents the upper limit on the block size, ensuring robust handling of data sizes typical in maritime operations. Additionally, the `PreferredMaxBytes` is set at 512 KB, an optimal size aimed at enhancing network throughput and reducing latency, which is critical for the time-sensitive nature of maritime activities. These configurations collectively contribute to a blockchain framework that is both efficient and scalable, addressing the unique needs of the maritime sector.

8.1.4 Performance Definition

The evaluation of software performance is a multidimensional endeavor that encompasses various metrics, each reflecting distinct aspects of system behavior under operational conditions. Commonly used metrics include per-request response time and transaction throughput, defined as the number of requests processed per unit of time.

In the context of a PCS, the transactional landscape is characterized by a finite and controlled number of requests, stemming exclusively from authorized PCS users, implying a bounded transactional volume. This thesis postulates an upper limit of 500 requests per day, which, while not reflective of the current utilization, provides a buffer to accommodate future increases in system traffic, thereby ensuring system scalability and reliability.

The architectural blueprint delineated in this dissertation focuses predominantly on the functional layer within a classical three-tiered architectural paradigm. Therefore, the response times

```
"result": {
  "message": "Success",
  "result": [
    {
      "TxId": "f393a959ab3982fdb150c3f04f989858d78ab4604d90e9145b17fb70c951824",
      "Value": null,
      "Timestamp": "2023-01-10 10:44:12.648 +0000 UTC",
      "IsDelete": "true"
    },
    {}
  ]
}
```

Figure 44: Deletion operation

of primary interest pertain to this layer, inclusive of the time contributions from the underlying data layer. This holistic approach to measuring response time ensures a comprehensive understanding of system performance from the end-user perspective.

In alignment with the performance classification schema articulated in the scholarly work (Rempel, 2015), the blockchain-based architectural solution proposed in this thesis aims to uphold the PoC “Complex Operations” category. This categorization is predicated on the computational intensity and replication processes inherent to blockchain operations, while also serving as a solid foundation for any system evolution. This category stipulates a response time threshold of no more than 5 seconds.

Given the focus on the functional layer, a target response time of 3 seconds is posited for this layer alone, representing 60% of the aggregate permissible response duration. Consequently, this allocates a residual 2 seconds for the presentation layer, tasked primarily with data rendering, a process that should be executed expeditiously, as asserted by the referenced performance metrics.

Drawing upon user requirements and scholarly insights ((Rempel, 2015), (Akidau et al., 2013), an acceptable response time of up to 3 seconds is established for the architectural construct proposed herein. This threshold applies to create, read, and update operations. Deletion requests are treated analogously to update operations, given that while data may be removed from the visible world state, it remains extant on the ledger, marked with a deletion attribute—thereby retaining a trace of its existence for auditability and historical analysis (cf. Figure 44).

This balanced allocation of response time across the system’s tiers is designed to deliver a responsive user experience while adhering to rigorous performance standards that ensure the PCS operates efficiently, securely, and in a manner that instills confidence in its end-users.

In the context of the system’s architecture, it is pertinent to note that the target response time established for the blockchain infrastructure operates independently from the response time of the existing PCS. The asynchronous nature of the two systems’ operations ensures that the PCS can function without being impeded by the blockchain’s processing time. This architectural decision ensures that the PCS’s performance remains unaffected by the blockchain layer, thus upholding the system’s operational efficiency and user experience. The blockchain component acts as a parallel process that enhances data integrity and traceability without imposing latency on the PCS’s primary functions.

Tables (8.4 and 8.5) present the test results for the primary smart contract methods for the

8.1. Evaluation of the Proposed PoC

500 requests denominated above. The columns indicate the number of objects included in each test batch. For every batch, the Average (AVG) is measured in seconds. The results are presented with a precision of two decimal places, with the third decimal place being rounded off. And the repetition of these tests for 3 rounds entailed a deviation in response time of 0.2 0.3 seconds.

Smart Contract	Method	Averages (s)		
		400 Objects	800 Objects	1600 Objects
User	Add New User	1.1	1.06	1.04
User	Modify User	1.05	1.1	1.12
Society	Add New Society	0.86	0.88	0.87
Society	Modify Society	0.9	0.83	0.87
Type Society	Add New Type Society	0.65	0.63	0.61
Type Society	Modify New Type Society	0.62	0.59	0.60
Manifest	Add New Manifest	1.24	1.25	1.25
Manifest	Modify New Manifest	1.23	1.22	1.19

Table 8.4: Smart Contract POST Test Results

Smart Contract	Method	Average(s)
User	Get User Info	0.78
User	Get User History	1.1
Society	Get Society Info	0.49
Society	Get Society History	0.71
Type Society	Get Type Society Info	0.25
Type Society	Get Type Society History	0.67
Manifest	Get Type Manifest Info	0.91
Manifest	Get Type Manifest History	2.05

Table 8.5: Smart Contract GET Test Results

The tables above encapsulate the empirical results from rigorous testing of the primary smart contract methods, providing a clear snapshot of the system's performance under a simulated load of 500 requests. The data delineates the response times for various batch sizes, detailing the average processing time for each method when handling 400, 800, and 1600 objects, respectively. As evidenced by the results, there is a consistency in performance across the different batch sizes, with a minor deviation in response times noted during the repeated test rounds. The variance of 0.2 to 0.3 seconds is within an acceptable range, demonstrating the resilience and stability of the smart contract processing within the blockchain network.

The observed response times for the 'POST' operations, which include adding and modifying entities such as users, societies, and manifests, indicate efficient transaction processing capabilities. Similarly, the 'GET' operations, which retrieve information and historical data, exhibit prompt response times, signifying a well-optimized data retrieval process within the blockchain network. These findings substantiate the blockchain system's capability to handle a significant volume of transactions with minimal impact on performance, thereby validating

the architecture's suitability for production scenarios within the PCS context. The tests further underscore the robustness of the proposed solution, affirming its readiness for deployment in a live maritime logistics environment.

8.2 On-going Future works

In the evaluation presented, we have delineated the implementation and testing of a traceability architecture conceived for the maritime logistics domain, employing Hyperledger Fabric as the foundational blockchain platform. The PoC showcases the applicability of this architecture in authentic operational scenarios, offering an empirical basis for its deployment.

The architecture stands out for its utilization of generic smart contracts, which provide a versatile framework for managing contractual milestones and incident reporting. This capability is particularly significant in a permissioned blockchain context, where such operations require strict control and oversight. The versatility of the smart contracts within our architecture ensures adaptability and relevance across a range of traceability scenarios, making it a competitive alternative to the state-of-the-art solutions in this domain.

It is, however, important to highlight that the performance tests executed during this evaluation were conducted with calls to the blockchain being made in a sequential order. This methodological choice was intentional, and aimed at isolating each transaction to precisely measure its execution time without the influence of concurrent processes. While this approach provides clarity on the transactional efficiency of individual calls, it does bring to light the architecture's modest transaction throughput when viewed through the lens of parallel processing capabilities typically expected in high-load systems.

The observed request throughput is under an extreme evaluation sequential process. It proved performant but we reckon that there might be room for optimization, particularly if the architecture were to be scaled for higher volumes of concurrent transactions. The sequential execution of calls in these tests offers a conservative perspective on performance, which, while indicative of a reliable and stable system, also points to potential areas for enhancement.

Future iterations of this architecture could benefit from exploring the implementation of parallel processing techniques and optimizing the blockchain network configuration to improve throughput. Such enhancements would likely further solidify the architecture's suitability for complex and demanding traceability applications in the maritime logistics sector, where efficiency and speed are paramount.

As we contemplate the broader implications of this PoC, the promising results attained thus far not only affirm the architectural design but also lay the groundwork for ongoing optimization efforts. These efforts will be instrumental in realizing a high-performing, scalable blockchain solution that aligns with the dynamic and evolving needs of global maritime logistics operations.

In emphasizing the innovative aspects of the seamless yet performant blockchain infrastructure presented in this PoC, it is essential to articulate how the architecture harmonizes ease

of use with operational efficiency. This balance represents a significant stride in blockchain applications, particularly in the context of maritime logistics.

The innovation in this architecture lies in its ability to integrate blockchain technology into existing maritime operational frameworks without causing disruption or requiring extensive system overhauls. This seamless integration is achieved through a thoughtful design that encapsulates blockchain complexities within user-friendly interfaces and familiar operational procedures. Users interact with the system through conventional GUIs and API calls, which now serve as gateways to enhanced functionalities underpinned by blockchain.

Simultaneously, the architecture does not compromise on performance. Despite its user-centric design, it maintains robust transactional capabilities and data integrity—key features of an effective blockchain solution. The system efficiently handles smart contracts for managing contractual milestones and incident reporting, demonstrating not just versatility but also the capacity to handle substantial transaction volumes within acceptable response times.

This dual achievement of seamless integration and robust performance is a notable advancement in blockchain technology applications. It addresses one of the primary challenges in adopting blockchain: making the technology accessible and practical for real-world applications without sacrificing its core benefits. By doing so, this architecture sets a new benchmark for blockchain implementations, particularly in sectors like maritime logistics, where the balance between technological advancement and operational continuity is crucial.

Furthermore, the potential for scalability and optimization, as evidenced in the performance tests, indicates that this architecture is not only effective in its current state but also poised for future enhancements. These enhancements could further refine the system's throughput and processing capabilities, ensuring its long-term viability and adaptability to evolving industry needs.

8.3 Inter-maritime Operations

This section aims to elaborate on how this PoC could be employed in the grand scheme of the maritime realm and draw upon our presented publication (Abdallah et al., 2023f). It outlines the prospective application of PoC within the broader maritime industry, demonstrating its potential impact and scalability.

The development of this PoC represents a proactive step towards establishing a more robust and interconnected maritime logistics network.

Starting from the proof of feasibility and performance of a local network, the current next step is for a more tangible implementation with a distribution of nodes across several legal entities that are distinct stakeholders of the maritime sector.

The PoC's next milestone is an ongoing development that we wish to detail as it stems from the PoC and represents a significant advancement beyond the foundational phase. Consequently laying the groundwork for enhanced robustness through the deployment of a real network of

Chapter 8. PoC Evaluation and Future Prospects

nodes distributed among various legal entities that are international stakeholders in the industry.

They are HAROPA PORT, EASYPORT, and SOGET.

SOGET SOGET is a software company that develops solutions to improve efficiency in ports, airports, and logistics <https://www.soget.fr/en>. Their product offerings include PCSs, Business Intelligence tools, and Port Operating Systems (POS). They are also committed to environmental sustainability and social responsibility.

Easyport was founded in 2022 by two founding members SOGET and HAROPA PORT. Some of the products offered by easyport include EasyPOS, My ETA, and My T&T. Easyport simplifies port operations for everyone involved by offering software for managing port calls, tracking cargo, and predicting ship arrivals.

The strategic decision to involve key maritime entities—HAROPA PORT, EASYPORT, and SOGET—highlights the commitment to creating a real network of nodes distributed among several legal entities. This collaborative approach is pivotal for two primary reasons:

- **Implementation of an Actual Network:** By integrating these entities, the PoC transcends from being a standalone system to becoming part of a comprehensive network. This expanded network facilitates direct communication with existing systems like the PCS TIMAD of HAROPA PORT and the CCS S)ONE. The integration of these systems heralds a new era of interconnectedness and data exchange efficiency within the maritime sector.
- **Stakeholder Engagement and Validation:** The involvement of these prominent maritime actors serves as a testament to the validity and potential of the PoC. The innovation and user-centric design of our architecture have laid the groundwork for convincing these stakeholders of the benefits of blockchain integration. Their participation not only adds credibility but also ensures that the system is tested and refined in a real-world context.

As this initiative progresses, stemming from the ongoing efforts of the thesis, it paves the way for comprehensive testing and the implementation of advanced security measures. The active engagement of additional maritime actors in this venture is indicative of the industry's readiness to embrace innovative solutions for enhanced operational efficiency and security.

Looking ahead, the PoC is envisioned as a foundational step towards a more interconnected and technologically advanced maritime domain. While acknowledging the need for further enhancements and refinements, the current stage of the PoC already leverages the capabilities of HF effectively. The innovative approaches adopted in this project have only begun to tap into the vast potential of what blockchain technology can offer to the maritime industry.

The progression of our project, as outlined in a recent publication under the title of Seamless Seas Leveraging Blockchain, offers a strategic roadmap for the future stages of implementation within the maritime sector. This publication aims not only to provide a comprehensive insight

into our approach but also to contribute to the broader academic and industry discourse, thereby paving the way for further testing and development of our blockchain-based solution.

Our work is aligned with the ongoing efforts in the maritime sector to enhance interoperability among maritime Information Systems (IS) and to promote open communication channels. This alignment is particularly relevant in the context of the 'MSW' project initiated by the International Maritime Organization (IMO) mentioned in the first chapter. The 'MSW' concept is a cornerstone initiative aimed at streamlining maritime logistics and trade through efficient information exchange. By ensuring compatibility with this initiative, our project contributes to a unified, industry-wide movement towards more integrated and transparent maritime operations.

The publication serves as a platform to demonstrate potential benefits and practical applications of our blockchain solution in achieving these industry objectives. It lays out the theoretical and practical aspects of the proposed approach, emphasizing how blockchain technology can enhance data sharing, security, and traceability within the maritime sector.

Furthermore, showcasing the feasibility and advantages of our solution has a crucial role in attracting additional stakeholders to join our network. The involvement of more entities not only broadens the network's scope but also enriches its data ecosystem, thereby enhancing the overall value proposition of the system.

In essence, our publication acts as both a beacon and a catalyst in the maritime sector's journey towards digital transformation. It illustrates how cutting-edge technology like blockchain can be effectively integrated into existing maritime frameworks, driving the industry towards a more interconnected, efficient, and transparent future. Through this endeavour, we aim to contribute significantly to the ongoing evolution of maritime logistics, aligning with and propelling forward the objectives set by leading maritime authorities like the IMO.

PCSs have already shown they can improve coordination and efficiency in maritime logistics through integrated data exchange and workflow management (Carlan et al., 2016a), so it would be counterproductive if proposed technological innovations completely undermined these existing foundations rather than intelligently building upon them incrementally. A cooperative approach theoretically illustrated in (cf. Figure 45) that smartly anchors current systems such as PCS and offer new capabilities, rather than advocating radical overhaul, will likely yield the best outcomes. It equips existing systems with a distributed blockchain infrastructure offering a widespread decentralization possibility for pre-existing siloed systems. Communication in traditional systems can be notarized on the shared ledger allowing the currently compromised fragmented transparency and hindered traceability.

After conducting comprehensive research and analysis of the specific requirements in the maritime domain, we have reached a firm conclusion consolidated by the PoC that HF, a permissioned blockchain is the most suitable for the maritime industry. Additionally, the most suitable approach, an innovative approach that we put forward is the 4seamless integration if existing and largely used IS (such as PCS, CCS, etc . . .) As it also overcomes the hybrid superstructure conundrum.

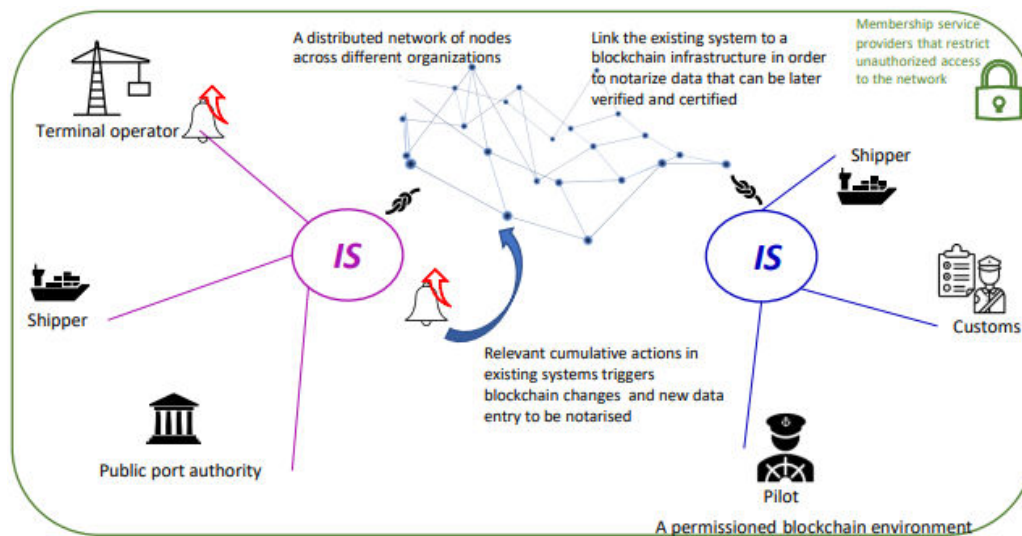


Figure 45: An illustration of the envisioned maritime environment

The proposed framework's modularity is highly suitable for the maritime network, especially when dealing with different actors possessing distinct capabilities and roles within the network. There are several key advantages to this approach. Firstly, it enables the network to restrict sensitive transaction endorsements to specific entities, ensuring that only trusted parties are responsible for such critical actions. In permissioned blockchain networks, the node entities are identifiable and recognized as either trusted or semi-trusted participants.

Secondly, all transactions being endorsed and linked to the authenticated entity that initiated them enhances accountability, traceability, and transparency on the network. Thirdly, the presence of trusted entities like governments and port authorities in the maritime sector allows for efficient handling of endorsements and management of ordering nodes responsible for achieving consensus on the network. We propose the raft consensus algorithm.

Being leader-based and governed by trusted entities, provides a sense of order and authority in decision-making, while its inherent randomness adds an extra layer of security and reliability. Furthermore, the proposed consensus architecture utilizes computing resources already in place in the maritime ecosystem across different information systems. It functions asynchronously so as not to obstruct current systems, but rather reinforce them. Additionally, memory usage, network traffic, and other resource requirements comply with existing maritime infrastructure as opposed to other reputable yet highly consumptive blockchains.

8.3.1 A maritime implementation

In the current phase of our research, our focus relied on proving the feasibility and implementational aspect of the proposal. Once in place, partly validated, and targeting a larger implementation spectrum. We put this in a larger spectrum, targeting additional stakeholders and a global business industry.

This approach is informed by valuable insights gained from past blockchain projects and pilot

initiatives, where premature implementation without a robust conceptual foundation resulted in resource wastage. Drawing inspiration from successful frameworks employed in other sectors that heavily relied on thorough conceptual work (Ravitch and Riggan, 2016), we seek to develop a solid groundwork that aligns precisely with the requirements of the maritime sector, while avoiding potential pitfalls.

We acknowledge the distinctiveness and conservatism of the maritime ecosystem, and thus, we do not discredit the aforementioned projects. Nonetheless, our current focus centers on building the necessary conceptual foundation that precisely caters to the sector's unique needs and challenges.

By engaging in limited implementation and small-scale prototyping, we adopt a prudent approach to test our concepts effectively. Scalability is a vital consideration for the future, but at this stage, we prioritize clarity in our concepts and partial implementation. This incremental approach will pave the way for broader adoption and scalability in the maritime sector. Rather than striving for a wide-scale consensus immediately, we propose a methodical and gradual progression towards conceptual clarity and partial implementation, which will eventually lead to substantial scalability within the sector.

The goal is to strategically adopt blockchain in a manner that minimizes disruptions during the transition phase. To achieve this, we leverage the permissioned blockchain framework HF, wherein each participating organization maintains its own CA (Fabric or other) and MSPs for authenticating actors within the blockchain-powered maritime

A conceptual next step representing a real-world analogous environment that combine insights from the industrial sector, our first step PoC thereby enhancing the applicability and relevance of the research.

The illustration in (Figure 46) showcases three actors that are common in all PCS systems. For the sake of simplicity and to focus on conceptualizing our approach potential. We will refrain from further developing any additional actors. Nevertheless, it is important to acknowledge the multimode and complexity of the ecosystems as this also emphasizes one of our strong points: seamless integration.

Maritime actors assume diverse roles within the ecosystem, each characterized by distinct capabilities, The PCS, an IS, possesses ample resources enabling the role of blockchain nodes responsible for maintaining the ledger. Moreover, its managing governance entity is tasked with the validation of transactions passing through the PCS, a process that involves its coupled endorser nodes.

Conversely, other entities may solely necessitate one type of node. For instance, terminal operators may exclusively require the endorsement of transactions. Consequently, they can deploy a containerized endorser node, which operates with limited resource consumption. Due to its role, which primarily entails transaction execution and proposal generation (including its signature), and does not encompass the comprehensive validation process, the containerized endorser node typically demands fewer computational and storage resources when contrasted

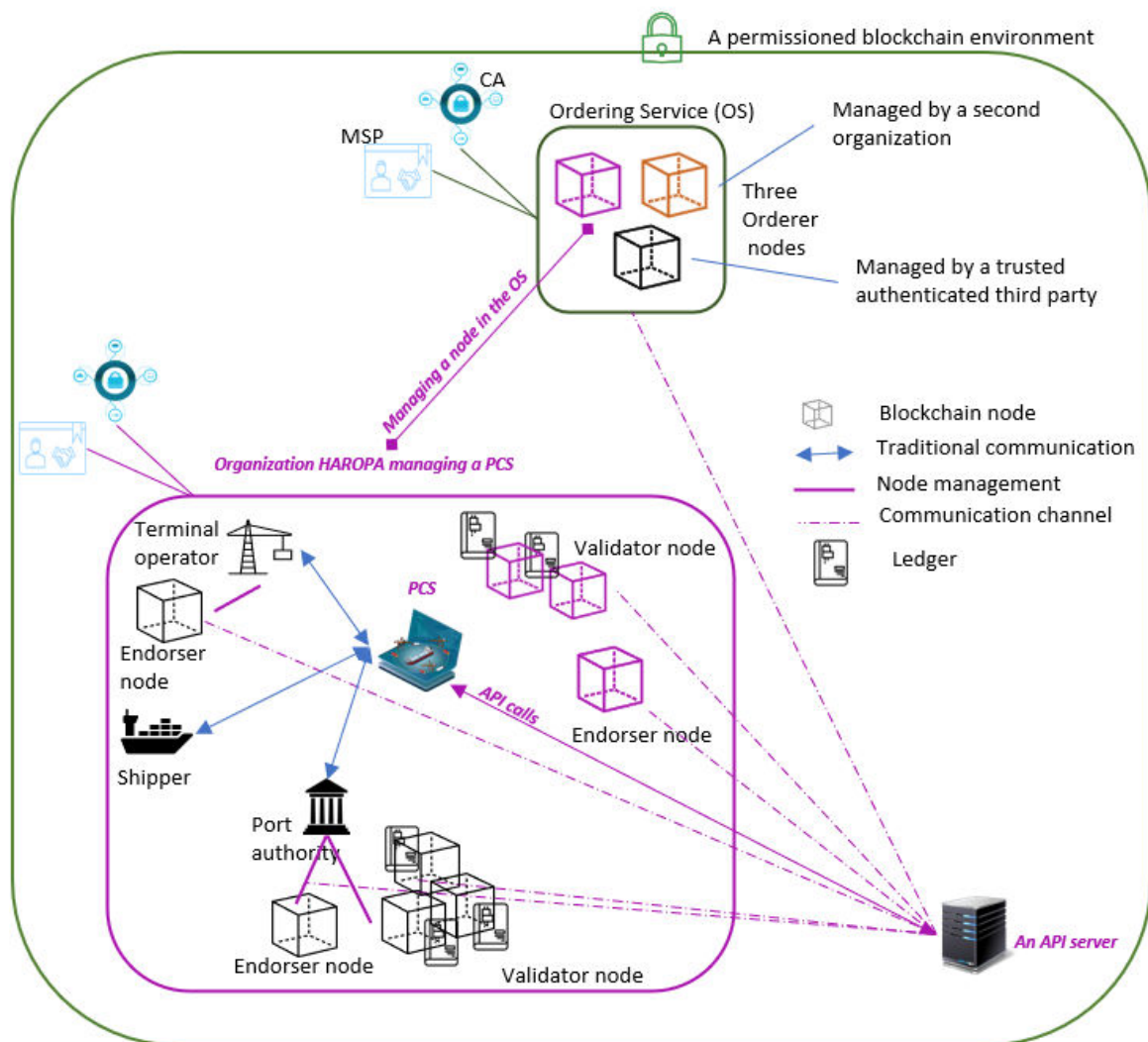


Figure 46: A blockchain-based maritime platform for maritime entities

with validator nodes.

Our approach in this research does not seek to undermine or introduce a new platform that could potentially alienate existing ISs. We recognize that some ISs in the maritime sector are developed by the ports themselves, and proposing a completely new platform may not be appealing to them. Instead, our approach revolves around providing an infrastructural solution that allows actors to choose the extent to which they integrate blockchain technology.

By adopting a modular approach that integrates legacy systems and promotes their interoperability, we introduce the desired traceability and transparency to the system without imposing a burden on the currently used Information Systems (ISs). The new permeate ecosystem leverages blockchain for efficient and secure transparent communication.

Importantly, due to the infrastructural nature of our system, the user experience remains unchanged, seamlessly blending into the existing systems. Users interact with familiar interfaces, ensuring a smooth transition to blockchain technology without disruptions to their accustomed

workflows. This strategic consideration underscores our commitment to not only technological advancement but also to the user experience and usability, ensuring that maritime actors find the proposed system user-friendly and easily adoptable within their established practices. Furthermore, the infrastructure itself is managed via Docker, where nodes are Docker containers easily deployable using the technology that maritime actors are already utilizing. In practice, relevant transactions continue to propagate through the PCS, which then communicates with the blockchain infrastructure through a connected server using API calls. We prioritize API calls due to their ability to enable seamless integration and secure data exchanges. Leveraging API technology comes with significant benefits, particularly because it is already widely utilized in the maritime sector. Thus, a simple API call can be employed in existing IS (such as the currently implemented API calls in our test case with the PCS) to communicate with the blockchain infrastructure without introducing additional complexity or necessitating specialized knowledge. This seamless integration allows maritime actors to harness the advantages of blockchain while preserving their existing systems and workflows.

To illustrate this, consider the following example: a shipper operating within PCS Haropa submits its manifest, which is approved, authorized by relevant entities through the PCS, then notarized, and signed via API calls to the server by the PCS on the blockchain infrastructure. Upon the ship's voyage to another port area governed by a different PCS, the shipper, present on the previous communication channel, retrieves its state information, and presents it to the new PCS's channel. The authenticity of this data is confirmed by cryptographic algorithms signed by the predecessor port authority, eliminating any redundant processes through two simple API calls: a query and a submission to the blockchain infrastructure.

Additionally, our system excels in its ability to facilitate seamless data exchange among different systems, effectively resolving process redundancy resulting from the lack of data exchanges between disparate systems, data standardization variations, and diverse regulations (cf. Figure 47).

This exemplifies the system's enduring capability to tackle the challenges prevalent in the current ecosystem, wherein diverse actors possess varying technical and technological capabilities. Entities with advanced capacities may actively participate in the network's infrastructure, while others can efficiently leverage the existing infrastructure through API calls, thereby streamlining the adoption of blockchain technology within the maritime industry.

Furthermore, within the context of SWs, our infrastructure furthers the simplification of processes by facilitating open yet secure communications, ultimately serving as a single source of truth for all stakeholders involved.

8.4 Conclusion

Realizing the proposed blockchain framework necessitates addressing critical factors around scalability, security, interoperability and performance. Benchmarks show leading blockchain

platforms like Hyperledger Fabric capable of processing over 3000 transactions per second at sub-second speeds, outperforming traditional systems (Melo et al., 2022). Permissioned access, encryption, and distributed architecture provide robust security, with analyses demonstrating resilience against common threats.

Integration with existing maritime systems is enabled through APIs, adhering to emerging standards for supply chain data sharing. Modular architecture allows incremental scaling while optimization strategies like off-chain processing boost throughput. Taken together, these technical capabilities demonstrate the feasibility of transforming current maritime processes through strategic blockchain adoption, without disrupting existing workflows and systems.

The technology holds immense disruptive potential for the maritime sector if embraced strategically. By offering enhanced transparency, traceability, security, and efficiency, it aligns perfectly with the industry's digitization needs. Our approach aims to demystify blockchain and accelerate its adoption by integrating it with existing systems in a modular, non-disruptive manner.

The proof-of-concept and methodology we have presented bridge the gap between theory and application, taking the first tangible steps towards unlocking blockchain's benefits for maritime stakeholders. While the journey has just begun, the course is set. Currently, fragmented communication between different IS arises due to various factors such as lack of standardization, the involvement of different actors in these IS, and varying regulations and competitiveness. To demonstrate the sustainability of our system, we simulate the presence of another organization with a different IS (in this case, we chose PCS for illustrative purposes, but it could be any type of IS) (cf. Figure 9 in chapter 4). Our concept of IS sustainability revolves around the system's ability to adapt, endure, and efficiently support organizational processes while minimizing environmental impacts. Although our main focus is on adaptation and endurance, it's important to note that the consensus mechanism we use remains eco-friendly in comparison to other blockchain alternatives, consuming resources equivalent to the currently available IS.

There is still work to be done in advancing and extending our platform. Further exploration of use cases, limitations, and benchmarks will help refine the solution and scale it to global-level adoption. Additionally, we must continuously expand the ecosystem of integrated legacy systems and partners.

Yet the possibilities are as boundless as the seas. With blockchain's help, maritime operations can reach unprecedented levels of efficiency, transparency and sustainability. Costly delays, duplications and paper-based processes will become artefacts of the past. Imagine smart contracts seamlessly coordinating logistics between ports, customs and shippers. Supply chain transparency will minimize fraud, errors and counterfeits. PCSs will securely share data to optimize workflows globally.

These breakthroughs are within reach. But the real work starts now - in pushing the boundaries of what is possible. Our research has set the groundwork and vision. The rest of the journey relies on innovation, collaboration and a spirit of exploration from maritime stakeholders worldwide.

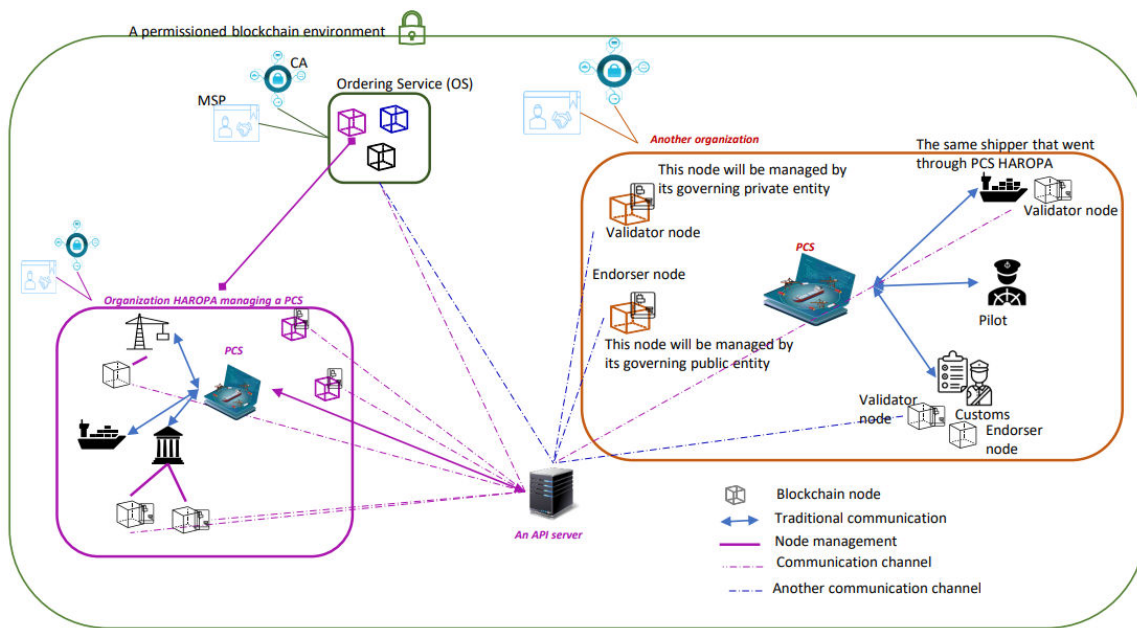


Figure 47: A full-scale blockchain-based maritime environment

We chart a course towards the seamless, blockchain-powered seas of the future.

CONCLUSION AND FUTURE DIRECTIONS

In conclusion, this exploration of the intersection between maritime logistics, blockchain technology, and digital transformation has yielded valuable insights. The research presented in this dissertation contributes to the ongoing conversation on how emerging technologies can reshape global trade.

This dissertation commenced with an elucidating incident – the grounding of the *Ever Given* in the Suez Canal – which not only underscored the fragile interconnectedness of global supply chains but also illustrated the imperative for technological evolution within the maritime industry.

Our exploration delved into the annals of maritime history, tracing the evolution from ancient seafaring ventures to the advent of containerization, and further, to the digital revolutions that are shaping the future of maritime logistics. This historical context set the stage for our investigation into the potential of blockchain technology as a harbinger of transformative change within this sector. We examined the profound impact of key developments like standardization and computerized logistics systems on enhancing trade flows and supply chain visibility. Yet, our analysis revealed persistent gaps and challenges including data silos, lack of transparency, and vulnerability to errors and fraud that continue to hinder the maritime industry's efficiency and resilience.

This dissertation has examined the complex interplay between technological advancements, physical capabilities, and infrastructural developments that have shaped the evolution of the maritime industry into a global powerhouse. The discussion navigated through the introduction of containerized shipping, the expansion of port infrastructures, and the pivotal role of Electronic Data Interchange (EDI) and PCSs in fostering efficiency and transparency across maritime logistics networks. We examined how contemporary PCS like TIMAD have digitalized documents and processes, yet still face limitations in seamless data sharing, immutability, and system interoperability across stakeholders.

In dissecting the challenges and opportunities presented by blockchain technology, our research illuminated the potential for this emergent technology to address longstanding inefficiencies, enhance traceability and security, and foster a more integrated, transparent maritime ecosystem. The core traits of blockchain – decentralization, immutability, and consensus-driven validation – position it as a catalyst for revolutionizing how data is shared, transactions are executed, and stakeholders collaborate within the maritime sector's complex operational landscape. Our investigation into the practical application of blockchain, through the lens of the PCS TIMAD, offered a tangible testament to the technology's viability and transformative potential

Chapter 9. Conclusion and future directions

within the sector.

This dissertation has not only bridged historical insights with contemporary technological advancements but has also contributed substantively to the academic discourse on blockchain's role in maritime logistics. It underscores the sector's readiness for digital evolution, highlighting blockchain's promise in advancing operational efficiency, safety, and sustainability. By presenting a holistic view that considers the industry's unique challenges, stakeholder dynamics, and technological requirements, this research offers a comprehensive blueprint for pragmatic blockchain adoption tailored to the maritime context.

The deployment of our PoC at a real-life scale has been a pivotal milestone, demonstrating the potential for blockchain to revolutionize maritime logistics through enhanced scalability, efficiency, and security. However, this is merely the beginning of a journey marked by continuous adaptation and technological exploration.

The preliminary stages of this research endeavour underscored the transformative potential of blockchain technology within the maritime logistics sector. Through a meticulous process of analysis and development, we crafted a strategic approach to integrating blockchain, emphasizing the creation of smart contracts tailored to enhance operational transparency and fortify data integrity across PCSs like TIMAD. This comprehensive framework not only demonstrated the practical applicability of blockchain but also established a robust foundation for real-world integration within the maritime domain. The architecture we devised, underpinned by a rigorous understanding of the sector's unique challenges and requirements, showcased the harmonious convergence of cutting-edge technology and industry-specific considerations. By bridging this critical gap, our work paved the way for a seamless transition towards a more secure, transparent, and efficient maritime logistics ecosystem.

Central to our efforts was a comprehensive evaluation of the proposed PoC, a pivotal undertaking that underlined the operational efficacy and scalability of our blockchain solution. Through systematic testing in a meticulously simulated environment, we affirmed the architectural framework's capacity to meet the complex and multifaceted demands of the maritime logistics sector. The rigorous evaluation protocols enabled us to assess the PoC's performance metrics across various operational scenarios, yielding compelling evidence that aligned with the industry's stringent thresholds for efficiency, security, and reliability. This comprehensive evaluation not only validated the viability of our proposed solution but also reinforced the broader potential of blockchain technology to catalyze transformative change within the maritime logistics landscape.

Envisioning a future defined by interconnectivity and technological advancement, our ongoing efforts are focused on expanding the blockchain network to encompass a broader array of stakeholders within the maritime ecosystem. This strategic move towards a truly collaborative framework represents a critical step in realizing the full potential of blockchain technology within the sector. By fostering a network of nodes distributed among key maritime entities, including port authorities, shipping lines, logistics providers, and regulatory bodies, we are paving the

way towards a transparent, efficient, and secure global maritime logistics landscape. This decentralized architecture, underpinned by the principles of immutability and consensus, promises to revolutionize the way data is shared, transactions are executed, and stakeholders collaborate within the intricate web of maritime operations. Imagine a future where cargo manifests, bills of lading, and customs clearances are seamlessly and securely shared in real-time, eliminating redundancies, errors, and delays that have long plagued the industry.

Recognizing the inherent complexities and operational intricacies of the maritime sector, this thesis proposes a pragmatic and incremental approach to blockchain integration. Our strategic roadmap advocates for a seamless yet performant infrastructure that minimizes disruption while maximizing the transformative impact of this disruptive technology. By meticulously aligning blockchain solutions with existing maritime operations and emphasizing user-centric interfaces, the proposed framework ensures a smooth transition towards digitized maritime processes. This holistic approach not only mitigates potential barriers to adoption but also cultivates an environment conducive to broad-scale acceptance and implementation. Through this strategic roadmap, we aim to catalyze a paradigm shift within the maritime industry, one that embraces the potential of blockchain while remaining grounded in the sector's operational realities.

In crafting this comprehensive exploration of blockchain technology's implications within the maritime sector, this thesis weaves together a multifaceted tapestry of contributions, both theoretical and practical, that collectively advance the understanding and application of blockchain in this critical domain. The contributions are manifold, spanning the analysis of extant blockchain projects in the maritime realm, the adaptation of research methodologies to the nuanced context of maritime logistics, the expansion of the academic corpus to address identified gaps, and the meticulous selection of a suitable blockchain application for the sector. Each of these elements represents a pivotal stride towards the overarching aim of harnessing blockchain technology for enhancing maritime operational efficiency, transparency, and security.

9.1 Future Directions : Sharding

Our discussion also acknowledges the broader implications of our research and the contributions made to the field of blockchain in maritime logistics. As we target the current status quo for maritime logistics and technological advancements, we also as part of our work would like to project prospects of future research direction that situates our PoC in line with blockchain technological advancement that stems from our analysis provided in Chapter 4. By situating our PoC within the framework of evolving blockchain technology, we acknowledge potential limitations that may not currently affect our PoC but could in the future. Delineating these limitations as part of our near-future work ensures the continued viability and optimal performance of our research in light of technological advancements.

Our interest in sharding stems from its potential synergy with Hyperledger Fabric (HF). HF's inherent features, such as channels for private and parallel transaction processing, and its plug-

Vertical & Horizontal Database Sharding

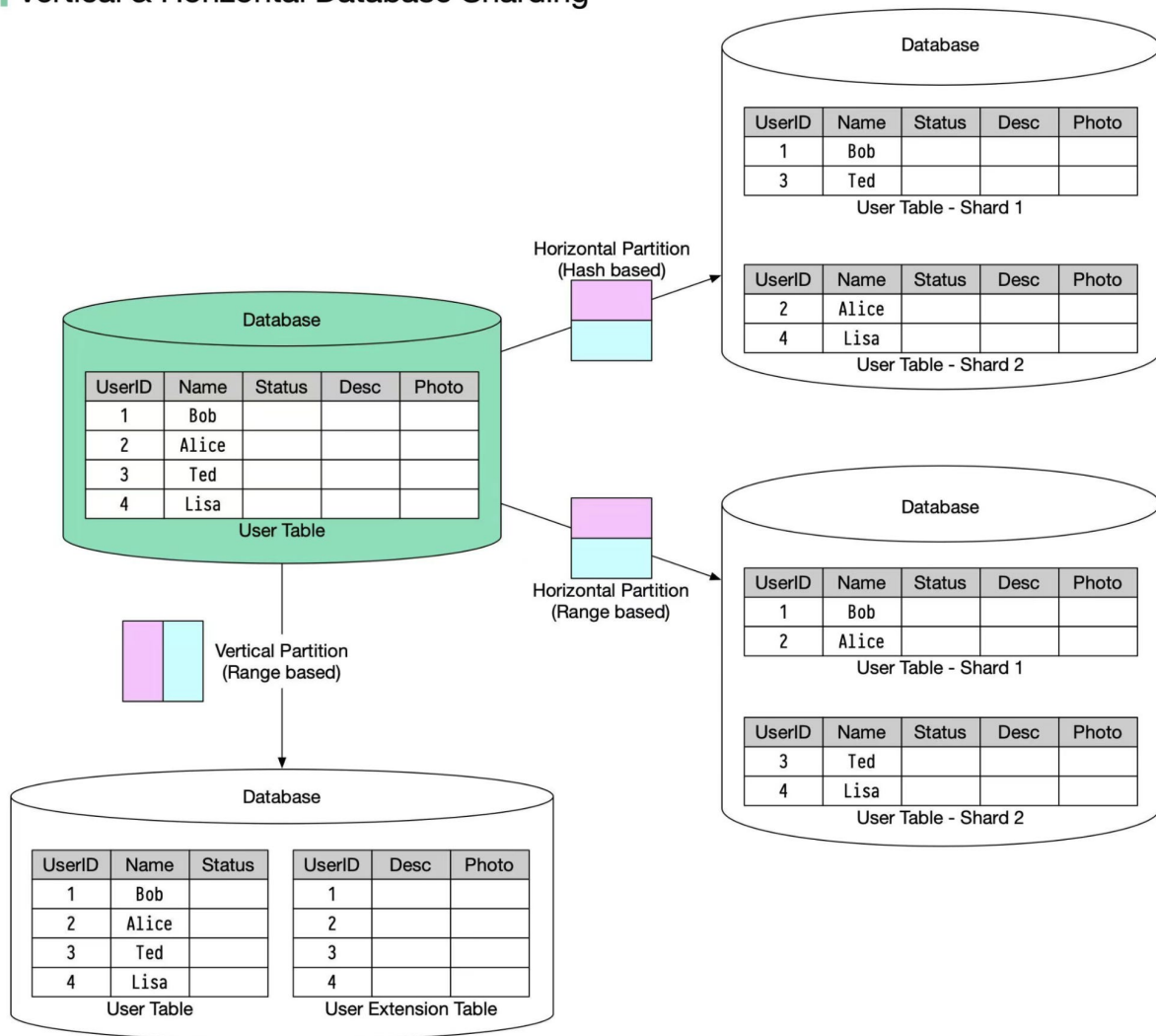


Figure 48: Database Sharding (ByteByteGo, 2024)

gale architecture that supports different ordering services with varying consensus algorithms, align well with sharding’s strengths.

Given the potential of sharding to address scalability challenges, we were particularly interested in further refined applications within HF notably within a maritime context.

Database Sharding is a database technique that would allow handle better storage scalability. Large database sets can be split into smaller more manageable chunks and stored scross multiple machines. In databases, we have two types of shardings (cf. Figure 48):

- **Horizontal Sharding** (also known as Data Sharding): The rows of a database table are split across multiple databases. This can be based on a hash of a key column to ensure even distribution (Hash-based) or by a range of values (Range-based).
- **Vertical Sharding:** The columns of a database table are split into different databases.

Blockchain Sharding partitions the blockchain into smaller, manageable segments known as shards, thereby significantly enhancing the system's capabilities. It can take several forms each designed to tackle specific challenges.

- **State Sharding:** As its name implies, this technique requires splitting the state of the blockchain (representing the current state of the distributed ledger after processing all previous valid transactions) (Kokoris-Kogias et al., 2018). Each shard maintains a portion of the state, meaning nodes only need to store and process transactions for their respective shards.
- **Transaction Sharding:** characterised by the distribution of TXs across various shards (group of nodes) each shard tasked with the independent processing of its specific set of transactions. This parallel processing capability augments the network's throughput. However, the challenges of inter-shard transactions rise (Zamani et al., 2018)
- **Network Sharding:** Network sharding entails the organization of nodes into distinct shards, each responsible for a subset of transactions (Danezis and Meiklejohn, 2015). This configuration is designed to minimise the overhead associated with node-to-node communication, as intra-shard communication predominates over inter-shard interactions, thereby contributing to the scalability of the network's infrastructure.
- **Data Sharding:** refers to the segmentation of the blockchain's ledger data across different shards. While akin to state sharding, data sharding concentrates more on the distribution of historical data storage(Wang et al., 2019b), aiming to mitigate the burden on any single node's storage capacity, thus facilitating scalability.

The process of allocating shards, known as shard formation typically involves random assignments. Consequently, the likelihood of encountering cross-shard transactions increases substantially. This limits the system's ability to scale effectively. According to (Zamani et al., 2018), in a 500-node network divided into 3 shards, with an average of 3 inputs and outputs per transaction, a staggering 96.3% of transactions involve multiple shards. In a larger 4000-node network split into 16 shards, the expected proportion of cross-shard transactions rises to an even more substantial 99.98%.

To project this into the context of our Poc and situated in coherence with maritime prospects. For maritime queries, often the engagement targets the current state of the Ledger, thus sharding can be employed to distribute the storage of the historical Ledger that can scale pretty fast with the multitude of stakeholders and data volumes of the maritime sector. Each shard of the ledger can be distributed across several replicated nodes to ensure data availability and respect blockchain concepts. This allows optimal storage distribution while guaranteeing the availability of historical data for accountability, transparency and better traceability.

To ensure the practical applicability and efficacy of this, a meticulous analysis and evaluation of sharding algorithms is indispensable. This endeavour necessitates a comprehensive understanding of the various sharding mechanisms, including state, transaction, network constraints and requirements, and data sharding, each with its unique strengths and challenges.

Critical analysis, following our approach in Chapter 4, is essential to identify the optimal algorithm driving these sharding strategies, examining factors such as shard formation, transaction processing efficiency, data consistency, and cross-shard communication. This analysis should employ both theoretical frameworks and empirical data, leveraging simulations or case studies within maritime contexts to discern the scalability, security, and performance implications of each sharding approach. Moreover, the refinement of these sharding algorithms must be informed by the real-world complexities of maritime logistics, which encompass high transaction volumes, robust security measures, and the demand for real-time data access across global supply chains. Consideration should be given to the integration challenges with existing maritime logistical systems, data privacy concerns, and the regulatory landscape governing maritime activities. The evaluation should extend our base historical ledger sharding proposition to explore the potential for hybrid sharding solutions that combine the strengths of different sharding types to address the specific demands of maritime logistics. Incorporating feedback loops for continuous improvement and scalability assessments will be crucial. This includes adapting sharding algorithms to accommodate evolutions within the sector. Furthermore, engaging with stakeholders from the maritime logistics field to gather insights and validate the practicality of these solutions will enrich the refinement process, ensuring the sharding approach remains responsive to the dynamic needs of the industry. Ultimately, this rigorous analysis and refinement process aims not only to enhance the performance and scalability of blockchain solutions in maritime logistics but also to foster and encourage innovation. As we did for our PoC, this future direction should be grounded in both theoretical rigour and practical insights. Researchers in collaboration with industry experts can contribute significantly to advancing innovation's role in reshaping maritime logistics for the better.

9.2 Conclusion

As we conclude this exploration, we recognize that the path forward is filled with both opportunities and challenges. The maritime logistics sector stands on the cusp of a digital revolution, with blockchain technology playing a pivotal role. Our commitment to innovation, rigorous testing, and stakeholder collaboration will be crucial in navigating the future of blockchain in maritime logistics. By continuously adapting to technological advancements and embracing new solutions like sharding techniques and scalable consensus algorithms, we aim to contribute to the development of a more efficient, transparent, and secure maritime logistics industry.

This journey, though concluded, marks the beginning of an exciting era of digital transformation within the maritime sector, promising to redefine the paradigms of global trade and

logistics. As we stand at the precipice of this new horizon, emboldened by the insights we have garnered and the challenges we have surmounted, we must embrace a posture of audacious curiosity and unwavering determination. The path ahead is arduous, but the promise it holds – that of unveiling deeper truths, fostering more equitable and sustainable practices, and contributing to the evolution of the maritime industry – is a clarion call that we cannot afford to ignore.

In undertaking this research, the importance of responsible knowledge pursuit has been paramount. The complexities of the maritime industry demand a thorough and ethical approach to identify areas for transformative change.

For it is in the crucible of intellectual rigour, ethical rectitude, and an unwavering commitment to progress that we shall find the courage and fortitude to confront the complexities that lie before us.

By critically examining these intricate complexities, this research endeavours to enrich and update the extant technological understanding within the maritime industry, elucidating the potential of advancements and the implementation and tangible utilization of sector-foreign complex technologies such as blockchain to enable this sector to fully harness its expansive capabilities.

BIBLIOGRAPHY

- Abdallah, R. and Abdallah, R. (2022). A blockchain based methodology for power grid control systems. In The International Conference on Innovations in Computing Research, pages 431–443. Springer.
- Abdallah, R., Bertelle, C., Besancenot, J., Duvallet, C., and Gilletta, F. (2023a). Repositioning blockchain technology in the maritime industry for increased accountability. In International Congress on Blockchain and Applications, pages 82–92. Springer.
- Abdallah, R., Bertelle, C., Duvallet, C., Besancenot, J., and Gilletta, F. (2022). Blockchain potentials in the maritime sector: A survey. In The International Conference on Innovations in Computing Research, pages 293–309. Springer.
- Abdallah, R., Bertelle, C., Duvallet, C., Besancenot, J., and Gilletta, F. (2023b). Blockchain for the maritime: A modular proposition. FRCCS 2023. Zenodo.
- Abdallah, R., Bertelle, C., Duvallet, C., Besancenot, J., and Gilletta, F. (2023c). Privileging permissioned blockchain deployment for the maritime sector. FRCCS 2023. Zenodo.
- Abdallah, R., Besancenot, J., Bertelle, C., Duvallet, C., and Gilletta, F. (2023d). Assessing blockchain challenges in the maritime sector. In Blockchain and Applications, 4th International Congress, pages 13–22. Springer.
- Abdallah, R., Besancenot, J., Bertelle, C., Duvallet, C., and Gilletta, F. (2023e). An extensive preliminary blockchain survey from a maritime perspective. Smart Cities, 6(2):846–877.
- Abdallah, R., Besancenot, J., Bertelle, C., Duvallet, C., and Gilletta, F. (2023f). Seamless seas leveraging blockchain. In Proceedings of the CCSET2023. Presented at CCSET2023. To be published in the IET Conference Proceedings.
- Acciaro, M., Ferrari, C., Lam, J. S., Macario, R., Roumboutsos, A., Sys, C., Tei, A., and Vanel-slander, T. (2018). Are the innovation processes in seaport terminal operations successful? Maritime Policy & Management, 45(6):787–802.
- Acciaro, M., Ghiara, H., and Cusano, M. I. (2014). Energy management in seaports: A new role for port authorities. Energy Policy, 71:4–12.
- Adler, J., Berryhill, R., Veneris, A., Poulos, Z., Veira, N., and Kastania, A. (2018). Astraea: A decentralized blockchain oracle. In 2018 IEEE international conference on internet of things (IThings) and IEEE green computing and communications (GreenCom) and IEEE

BIBLIOGRAPHY

- cyber, physical and social computing (CPSCoM) and IEEE smart data (SmartData), pages 1145–1152. IEEE.
- Afenyo, M. and Caesar, L. D. (2023). Maritime cybersecurity threats: Gaps and directions for future research. Ocean & Coastal Management, 236:106493.
- Aguilar, D. (22). Ethereum post-Merge hard forks are here — Now what? — coin-telegraph.com. <https://cointelegraph.com/news/ethereum-post-merge-hard-forks-are-here-now-what>. [Accessed 18-Nov-2022].
- Akidau, T., Balikov, A., Bekiroğlu, K., Chernyak, S., Haberman, J., Lax, R., McVeety, S., Mills, D., Nordstrom, P., and Whittle, S. (2013). Millwheel: Fault-tolerant stream processing at internet scale. Proceedings of the VLDB Endowment, 6(11):1033–1044.
- Al-Rakhami, M. and Al-Mashari, M. (2022). Interoperability approaches of blockchain technology for supply chain systems. Business process management journal, 28(5/6):1251–1276.
- Altarawneh, A., Herschberg, T., Medury, S., Kandah, F., and Skjellum, A. (2020). Buterin’s scalability trilemma viewed through a state-change-based classification for common consensus algorithms. In 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), pages 0727–0736. IEEE.
- Andersen, J. V. and Bogusz, C. I. (2019). Self-organizing in blockchain infrastructures: Generativity through shifting objectives and forking. Journal of the Association for Information Systems, 20(9):11.
- Andersen, T. (2009). E-government as an anti-corruption strategy. Information Economics and Policy, 21:201–210.
- Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., et al. (2018). Hyperledger fabric: a distributed operating system for permissioned blockchains. In Proceedings of the thirteenth EuroSys conference, pages 1–15.
- Androulaki, E., Camenisch, J., Caro, A. D., Dubovitskaya, M., Elkhiyaoui, K., and Tackmann, B. (2020). Privacy-preserving auditable token payments in a permissioned blockchain system. In Proceedings of the 2nd ACM Conference on Advances in Financial Technologies, pages 255–267.
- Androutsellis-Theotokis, S. and Spinellis, D. (2004). A survey of peer-to-peer content distribution technologies. ACM computing surveys (CSUR), 36(4):335–371.
- Antonopoulos, A. M. and Wood, G. (2018). Mastering ethereum: building smart contracts and dapps. O’reilly Media.

- antonylewis2015 (2017). Three common misconceptions about smart contracts – Bits on Blocks — bitsonblocks.net. <https://bitsonblocks.net/2017/03/07/three-common-misconceptions-about-smart-contracts/>. [Accessed 17-Nov-2022].
- Arayankalam, J., Khan, A., and Krishnan, S. (2021). How to deal with corruption? examining the roles of e-government maturity, government administrative effectiveness, and virtual social networks diffusion. *International Journal of Information Management*, 58:102203.
- Arduino, G., Aronietis, R., Crozet, Y., Frouws, K., Ferrari, C., Guihéry, L., Kapros, S., Kourounioti, I., Laroche, F., Lambrou, M., et al. (2013). How to turn an innovative concept into a success? an application to seaport-related innovation. *Research in Transportation Economics*, 42(1):97–107.
- Asare, A. K., Brashear-Alejandro, T. G., and Kang, J. (2016). B2b technology adoption in customer driven supply chains. *Journal of Business & Industrial Marketing*, 31(1):1–12.
- Ávila-Zúñiga-Nordfjeld, A., Liwång, H., and Dalaklis, D. (2023). Implications of technological innovation and respective regulations to strengthen port and maritime security: An international agenda to reduce illegal drug traffic and countering terrorism at sea. In *Smart Ports and Robotic Systems: Navigating the Waves of Techno-Regulation and Governance*, pages 135–147. Springer.
- Back, A. (1997). Hashcash. 1997. URL: <http://www.hashcash.org> (cit. on p. 3).
- Balaji, S., Krishnan, M. N., Vajha, M., Ramkumar, V., Sasidharan, B., and Kumar, P. V. (2018). Erasure coding for distributed storage: An overview. *Science China Information Sciences*, 61:1–45.
- Bank, W. (2020). *Accelerating Digitalization: Critical Actions to Strengthen the Resilience of the Maritime Supply Chain*. World Bank.
- Barnawi, A., Aggarwal, S., Kumar, N., Alghazzawi, D. M., Alzahrani, B., and Boulares, M. (2021). Path planning for energy management of smart maritime electric vehicles: A blockchain-based solution. *IEEE Transactions on Intelligent Transportation Systems*.
- Bauk, S. (2022). Maritime blockchain conceptual framework and blockshipping application. In *2022 11th Mediterranean Conference on Embedded Computing (MECO)*, pages 1–6. IEEE.
- Bayer, D., Haber, S., and Stornetta, W. S. (1993). Improving the efficiency and reliability of digital time-stamping. In *Sequences II: Methods in Communication, Security, and Computer Science*, pages 329–334. Springer.
- Beck, R., Avital, M., Rossi, M., and Thatcher, J. (2018). Blockchain technology in business and information systems research. *Business & Information Systems Engineering*, 60(6):381–384.

BIBLIOGRAPHY

- Belchior, R., Vasconcelos, A., Guerreiro, S., and Correia, M. (2021). A survey on blockchain interoperability: Past, present, and future trends. ACM Comput. Surv., 54(8).
- Benet, J. (2017). Filecoin research roadmap for 2017. Protocol Labs: An Open-Source Research, Development, and Deployment Laboratory, pages 1–6.
- Benhamouda, F., Gentry, C., Gorbunov, S., Halevi, S., Krawczyk, H., Lin, C., Rabin, T., and Reyzin, L. (2020). Can a public blockchain keep a secret? In Theory of Cryptography: 18th International Conference, TCC 2020, Durham, NC, USA, November 16–19, 2020, Proceedings, Part I 18, pages 260–290. Springer.
- Beniiche, A. (2020). A study of blockchain oracles. arXiv preprint arXiv:2004.07140.
- Bernardi, T., Dor, N., Fedotov, A., Grossman, S., Immerman, N., Jackson, D., Nutz, A., Oppenheim, L., Pistiner, O., Rinetzky, N., et al. (2020). Wip: Finding bugs automatically in smart contracts with parameterized invariants. Retrieved July, 14:2020.
- Bichou, K. (2013). An empirical study of the impacts of operating and market conditions on container-port efficiency and benchmarking. Research in Transportation Economics, 42(1):28–37.
- Blockchaining.org (2023). Discontinuation of tradelens: The end of a blockchain-enabled global trade platform by maersk and ibm. <https://blockchaining.org/2023/02/12/end-of-blockchain-trade-platform.html>. [Online; accessed 15-January-2024].
- Bodó, B., Brekke, J. K., and Hoepman, J.-H. (2021). Decentralisation: A multidisciplinary perspective. Internet Policy Review, 10(2):1–21.
- Bonuedi, I., Kamasa, K., and Opoku, E. E. O. (2020). Enabling trade across borders and food security in africa. Food Security, 12(5):1121–1140.
- Botton, N. (2018). Blockchain and trade: Not a fix for brexit, but could revolutionise global value chains (if governments let it). ECIPE Policy Brief 1/2018, European Centre for International Political Economy, Brussels.
- Boullauazan, Y., Sys, C., and Vanelslander, T. (2023). Developing and demonstrating a maturity model for smart ports. Maritime Policy & Management, 50(4):447–465.
- Broeze, F. (2017). The Globalisation of the Oceans: Containerisation from the 1950s to the Present. Liverpool University Press.
- Brooks, M., Pallis, A., and Perkins, S. (2014). Port Investment and Container Shipping Markets (DP 2014-03). OECD International Transport Forum.

- Brooks, M. R. and Cullinane, K. (2006). Devolution, port governance and port performance. Elsevier.
- Brunila, O.-P., Kunnaala-Hyrkki, V., and Inkinen, T. (2021). Hindrances in port digitalization? identifying problems in adoption and implementation. European Transport Research Review, 13:1–10.
- Bryman, A. (2016). Social research methods. Oxford university press.
- Buterin, V. (2016). Ethereum: platform review. Opportunities and Challenges for Private and Consortium Blockchains, 45.
- Buterin, V. et al. (2013). Ethereum white paper. GitHub repository, 1:22–23.
- Buterin, V. et al. (2014). A next-generation smart contract and decentralized application platform. white paper, 3(37):2–1.
- ByteByteGo (2024). Vertical partitioning vs. horizontal partitioning.
- Cachin, C. et al. (2016). Architecture of the hyperledger blockchain fabric. In Workshop on distributed cryptocurrencies and consensus ledgers, volume 310, pages 1–4. Chicago, IL.
- Cai, Y. and Zhu, D. (2016). Fraud detections for online businesses: a perspective from blockchain technology. Financial Innovation, 2:1–10.
- Calatayud, A., Palacin, R., Mangan, J., Jackson, E., and Ruiz-Rua, A. (2016). Understanding connectivity to international markets: a systematic review. Transport Reviews, 36(6):713–736.
- Caldeirinha, V., Felício, J. A., Salvador, A. S., Nabais, J., and Pinho, T. (2020). The impact of port community systems (pcs) characteristics on performance. Research in Transportation Economics, 80:100818.
- Caldeirinha, V., Nabais, J. L., and Pinto, C. (2022). Port community systems: accelerating the transition of seaports toward the physical internet—the portuguese case. Journal of Marine Science and Engineering, 10(2):152.
- Carlan, V., Sys, C., and Vanelslander, T. (2016a). How port community systems can contribute to port competitiveness: Developing a cost–benefit framework. Research in transportation business & management, 19:51–64.
- Carlan, V., Sys, C., and Vanelslander, T. (2016b). How port community systems can contribute to port competitiveness: Developing a cost–benefit framework. Research in Transportation Business Management, 19:51–64.

BIBLIOGRAPHY

- Carlan, V., Sys, C., Vanelslander, T., and Roumboutsos, A. (2017). Digital innovation in the port sector: Barriers and facilitators. Competition and regulation in network industries, 18(1-2):71–93.
- Certora (2024). Certora Prover.
- Chang, Y.-C., Lin, Z.-S., and Chen, J.-L. (2006). Cluster based self-organization management protocols for wireless sensor networks. IEEE Transactions on Consumer Electronics, 52(1):75–80.
- Chanson, M., Bogner, A., Bilgeri, D., Fleisch, E., and Wortmann, F. (2019). Blockchain for the iot: privacy-preserving protection of sensor data. Journal of the Association for Information Systems, 20(9):1274–1309.
- Chen, Y., Li, H., Li, K., and Zhang, J. (2017a). An improved p2p file system scheme based on ipfs and blockchain. In 2017 IEEE International Conference on Big Data (Big Data), pages 2652–2657. IEEE.
- Chen, Y., Li, H., Li, K., and Zhang, J. (2017b). An improved p2p file system scheme based on ipfs and blockchain. In 2017 IEEE International Conference on Big Data (Big Data), pages 2652–2657. IEEE.
- Chew, S. C. (2001). World ecological degradation: Accumulation, urbanization, and deforestation, 3000 BC-AD 2000. Rowman Altamira.
- Choi, J. Y. (2011). A survey of single window implementation. WCO research Paper, 17:11–20.
- Christidis, K. and Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. Ieee Access, 4:2292–2303.
- Cohen, L., Manion, L., and Morrison, K. (2002). Research methods in education. routledge.
- CoinWarz (2023). Bitcoin hashrate chart. <https://www.coinwarz.com/mining/bitcoin/hashrate-chart/2023>. Accessed: 2023-11-19.
- Conti, M., Kumar, E. S., Lal, C., and Ruj, S. (2018). A survey on security and privacy issues of bitcoin. IEEE communications surveys & tutorials, 20(4):3416–3452.
- Coulouris, G. F., Dollimore, J., and Kindberg, T. (2005). Distributed systems: concepts and design. pearson education.
- Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V., et al. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation, 2(6-10):71.

- Czachorowski, K., Solesvik, M., and Kondratenko, Y. (2019a). The application of blockchain technology in the maritime industry. In Green IT Engineering: Social, Business and Industrial Applications, pages 561–577. Springer.
- Czachorowski, K., Solesvik, M., and Kondratenko, Y. (2019b). The application of blockchain technology in the maritime industry. In Green IT engineering: Social, business and industrial applications, pages 561–577. Springer.
- da Silva, F. J. C., Damsgaard, S. B., Sorensen, M. A. M., Marty, F., Altariqi, B., Chatzigianni, E., Madsen, T. K., and Schwefel, H. P. (2019). Analysis of blockchain forking on an ethereum network. In European Wireless 2019; 25th European Wireless Conference, pages 1–6. VDE.
- Dahiya, S., Yermack, D., and Srinivasan, S. (2017). Why good companies go bad: An analysis of corporate governance failures. In Vo, T.-N. T. and Vandekerckhove, W. A., editors, The Financial Crisis and Corporate Governance, chapter 4. JAI Press.
- Dai, J., He, N., and Yu, H. (2019). Utilizing blockchain and smart contracts to enable audit 4.0: From the perspective of accountability audit of air pollution control in china. Journal of Emerging Technologies in Accounting, 16(2):23–41.
- Dai, M., Zhang, S., Wang, H., and Jin, S. (2018). A low storage requirement framework for distributed ledger in blockchain. IEEE access, 6:22970–22975.
- Danezis, G. and Meiklejohn, S. (2015). Centrally banked cryptocurrencies. arXiv preprint arXiv:1505.06895.
- de Commerce de Port-La Nouvelle, P. (2023). Port la nouvelle. <https://www.port-la-nouvelle.com/>. Accessed: 2024-04-13.
- de Souza, R. C., Luciano, E. M., and Wiedenhöft, G. C. (2018a). The uses of the blockchain smart contracts to reduce the levels of corruption. In Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age. ACM.
- de Souza, R. C., Luciano, E. M., and Wiedenhöft, G. C. (2018b). The uses of the blockchain smart contracts to reduce the levels of corruption: Some preliminary thoughts. In Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age, pages 1–2.
- de Tazoult, C. T., Chiky, R., and Foltescu, V. (2019). A distributed pollution monitoring system: The application of blockchain to air quality monitoring. In Computational Collective Intelligence, pages 688–697. Springer International Publishing.
- Desiderio, D. (2011). Port community systems, customs one-stop-shops and their possible combination with a single window. J. Cust. Trade, 3:3–14.

BIBLIOGRAPHY

- DeWitt, D., Ghandeharizadeh, S., Schneider, D., Bricker, A., Hsiao, H.-I., and Rasmussen, R. (1990). The gamma database machine project. IEEE Transactions on Knowledge and Data Engineering, 2(1):44–62.
- Dewulf, W., Dekker, R., Notteboom, T., and Van Hooydonk, E. (2015). Digitalization of port logistics: A review of the port of rotterdam. Maritime Economics & Logistics, 17(1):1–18.
- Di Gregorio, R., Nustad, S. S., and Constantiou, I. (2017). Blockchain adoption in the shipping industry. A study of adoption likelihood and scenario-based opportunities and risks for IT service providers, Copenhagen Business School, Number of STUs, 272.
- Dib, O., Brousmiche, K.-L., Durand, A., Thea, E., and Hamida, E. B. (2018). Consortium blockchains: Overview, applications and challenges. International Journal On Advances in Telecommunications, 11(1&2):51–64.
- Dib, O. and Toumi, K. (2020a). Decentralized identity systems: Architecture, challenges, solutions and future directions. Annals of Emerging Technologies in Computing.
- Dib, O. and Toumi, K. (2020b). Decentralized identity systems: Architecture, challenges, solutions and future directions. Annals of Emerging Technologies in Computing (AETiC), Print ISSN, pages 2516–0281.
- Digiconomist (2024). Bitcoin Energy Consumption Index.
- Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., and Wang, J. (2018). Untangling blockchain: A data processing view of blockchain systems. IEEE transactions on knowledge and data engineering, 30(7):1366–1385.
- DiRenzo, J., Goward, D. A., and Roberts, F. S. (2015). The little-known challenge of maritime cyber security. In 2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA), pages 1–5. IEEE.
- Doerry, N. and Fireman, H. (2009). Fleet capabilities-based assessment. Naval Engineers Journal, 121(4):107–116.
- Dutta, P., Choi, T.-M., Somani, S., and Butala, R. (2020). Blockchain technology in supply chain operations: Applications, challenges and research opportunities. Transportation research part e: Logistics and transportation review, 142:102067.
- ecologie.gouv.fr (2022). Le guichet unique maritime et portuaire (GUMP) — ecologie.gouv.fr. https://www.ecologie.gouv.fr/guichet-unique-maritime-et-portuaire-gump#scroll-nav__2. [Accessed 17-Nov-2022].
- Egberts, A. (2017). The oracle problem-an analysis of how blockchain oracles undermine the advantages of decentralized ledger systems. Available at SSRN 3382343.

- Ekström, L. (2018). Estimating fuel consumption using regression and machine learning.
- Elineau, S., Duperret, A., Mallet, P., and Caspar, R. (2011). Urban tidal flooding in normandy (le havre, nw france). In Geophysical Research Abstracts, volume 13, page 201.
- etherpot (2024). EtherPot.
- Eyal, I. and Sirer, E. G. (2018). Majority is not enough: Bitcoin mining is vulnerable. Communications of the ACM, 61(7):95–102.
- Fedi, L., Lavissiere, A., Russell, D., and Swanson, D. (2019). The facilitating role of IT systems for legal compliance: the case of port community systems and container verified gross mass (VGM). Supply Chain Forum: An International Journal, 20(1):29–42.
- Finextra (2016). Marine Transport International applies blockchain to shipping supply chain.
- Finley, K. (2016). Someone Just Stole \$50 Million from the Biggest Crowdfunded Project Ever. (Humans Can't Be Trusted). Wired.
- for Standardization, I. O. (2022). ISO 6346:Freight containers Coding, identification and marking. ISO Standard No. 83558.
- Freedman, M. J. and Mazieres, D. (2003). Sloppy hashing and self-organizing clusters. In Peer-to-Peer Systems II: Second International Workshop, IPTPS 2003, Berkeley, CA, USA, February 21-22, 2003. Revised Papers 2, pages 45–55. Springer.
- Ganne, E. (2018). Can Blockchain revolutionize international trade? World Trade Organization Geneva.
- Gao, J., Li, B., and Li, Z. (2020). Blockchain storage analysis and optimization of bitcoin miner node. In Communications, Signal Processing, and Systems: Proceedings of the 2018 CSPS Volume III: Systems 7th, pages 922–932. Springer.
- Gaukler, G. M. and Seifert, R. W. (2007). Applications of rfid in supply chains. Trends in supply chain design and management: technologies and methodologies, pages 29–48.
- GCaptain (2014). IMO Approves SOLAS Container Weight Verification Amendments.
- Genç, Y. and Afacan, E. (2021). Design and implementation of an efficient elliptic curve digital signature algorithm (ecdsa). In 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), pages 1–6. IEEE.
- Gligor, D. M. and Holcomb, M. C. (2012). Antecedents and consequences of supply chain agility: establishing the link to firm performance. Journal of Business logistics, 33(4):295–308.

BIBLIOGRAPHY

- Gold, E. (1999a). Learning from disaster: lessons in regulatory enforcement in the maritime sector. Rev. Eur. Comp. & Int'l Envtl. L., 8:16.
- Gold, E. (1999b). Learning from disaster: lessons in regulatory enforcement in the maritime sector. Rev. Eur. Comp. & Int'l Envtl. L., 8:16.
- Grimmer, R. (2018). Imo 2020 part 5: Enforcement. <https://stillwaterassociates.com/imo-2020-part-5-enforcement/>.
- Grosman-Rimon, L., Li, D. H., Collins, B. E., and Wegier, P. (2023). Can we improve health-care with centralized management systems, supported by information technology, predictive analytics, and real-time data?: A review. Medicine, 102(45):e35769.
- GS1 Switzerland (2022). GS1 Standards. <https://www.gs1.ch/en/barcodes-standards/gs1-standards>. Accessed: 2023-04-10.
- Gu, B. and Liu, J. (2023). A systematic review of resilience in the maritime transport. International Journal of Logistics Research and Applications, pages 1–22.
- Haber, S. and Stornetta, W. S. (1990). How to time-stamp a digital document. In Conference on the Theory and Application of Cryptography, pages 437–455. Springer.
- Haber, S. and Stornetta, W. S. (1991). How to time-stamp a digital document. Springer.
- Hampstead, J. (2018). Swiss firm brings blockchain to the biopharmaceutical cold chain. freightwaves.
- Haring, T. W., Mathieu, J. L., and Andersson, G. (2015). Comparing centralized and decentralized contract design enabling direct load control for reserves. IEEE Transactions on Power Systems, 31(3):2044–2054.
- Hasan, R., Sion, R., and Winslett, M. (2009). Sprov 2.0: A highly-configurable platform-independent library for secure provenance. In ACM Conference on Computer and Communications Security (CCS), page 122.
- He, J., Balunović, M., Ambroladze, N., Tsankov, P., and Vechev, M. (2019). Learning to fuzz from symbolic execution with application to smart contracts. In Proceedings of the 2019 ACM SIGSAC conference on computer and communications security, pages 531–548.
- Heilig, L., Lalla-Ruiz, E., and Voß, S. (2017). Digital transformation in maritime ports: analysis and a game theoretic framework. Netnomics: Economic research and electronic networking, 18(2):227–254.
- Heilig, L. and Voß, S. (2017). Information systems in seaports: a categorization and overview. Information Technology and Management, 18:179–201.

- Henesey, L., Notteboom, T., and Davidsson, P. (2003). Agent-based simulation of stakeholders relations: An approach to sustainable port and terminal management. Multi-Agent Systems for Container Terminal Management, 99.
- Hesarkazzazi, S., Bakhshipour, A. E., Hajibabaei, M., Dittmer, U., Haghghi, A., and Sitzenfrei, R. (2022). Battle of centralized and decentralized urban stormwater networks: from redundancy perspective. Water Research, 222:118910.
- Hoagland, P., Steele, J. H., Thorpe, S., and Turekian, K. K. (2010). Marine policy & economics: a derivative of encyclopedia of ocean sciences. (No Title).
- Howard, H., Schwarzkopf, M., Madhavapeddy, A., and Crowcroft, J. (2015). Raft refloated: Do we have consensus? ACM SIGOPS Operating Systems Review, 49(1):12–21.
- <https://dfreight.org/> (2022). What Is the Cheapest Shipping Method? — dfreight.org. <https://dfreight.org/blog/what-is-the-cheapest-shipping-method-in-2022/>. [Accessed 18-Nov-2022].
- Huang, H.-L., Zhao, Y.-W., Li, T., Li, F.-G., Du, Y.-T., Fu, X.-Q., Zhang, S., Wang, X., and Bao, W.-S. (2017). Homomorphic encryption experiments on ibm’s cloud quantum computing platform. Frontiers of Physics, 12:1–6.
- Huang, J., Kong, L., Chen, G., Wu, M.-Y., Liu, X., and Zeng, P. (2019). Towards secure industrial iot: Blockchain system with credit-based consensus mechanism. IEEE Transactions on Industrial Informatics, 15(6):3680–3689.
- IBM (2022). IBM - United States.
- IMO (2016). Verification of the gross mass of a packed container. <https://www.imo.org/en/OurWork/Safety/Pages/Verification-of-the-gross-mass.aspx>. Accessed: 2023-10-06.
- international maritime orgainzation (2022). Single window for ship data exchange to become mandatory.
- International Maritime Organization (2022). Interim guidelines for development and application of e-navigation. Technical Report FAL.16(47), IMO.
- International Maritime Organization (2023). Mandatory maritime single window: One year to go. <https://www.imo.org/en/MediaCentre/PressBriefings/pages/Mandatory-Maritime-Single-Window-One-year-to-go-.aspx>. Accessed: 2023-1-2.
- IPCSA (2022). Port community systems. <https://ipcsa.international/pcs/pcs-general/>. [Accessed 16-Nov-2022].

BIBLIOGRAPHY

- Jamilov, R., Rey, H., and Tahoun, A. (2021). The anatomy of cyber risk. Technical report, National Bureau of Economic Research.
- Jensen, T., Bjørn-Andersen, N., and Vatrapu, R. (2014). Avocados crossing borders: the missing common information infrastructure for international trade. In Proceedings of the 5th ACM international conference on Collaboration across boundaries: culture, distance & technology, pages 15–24.
- Jensen, T., Hedman, J., and Henningsson, S. (2019). How tradelens delivers business value with blockchain technology. MIS Quarterly Executive, 18(4).
- Jiang, Y., Xu, X., Gao, H., Rajab, A. D., Xiao, F., and Wang, X. (2022). Lblockchaine: A lightweight blockchain for edge iot-enabled maritime transportation systems. IEEE Transactions on Intelligent Transportation Systems, 24(2):2307–2321.
- Jin, H., Dai, X., and Xiao, J. (2018). Towards a novel architecture for enabling interoperability amongst multiple blockchains. In 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), pages 1203–1211. IEEE.
- Jotun.com (2022). How technology is transforming shipping | Jotun — jotun.com. <https://www.jotun.com/ww-en/industries/news-and-stories/jotun-insider/how-technology-is-transforming-shipping>. [Accessed 16-Nov-2022].
- Jović, M., Tijan, E., Žgaljić, D., and Aksentijević, S. (2020). Improving maritime transport sustainability using blockchain-based information exchange. Sustainability, 12(21):8866.
- Kalgora, B. and Christian, T. M. (2016). The Financial and Economic Crisis, Its Impacts on the Shipping Industry, Lessons to Learn: The Container-Ships Market Analysis. Open Journal of Social Sciences, 4(1):38–44.
- Kapidani, N., Bauk, S., and Davidson, I. E. (2020). Digitalization in developing maritime business environments towards ensuring sustainability. Sustainability, 12(21):9235.
- Kapidani, N., Bauk, S., and Davidson, I. E. (2021). Developing countries’ concerns regarding blockchain adoption in maritime. Journal of Marine Science and Engineering, 9(12):1326.
- Kaplan, R. S. and Norton, D. P. (2004). The strategy map: guide to aligning intangible assets. Strategy & leadership.
- Kelepouris, T., Pramataris, K., and Doukidis, G. (2007). Rfid-enabled traceability in the food supply chain. Industrial Management & data systems, 107(2):183–200.
- Khan, M. A. and Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82:395–411.

- Khatal, S., Rane, J., Patel, D., Patel, P., and Busnel, Y. (2021). Fileshare: A blockchain and ipfs framework for secure file sharing and data provenance. In Advances in Machine Learning and Computational Intelligence: Proceedings of ICMLCI 2019, pages 825–833. Springer.
- Kim, S. and Deka, G. C. (2020). Advanced applications of blockchain technology. Springer.
- King, S. and Nadal, S. (2012). Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. self-published paper, August, 19(1).
- Kivo, D. (2018). The \$55 million mistake that vitalik buterin made with ethereum.
- Köhler, S. and Pizzol, M. (2020). Technology assessment of blockchain-based technologies in the food supply chain. Journal of cleaner production, 269:122193.
- Köhler, S. and Pizzol, M. (2020). Technology assessment of blockchain-based technologies in the food supply chain. Journal of Cleaner Production, 269:122193.
- Kokoris-Kogias, E., Jovanovic, P., Gasser, L., Gailly, N., Syta, E., and Ford, B. (2018). Omniledger: A secure, scale-out, decentralized ledger via sharding. In 2018 IEEE symposium on security and privacy (SP), pages 583–598. IEEE.
- Kshetri, N. (2018). Can blockchain strengthen the internet of things? IT Professional, 20(4):68–72.
- Kshetri, N. and Voas, J. (2018). Blockchain in developing countries. It Professional, 20(2):11–14.
- Kuehne + Nagel (2018). Kuehne + nagel deploys blockchain technology for vgm portal. Accessed: 2023-11-11.
- Kwon, J. and Buchman, E. (2019). Cosmos whitepaper. A Netw. Distrib. Ledgers, 27:1–32.
- Kyriakoulis, A. and Botham, J. (2018). Ports & terminals in the united kingdom. <https://www.lexology.com/library/detail.aspx?g=6fa96be5-8e06-4084-b76f-b6419ddb0c6e>. Accessed: 2024-04-12.
- Lafourcade, P. and Lombard-Platet, M. (2020). About blockchain interoperability. Information Processing Letters, 161:105976.
- Lamport, L. and Lynch, N. A. (1989). Chapter on distributed computing. Massachusetts Institute of Technology, Laboratory for Computer Science.
- Lee, J. M.-y. and Wong, E. Y.-c. (2021). Suez canal blockage: an analysis of legal impact, risks and liabilities to the global supply chain. In MATEC web of conferences, volume 339, page 1019. EDP Sciences.

BIBLIOGRAPHY

- Lee, P. T.-W. and Lam, J. S. L. (2016). Developing the fifth generation ports model. Dynamic Shipping and Port Development in the Globalized Economy: Volume 2: Emerging Trends in Ports, pages 186–210.
- Lehmacher, W. (2017). Why blockchain should be global trade's next port of call. In World Economic Forum, volume 23.
- Leible, S., Schlager, S., Schubotz, M., and Gipp, B. (2019). A review on blockchain technology and blockchain projects fostering open science. Frontiers in Blockchain, page 16.
- Li, Z., Xu, M., and Shi, Y. (2014). Centrality in global shipping network basing on worldwide shipping areas. GeoJournal, 80(1):47–60.
- Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., and Njilla, L. (2017). Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), pages 468–477. IEEE.
- Lieber, A. (2017). Trust in trade: Announcing a new blockchain partner.
- Lind, M., Michaelides, M., Ward, R., and Watson, R. T. (2021). Maritime informatics. Springer.
- Line, O. O. C. (2024). Verified Gross Mass (VGM) requirements under the Safety of Life at Sea (SOLAS) Convention. <https://www.oocl.com/eng/resourcecenter/vgm/Pages/default.aspx>. Accessed: 2024-03-21.
- Lio, M.-C., Liu, M.-C., and Ou, Y.-P. (2011). Can the internet reduce corruption? a cross-country study based on dynamic panel data models. Government Information Quarterly, 28(1):47–53.
- Liu, J., Zhang, H., and Zhen, L. (2023). Blockchain technology in maritime supply chains: Applications, architecture and challenges. International Journal of Production Research, 61(11):3547–3563.
- Liu, Y., Wang, K., Lin, Y., and Xu, W. (2019). Lightchain : a lightweight blockchain system for industrial internet of things. IEEE Transactions on Industrial Informatics, 15(6):3571–3581.
- Lorenz-Meyer, F. and Santos, V. (2023). Blockchain in the shipping industry: A proposal for the use of blockchain for smes in the maritime industry. Procedia Computer Science, 219:807–814. [Online; accessed 12-January-2023].
- Louw-Reimer, J., Nielsen, J. L. M., Bjørn-Andersen, N., and Kouwenhoven, N. (2021). Boosting the effectiveness of containerised supply chains: A case study of tradelens. In Maritime Informatics: Additional Perspectives and Applications, pages 95–115. Springer.

- Lynch, S. (2018). OpenLitterMap.com – open data on plastic pollution with blockchain rewards (littercoin). Open Geospatial Data, Software and Standards, 3(1).
- Lyon, K. (2022). Tradelens' demise is not a blockchain failure. <https://www.ti-insight.com/briefs/tradelens-demise-is-not-a-blockchain-failure/>. [Online; accessed 15-January-2024].
- Maldonado-Ruiz, D., Torres, J., El Madhoun, N., and Badra, M. (2021). An innovative and decentralized identity framework based on blockchain technology. In 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS), pages 1–8. IEEE.
- Mansfield-Devine, S. (2018). Critical infrastructure: understanding the threat. Computer Fraud & Security, 2018(7):16–20.
- Marchesi, L., Marchesi, M., Destefanis, G., Barabino, G., and Tigano, D. (2020). Design patterns for gas optimization in ethereum. In 2020 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE), pages 9–15. IEEE.
- Mathews, L. (2017). Notpetya ransomware attack cost shipping giant maersk over 200 million. <https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/>.
- Maymounkov, P. and Mazieres, D. (2002). Kademia: A peer-to-peer information system based on the xor metric. In International Workshop on Peer-to-Peer Systems, pages 53–65. Springer.
- Melo, C., Oliveira, F., Dantas, J., Araujo, J., Pereira, P., Maciel, R., and Maciel, P. (2022). Performance and availability evaluation of the blockchain platform hyperledger fabric. The Journal of Supercomputing, 78(10):12505–12527.
- Merk, O., Ducruet, C., Dubarle, P., Haezendonck, E., and Dooms, M. (2011). The competitiveness of global port-cities: the case of the seine axis (le havre, rouen, paris, caen), france. OECD Working Papers on Regional Development.
- Merkle, R. C. (1987). A digital signature based on a conventional encryption function. In Conference on the theory and application of cryptographic techniques, pages 369–378. Springer.
- Miseviciute, J. (2018). Blockchain and virtual currency regulation in the eu. Journal of Investment Compliance, 19(3):33–38.
- Morley, H. (2017). Industry skeptical of pace of logistics tech adoption. JOC: New York, NY, USA.
- Nakamoto, S. (2008a). Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, page 21260.

BIBLIOGRAPHY

- Nakamoto, S. (2008b). A peer-to-peer electronic cash system. Bitcoin.–URL: <https://bitcoin.org/bitcoin.pdf>, 4(2):15.
- Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press.
- Nathani, M. U. and Singh, J. S. K. (2020). Using blockchain for effective risk management in supply chain: A qualitative study. Global Business & Management Research, 12(3).
- Ndanu, M. C. and Syombua, M. J. (2015). Mixed methods research: The hidden cracks of the triangulation. Name: General Education Journal, 4(2).
- Network, D. (2021). Decentralized information asset (dia). <https://docs.diadata.org/documentation>.
- Nguyen, L. N., Nguyen, T. D., Dinh, T. N., and Thai, M. T. (2019). Optchain: optimal transactions placement for scalable blockchain sharding. In 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), pages 525–535. IEEE.
- Nguyen, S., Chen, P. S.-L., and Du, Y. (2022). Risk assessment of maritime container shipping blockchain-integrated systems: An analysis of multi-event scenarios. Transportation Research Part E: Logistics and Transportation Review, 163:102764.
- Nizamuddin, N., Salah, K., Azad, M. A., Arshad, J., and Rehman, M. (2019). Decentralized document version control using ethereum blockchain and ipfs. Computers & Electrical Engineering, 76:183–197.
- Notteboom, T. E. and Winkelmanns, W. (2001). Structural changes in logistics: how will port authorities face the challenge? Maritime Policy & Management, 28(1):71–89.
- Orcutt, M. (2019). Once hailed as unhackable, blockchains are now getting hacked. Technology Review.
- Palai, A., Vora, M., and Shah, A. (2018). Empowering light nodes in blockchains with block summarization. In 2018 9th IFIP international conference on new technologies, mobility and security (NTMS), pages 1–5. IEEE.
- Pallis, A. (2023). Port governance and reform. <https://porteconomicsmanagement.org/pemp/contents/part4/port-reform-and-governance/>. Accessed: 2024-04-12.
- Pansiri, J. (2005). Pragmatism: A methodological approach to researching strategic alliances in tourism. Tourism and Hospitality Planning & Development, 2(3):191–206.
- Park, J., Kim, H., Kim, G., and Ryou, J. (2020). Smart contract data feed framework for privacy-preserving oracle system on blockchain. Computers, 10(1):7.

- Pasdar, A., Lee, Y. C., and Dong, Z. (2023). Connect api with blockchain: A survey on blockchain oracle implementation. ACM Computing Surveys, 55(10):1–39.
- Pavlo, A. and Aslett, M. (2016). What’s really new with newsql? ACM Sigmod Record, 45(2):45–55.
- PierNext (2023). The closure of tradelens: when technology is not enough. <https://piernext.portdebarcelona.cat/en/technology/the-closure-of-tradelens/>. [Online; accessed 24-September-2023].
- Pontiveros, B. B. F., Norvill, R., and State, R. (2018). Recycling smart contracts: Compression of the ethereum blockchain. In 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), pages 1–5. IEEE.
- Popper, N. (2015). Digital gold: Bitcoin and the inside story of the misfits and millionaires trying to reinvent money. HarperCollins Publishers.
- Pu, S. and Lam, J. S. L. (2020). Blockchain adoptions in the maritime industry: a conceptual framework. Maritime Policy Management, 48(6):777–794.
- Pu, S. and Lam, J. S. L. (2021). Blockchain adoptions in the maritime industry: A conceptual framework. Maritime Policy & Management, 48(6):777–794.
- Radl, A. and Lin, J. (2019). How to make trade single windows more efficient with blockchain.
- Rauchs, M. and Hileman, G. (2017). Global Cryptocurrency Benchmarking Study. Cambridge Centre for Alternative Finance Reports, Cambridge Centre for Alternative Finance, Cambridge Judge Business School, University of Cambridge.
- Ravitch, S. M. and Riggan, M. (2016). Reason & rigor: How conceptual frameworks guide research. Sage Publications.
- Reddick, C. G., Cid, G. P., and Ganapati, S. (2019). Determinants of blockchain adoption in the public sector: An empirical examination. Information Polity, 24(4):379–396.
- Rempel, G. (2015). Defining standards for web page performance in business applications. In Proceedings of the 6th ACM/SPEC International Conference on Performance Engineering, pages 245–252.
- Reuters (2019). Explainer: U.n. body agrees to tougher shipping emission rules, what’s next?
- Reuters (2019). Factbox: Imo 2020 - a major shake-up for oil and shipping. <https://www.reuters.com/article/us-shipping-imo-enforcement-rules-factbo-idCAKBN1YN1UZ>.

BIBLIOGRAPHY

- Reyna, A., Martín, C., Chen, J., Soler, E., and Díaz, M. (2018). On blockchain and its integration with iot. challenges and opportunities. Future generation computer systems, 88:173–190.
- Reynolds, G. S. (2000). The regulation of international shipping: systematic issues facing states in the administration of maritime affairs and the eradication of substandard shipping. WORLD MARITIME UNIVERSITY DISSERTATIONS.
- Rieger, A., Lockl, J., Urbach, N., Guggenmos, F., and Fridgen, G. (2019). Building a blockchain application that complies with the eu general data protection regulation. MIS Quarterly Executive, 18(4).
- Rodrigue, J.-P. (2010). Maritime transportation: drivers for the shipping and port industries. In International Transport Forum, pages 1–21.
- Rodriguez, J. (2016). Beyond bitcoin: Can the blockchain power industrial iot’.
- Rogers, E. M., Singhal, A., and Quinlan, M. M. (2014). Diffusion of innovations. In An integrated approach to communication theory and research, pages 432–448. Routledge.
- Rosa, R. V. and Rothenberg, C. E. (2018). Blockchain-based decentralized applications for multiple administrative domain networking. IEEE Communications Standards Magazine, 2(3):29–37.
- Sahin, I. (2006). Detailed review of rogers’ diffusion of innovations theory and educational technology-related studies based on rogers’ theory. Turkish Online Journal of Educational Technology-TOJET, 5(2):14–23.
- Sanchez-Gonzalez, P.-L., Díaz-Gutiérrez, D., Leo, T. J., and Núñez-Rivas, L. R. (2019). Toward digitalization of maritime transport? Sensors, 19(4):926.
- Santiso, C. (2018). Will blockchain disrupt government corruption? Stanford Social Innovation Review.
- Sarda, P., Chowdhury, M. J. M., Colman, A., Kabir, M. A., and Han, J. (2018). Blockchain for fraud prevention: a work-history fraud prevention system. In 2018 17th IEEE international conference on trust, security and privacy in computing and communications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE), pages 1858–1863. IEEE.
- Schapranow, M.-P. and Plattner, H. (2013). In-memory technology enables history-based access control for rfid-aided supply chains. The secure information society: Ethical, legal and political challenges, pages 187–213.
- Schiffing, S. and Valantis Kanellos, N. (2021). Ship happens: Ever given and forgotten. World Infrastructure Journal.

- Selectra (2016). What is an Average Energy Bill in France?
- Serry, A. (2022). Les données géographiques pour étudier la desserte maritime de l'axe seine : une concurrence sur terre et en mer. ResearchGate. Accessed: 2024-04-04.
- SERVICE, C. P. V. (2022). VGM Information. <https://cmp-vgm.com/faq/vgm-information/>. Accessed: 2022-03-21.
- Shamir, A. (1979). How to share a secret. Communications of the ACM, 22(11):612–613.
- Sharad Mangrulkar, R. and Vijay Chavan, P. (2024). Introduction to Blockchain, pages 1–46. Apress, Berkeley, CA.
- Sharkey, G. (2022). Q&a: Cargox coo sees tradelens' failure as learning opportunity. <https://www.freightwaves.com/news/qa-cargox-coo-sees-tradelens-failure-as-learning-opportunity>. [Online; accessed 15-January-2024].
- Shipping and Freight Resource (2022). Tradelens to be shutdown due to lack of commercial viability. <https://www.shippingandfreightresource.com/tradelens-to-be-shutdown-due-to-lack-of-commercial-viability>. [Online; accessed 15-January-2024].
- Singh, A. (2022). Port development: History, present and future challenges. In Infrastructure Planning and Management in India: Opportunities and Challenges, pages 25–34. Springer.
- Singhal, B., Dhameja, G., and Panda, P. S. (2018). How blockchain works. In Beginning Blockchain, pages 31–148. Apress.
- Sofiev, M., Winebrake, J. J., Johansson, L., Carr, E. W., Prank, M., Soares, J., Vira, J., Kouznetsov, R., Jalkanen, J.-P., and Corbett, J. J. (2018). Cleaner fuels for ships provide public health benefits with climate tradeoffs. Nature communications, 9(1):406.
- Srivastava, S., Teo, T., and Devaraj, S. (2016). You can't bribe a computer: Dealing with the societal challenge of corruption through ict. MIS Quarterly, 40:511–526.
- St Denis, T. and Johnson, S. (2007). Chapter 5 - hash functions. In St Denis, T. and Johnson, S., editors, Cryptography for Developers, pages 203–250. Syngress, Burlington.
- Statista (2022). A.p. møller – mærsk a/s - statistics & facts. [Online; accessed 15-January-2024].
- Stergiopoulos, G., Valvis, E., Mitrodimas, D., Lekkas, D., and Gritzalis, D. (2018). Analyzing congestion interdependencies of ports and container ship routes in the maritime network infrastructure. IEEE Access, 6:63823–63832.

BIBLIOGRAPHY

- Stockburger, L., Kokosioulis, G., Mukkamala, A., Mukkamala, R. R., and Avital, M. (2021). Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation. Blockchain: Research and Applications, 2(2):100014.
- Stonebraker, M., Anton, J., and Hanson, E. (1987). Extending a database system with procedures. ACM Transactions on Database Systems (TODS), 12(3):350–376.
- Stonebraker, M., Çetintemel, U., and Zdonik, S. (2005). The 8 requirements of real-time stream processing. ACM Sigmod Record, 34(4):42–47.
- Stopford, M. (2008). Maritime economics 3e. Routledge.
- Strehle, E. and Ante, L. (2020). Exclusive mining of blockchain transactions. SSRN.
- Sullivan, C. and Burger, E. (2017a). E-residency and blockchain. computer law & security review, 33(4):470–481.
- Sullivan, C. and Burger, E. (2017b). E-residency and blockchain. computer law & security review, 33(4):470–481.
- Sun, Y., Zhang, L., Feng, G., Yang, B., Cao, B., and Imran, M. A. (2019). Blockchain-enabled wireless internet of things: Performance analysis and optimal communication node deployment. IEEE Internet of Things Journal, 6(3):5791–5802.
- Sun Yin, H. H., Langenheldt, K., Harlev, M., Mukkamala, R. R., and Vatrappu, R. (2019a). Regulating cryptocurrencies: a supervised machine learning approach to de-anonymizing the bitcoin blockchain. Journal of Management Information Systems, 36(1):37–73.
- Sun Yin, H. H., Langenheldt, K., Harlev, M., Mukkamala, R. R., and Vatrappu, R. (2019b). Regulating Cryptocurrencies: A Supervised Machine Learning Approach to De-Anonymizing the Bitcoin Blockchain. Journal of Management Information Systems, 36(1):37–73.
- Sunny, J., Undralla, N., and Pillai, V. M. (2020). Supply chain transparency through blockchain-based traceability: An overview with demonstration. Computers & Industrial Engineering, 150:106895.
- Suvannaphakdy, S. (2020). Asean single window: Time to enlarge the aperture.
- Swan, M. (2015). Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc."
- Szabo, N. (1996). Smart contracts: building blocks for digital markets. EXTROPY: The Journal of Transhumanist Thought,(16), 18(2):28.
- Tan, E. (2023). The missing piece: the link between blockchain and public policy design. Policy Design and Practice, 6(4):488–504.

- Tapscott, D. and Tapscott, A. (2016). Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world. Penguin.
- Team, C. N. (2018). Kuehne+Nagel deploys blockchain technology. <https://container-news.com/kuehne-nagel-blockchain-technology/>. Accessed: 2023-03-25.
- Thakkar, P., Nathan, S., and Viswanathan, B. (2018). Performance benchmarking and optimizing hyperledger fabric blockchain platform. In 2018 IEEE 26th international symposium on modeling, analysis, and simulation of computer and telecommunication systems (MASCOTS), pages 264–276. IEEE.
- Thompson, B. (2018). The solas vgm regulations explained. Accessed: 2024-03-21.
- Thurmond, V. A. (2001). The point of triangulation. Journal of nursing scholarship, 33(3):253–258.
- Tian, F. (2016). 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), pages 1–6. IEEE.
- Tijan, E., Agatić, A., and Hlača, B. (2012). The necessity of port community system implementation in the croatian seaports. PROMET-Traffic&Transportation, 24(4):305–315.
- Tijan, E., Jović, M., Panjako, A., and Žgaljić, D. (2021). The role of port authority in port governance and port community system implementation. Sustainability, 13(5).
- Tomescu, A. and Devadas, S. (2017). Catena: Efficient non-equivocation via bitcoin. In 2017 IEEE Symposium on Security and Privacy (SP), pages 393–409. IEEE.
- Triangulation, D. S. (2014). The use of triangulation in qualitative research. In Oncol Nurs Forum, volume 41, pages 545–7.
- Tschorsch, F. and Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 18(3):2084–2123.
- Tsiulin, S., Reinau, K. H., Hilmola, O.-P., Goryaev, N., and Karam, A. (2020). Blockchain-based applications in shipping and port management: a literature review towards defining key conceptual frameworks. Review of International Business and Strategy, 30(2):201–224.
- UNECE (2020). White paper on blockchain in trade facilitation (ece/trade/457).
- unfccc (2015). The paris agreement. <https://unfccc.int/process-and-meetings/the-paris-agreement/the-paris-agreement>. Accessed: 2024-01-17.
- United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) (2012). Buy-ship-pay model, version 1.0. Technical report, UNECE.

BIBLIOGRAPHY

- United Nations Environment Programme (2021). Annual report 2021. <https://www.unep.org/resources/annual-report-2021>.
- United Nations Statistics Division (2023). Overview of ais dataset.
- Valsamos, G., Larcher, M., and Casadei, F. (2021). Beirut explosion 2020: A case study for a large-scale urban blast simulation. Safety science, 137:105190.
- Van Der Lugt, L., Dooms, M., and Parola, F. (2013). Strategy making by hybrid organizations: The case of the port authority. Research in Transportation Business & Management, 8:103–113.
- Verhoeven, P. (2010). A review of port authority functions: towards a renaissance? Maritime Policy & Management, 37(3):247–270.
- Vivaldini, M. and de Sousa, P. R. (2021). Blockchain connectivity inhibitors: weaknesses affecting supply chain interaction and resilience. Benchmarking: An International Journal, 28(10):3102–3136.
- Vorick, D. and Champine, L. (2014). Sia: Simple decentralized storage. Retrieved May, 8:2018.
- Vranken, H. (2017). Sustainability of bitcoin and blockchains. Current opinion in environmental sustainability, 28:1–9.
- Vukolić, M. (2017). Rethinking permissioned blockchains. In Proceedings of the ACM workshop on blockchain, cryptocurrencies and contracts, pages 3–7.
- Wan, C., Yan, X., Zhang, D., Qu, Z., and Yang, Z. (2019a). An advanced fuzzy bayesian-based fmea approach for assessing maritime supply chain risks. Transportation Research Part E: Logistics and Transportation Review, 125:222–240.
- Wan, J., Li, J., Imran, M., Li, D., et al. (2019b). A blockchain-based solution for enhancing security and privacy in smart factory. IEEE Transactions on Industrial Informatics, 15(6):3652–3660.
- Wang, F. (2018). Interagency coordination in the implementation of single window: Lessons and good practice from korea. World Customs Journal, 12(1).
- Wang, G., Shi, Z. J., Nixon, M., and Han, S. (2019a). Sok: Sharding on blockchain. In Proceedings of the 1st ACM Conference on Advances in Financial Technologies, pages 41–61.
- Wang, S. and Qu, X. (2019). Blockchain applications in shipping, transportation, logistics, and supply chain. In Smart transportation systems 2019, pages 225–231. Springer.

- Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., Wen, Y., and Kim, D. I. (2019b). A survey on consensus mechanisms and mining strategy management in blockchain networks. *Ieee Access*, 7:22328–22370.
- WatchGuard Technologies (2023). Power of multiple security layers. *WatchGuard Blog*.
- Weernink, M. O., van den Engh, W., and Thorborg, M. F. F. (2017). The blockchain potential for port logistics. whitepaper, Smart Port, the Port of Rotterdam Authority, TU Delft.
- weforum (2022). Enabling Trade: Valuing Growth Opportunities — reports.weforum.org. <https://www.weforum.org/reports/enabling-trade-valuing-growth-opportunities/>. [Accessed 16-Nov-2022].
- Wilkinson, S., Lowry, J., and Boshevski, T. (2014). Metadisk a blockchain-based decentralized file storage application. *Storj Labs Inc., Technical Report*, hal, 1(11).
- World Economic Forum (2016). Global enabling trade report 2016. Technical report, World Economic Forum.
- Yang, C.-S. (2019). Maritime shipping digitalization: Blockchain-based technology applications, future improvements, and intention to use. *Transportation Research Part E: Logistics and Transportation Review*, 131:108–117.
- Yang, R., Wakefield, R., Lyu, S., Jayasuriya, S., Han, F., Yi, X., Yang, X., Amarasinghe, G., and Chen, S. (2020). Public and private blockchain in construction business process and information integration. *Automation in construction*, 118:103276.
- Yeasmin, N., Zaman, R., and Mouri, I. J. (2016). Traffic control management and road safety using vehicle to vehicle data transmission based on li-fi technology. *International Journal of Computer Science, Engineering and Information Technology*, 6(3/4):1–7.
- Zamani, M., Movahedi, M., and Raykova, M. (2018). Rapidchain: Scaling blockchain via full sharding. In *Proceedings of the 2018 ACM SIGSAC conference on computer and communications security*, pages 931–948.
- Zheng, Q., Li, Y., Chen, P., and Dong, X. (2018a). An innovative ipfs-based storage model for blockchain. In *2018 IEEE/WIC/ACM international conference on web intelligence (WI)*, pages 704–708. IEEE.
- Zheng, Q., Li, Y., Chen, P., and Dong, X. (2018b). An innovative ipfs-based storage model for blockchain. In *2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI)*, pages 704–708.

- Zimmermann, M., Winker, M., and Schramm, E. (2018). Vulnerability analysis of critical infrastructures in the case of a semi-centralised water reuse system in qingdao, china. International Journal of Critical Infrastructure Protection, 22:4–15.
- Ziolkowski, R., Miscione, G., and Schwabe, G. (2020). Decision problems in blockchain governance: Old wine in new bottles or walking in someone else’s shoes? Journal of Management Information Systems, 37(2):316–348.
- ZMUDZINSKI, A. (2019). Shipping startup 300cubits suspends its blockchain operations. Cointelegraph. Accessed: 2024-03-21.

Appendix

SMART CONTRACTS ALGORITHM

Algorithm 1 Society SC

- 1: **Initialization**
 - 2: **Init():** Initializes the smart contract.
 - 3: **Invoke():** Entry point for invoking functions. Dispatches to appropriate functions based on function name.
 - 4: **Society Structure**
 - 5: **Society:** Structure representing a society with various fields
 - 6: **CRUD Operations**
 - 7: **querySocietyByKey(key):** Retrieves the society with the given key.
 - 8: **deleteSocietyByKey(key):** Deletes the society with the given key.
 - 9: **createNewSociety(args):** Creates a new society with provided arguments.
 - 10: **modifySociety(key, args):** Updates a society's fields based on provided arguments.
 - 11: **Ledger Management**
 - 12: **initLedger():** Initializes the ledger with system societies.
 - 13: **Data Retrieval**
 - 14: **queryAllSocieties():** Retrieves all societies from the ledger.
 - 15: **getSocietyHistory(key):** Retrieves the history of transactions for a given society key.
 - 16: **Error Handling**
 - 17: **shim.Error(message):** Returns an error message to the caller.
 - 18: **Logging**
 - 19: **logger.Infof(format, args...):** Logs information messages for debugging.
 - 20: **Utility Functions**
 - 21: **strconv.Atoi(string):** Converts a string to an integer.
 - 22: **json.Marshal(object):** Converts an object to JSON bytes.
 - 23: **json.Unmarshal(bytes, object):** Unmarshals JSON bytes into an object.
 - 24: **ChaincodeStubInterface**
 - 25: Provides methods for interacting with the ledger.
-

Algorithm 2 Type Society Smart Contract

Initialization

2: **Init():** Initializes the smart contract, generally with no specific actions.

Invoke(): Dispatches incoming function calls to the appropriate handler.

4: **Data Structures**

Type_Society: Represents a type of society with its fields.

6: **Core Functions**

queryTypeSocietyByKey(key): Retrieves a Type_Society by its ID.

8: **deleteTypeSocietyByKey(key):** Deletes a Type_Society by its ID.

createNewTypeSociety(args): Creates a new Type_Society with provided arguments.

10: **modifyTypeSociety(key, args):** Updates fields of an existing Type_Society.

Ledger Management

12: **initLedger():** Initializes the ledger with system Type_Society data.

Data Retrieval

14: **queryAllTypeSocs():** Retrieves all Type_Societies from the ledger.

getTypeSocietyHistory(key): Retrieves the transaction history for a Type_Society. .

16: **Error Handling**

Uses shim.Error(message) to return error messages to the caller.

18: **Logging**

Uses logger.Infof(format, args...) for debugging.

20: **Utility Functions**

Employs strconv.Atoi(string) to convert strings to integers.

22: Uses json.Marshal(object) to convert objects to JSON bytes.

Uses json.Unmarshal(bytes, object) to unmarshal JSON bytes into objects.

24: **ChaincodeStubInterface**

Interacts with the ledger using methods.

Algorithm 3 User Management Smart Contract

Initialization and Setup

Init(): Initializes the smart contract.

- 3: **Invoke():** Entry point for invoking functions. Redirects to appropriate functions based on function names.

User Structure

User: Structure representing a user with various fields

- 6: **CRUD Operations on Users**

queryUserByKey(key): Retrieves a user by its key.

createNewUser(args): Creates a new user with provided arguments.

- 9: **modifyUser(key, args):** Updates a user's fields based on provided arguments.

deleteUserByKey(key): Deletes a user with the given key.

Data Retrieval

- 12: **queryAllUsers():** Retrieves all users from the ledger.

getUserHistory(key): Retrieves the transaction history for a given user key.

Utility Functions

- 15: **initLedger():** Initializes the ledger with system users.

ChaincodeStubInterface

Interacts with the ledger using methods.

- 18: **Logging:** Uses `logger.Infof()` for logging information messages.

JSON Encoding/Decoding: Uses `json.Marshal()` and `json.Unmarshal()` to convert user structures to/from JSON bytes.

Composite Keys: Use and create composite keys for efficient retrieval.

Algorithm 4 Manifest Management Blockchain Smart Contract

Initialization:

Define the *SmartContract* struct as the main structure for the chaincode.

Define data structures for *Manifest*, ... and several other data structures to represent manifest data and their associated information.

4: Functions:

InitLedger: Initializes mock data for manifests and stores them in the ledger.

Invoke: Entry point for all chaincode invocations. Dispatches calls to appropriate functions based on the requested function name.

CreateNewManifest: Creates a new manifest based on provided arguments. Performs data validation and type conversions. Stores the new manifest in the ledger.

8: QueryManifestByID: Retrieves a manifest from the ledger by its ID.

DeleteManifestByID: Deletes a manifest from the ledger by its ID.

QueryAllManifests: Retrieves all manifests from the ledger.

GetManifestHistory: Retrieves the transaction history for a specific manifest.

12: ModifyManifest: Updates an existing manifest's information based on provided arguments.**Key Functionalities:**

Creating manifests: *CreateNewManifest* function.

Querying manifests: *QueryManifestByID*, *QueryAllManifests* functions.

16: Updating manifests: *ModifyManifest* function.

Deleting manifests: *DeleteManifestByID* function.

Retrieving history: *GetManifestHistory* function.

Data Storage:**20: Manifests are stored in the ledger using their IDs as keys.**

History of transactions for each manifest is also stored in the ledger.

Interaction with Ledger:

The chaincode interacts with the ledger using the *APIStub* interface, which provides functions for reading and writing data to the ledger, querying and iterating over data, and retrieving transaction history.

24: Error Handling:

The code includes error handling for invalid function calls, data validation errors, and errors during ledger interactions.
