Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Review article

A survey on blockchain technology in the maritime industry: Challenges and future perspectives

Mohamed Ben Farah [a,*], Yussuf Ahmed [a], Haithem Mahmoud [a], Syed Attique Shah [a], M. Omar Al-kadri [b], Sandy Taramonli [c], Xavier Bellekens [d,e], Raouf Abozariba [a], Moad Idrissi [a], Adel Aneiba [a]

[a] *School of Computing and Digital Technology, Birmingham City University, Birmingham, B4 7XG, UK*
[b] *University of Doha for Science and Technology, Doha, Qatar*
[c] *University of Warwick, Coventry, CV4 7AL, UK*
[d] *Lupovis Limited, Glasgow, G1 1XW, UK*
[e] *The Scowcroft Center for Strategy and Security at the Atlantic Council, Washington, DC 20005, USA*

ARTICLE INFO

Keywords:
Blockchain technology
Supply chain
Maritime logistics
Smart contracts
Internet of Things
Cybersecurity

ABSTRACT

Blockchain technology has emerged as a potential solution to address the imperative need for enhancing security, transparency, and efficiency in the maritime industry, where increasing reliance on digital systems and data prevails. However, the integration of blockchain in the maritime sector is still an underexplored territory, necessitating a comprehensive investigation into its impact, challenges, and implementation strategies to harness its transformative potential effectively. This survey paper investigates the impact of Maritime Blockchain on Supply Chain Management, shedding light on its ability to enhance transparency, traceability, and overall efficiency in the complex realm of maritime logistics. Furthermore, the paper offers a practical roadmap for the integration of blockchain technology into the Maritime Industry, presenting a comprehensive framework that maritime stakeholders can adopt to unlock the advantages of blockchain in their operations. In addition to these aspects, the study conducts a thorough examination of the current network infrastructure in Ports and Vessels. This assessment provides a holistic view of the technological landscape within the maritime sector, which is crucial for understanding the challenges and opportunities for the successful implementation of blockchain technology. Moreover, the research identifies and analyzes specific Blockchain cybersecurity challenges that are pertinent to the Maritime Industry.

1. Introduction

Blockchain is defined as a distributed ledger, keeping a permanent and tamper-proof record of data transactions. It is a decentralized system based on a peer-to-peer network, where each node keeps a copy of the ledger to avoid a single point of failure. Although the first objective of the blockchain was the resolution of multiple spending in crypto-money [1], the flexibility of the technology made it attractive to various sectors [2]. It is therefore key for a blockchain-based system to be decentralized, trust-less, collectively maintainable, reliable and anonymous or pseudonymous [3].

Since its inception in 2008, blockchain technology captured the imagination and investment of stakeholders. This revolutionary technology, initially conceived as the underlying framework for cryptocurrencies, has transcended its initial purpose and garnered significant attention across a wide spectrum of industries. Notably, blockchain's applications include supply chain management, logistics, smart contracts, cybersecurity, and the Internet of Things (IoT) [4–7]. The advent of blockchain has brought about a transformative wave in these domains, reshaping traditional processes and introducing new paradigms that promise to enhance transparency, security, and efficiency [8].

The maritime transport sector is inherently marked by the intricate processes involved in the *movement of goods*, entailing the handling of associated information and metadata. The shipping of goods and the maintenance of records within the intricate web of the supply chain pose considerable challenges, primarily due to the voluminous exchange of documents among suppliers, clients, intermediaries, ports, and shipping companies, among others [9]. Moreover, it is imperative that documents directly pertaining to cargo operations remain easily traceable [10]. Current practices, however, often fall short of achieving the desired level of traceability for crucial digital documents, primarily

[*] Corresponding author.
E-mail address: mohamed.benfarah@bcu.ac.uk (M.B. Farah).

https://doi.org/10.1016/j.future.2024.03.046
Received 26 October 2023; Received in revised form 20 February 2024; Accepted 30 March 2024
Available online 8 April 2024

due to cost constraints or the inherent complexity of the systems. The integration of blockchain technology within the maritime shipping industry holds the potential to yield a multitude of advantages, particularly in the realms of secure document traceability and the verification of goods' provenance for all stakeholders [11].

In an era where digitalization and secure data management are paramount, this paper presents a comprehensive exploration of blockchain innovation and its fundamental principles, effectively laying the foundation for understanding how this revolutionary technology can be seamlessly integrated into the maritime industry [12]. By delving deep into the nuances of blockchain's incorporation, this research work provides an analysis of its applicability, considering the existing networking infrastructure within ports and vessels. The maritime industry, characterized by its intricate and information-intensive operations, stands to gain immensely from the implementation of blockchain, offering solutions to longstanding challenges such as document traceability, provenance verification, and security concerns [13–15]. In this context, this survey underscores the fundamental importance that blockchain can play in the industry's modernization, offering a forward-looking perspective on the challenges and potential opportunities that lie ahead. This survey paper offers valuable insights into the role of blockchain technology in the maritime domain, encompassing its potential benefits, integration strategies, technological landscape, and cybersecurity considerations. The paper, thus, serves as a beacon for both researchers and practitioners, guiding them towards a deeper comprehension of the synergies between blockchain technology and maritime operations, and the promising horizons that await exploration.

The main contributions of this paper are as follows,

- The research delves into the impact of Maritime Blockchain on Supply Chain Management, shedding light on how this transformative technology can enhance transparency, traceability, and efficiency within the complex web of maritime logistics.
- Provides a roadmap for integrating blockchain technology into the Maritime Industry, offering a detailed framework that maritime stakeholders can follow to harness the potential benefits of blockchain in their operations.
- Presents an extensive examination of the existing network infrastructure in Ports and Vessels, providing a comprehensive view of the technological landscape in the maritime sector.
- Identifies and analyzes Blockchain cybersecurity challenges specific to the Maritime Industry, creating awareness about potential vulnerabilities and highlighting the importance of robust security measures in the era of digital transformation in maritime operations.

These contributions collectively advance our understanding of the role of blockchain technology in the maritime domain, offering insights into its potential benefits and challenges while guiding the industry towards more secure, efficient, and transparent practices.

The remainder of the paper is organized as follows. Section 2 provides an overview of related work. Section 4 depicts the use of blockchain in supply chain management. Section 5 describes integration methods of blockchain in the Maritime sector; furthermore, Section 6 highlights the security risks associated with the blockchain while the paper concludes with Section 8. Fig. 1 describes the structure of the paper and Table 1 lists the acronyms and descriptions.

2. Related work

This section explores various studies and applications related to blockchain technology in supply chain management and maritime logistics. These works provide valuable insights into blockchain technology's benefits, challenges, and potential in these domains.

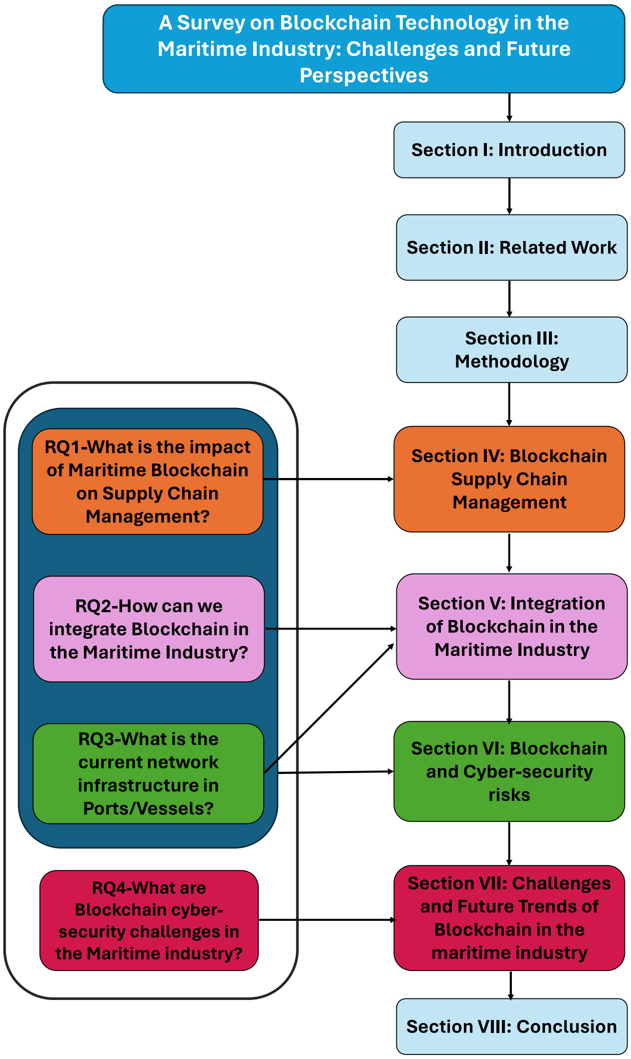

A Survey on Blockchain Technology in the Maritime Industry: Challenges and Future Perspectives
Section I: Introduction
Section II: Related Work
Section III: Methodology
RQ1-What is the impact of Maritime Blockchain on Supply Chain Management?
Section IV: Blockchain Supply Chain Management
RQ2-How can we integrate Blockchain in the Maritime Industry?
Section V: Integration of Blockchain in the Maritime Industry
RQ3-What is the current network infrastructure in Ports/Vessels?
Section VI: Blockchain and Cyber-security risks
RQ4-What are Blockchain cyber-security challenges in the Maritime industry?
Section VII: Challenges and Future Trends of Blockchain in the maritime industry
Section VIII: Conclusion

Fig. 1. Structure of the paper.

Kumar et al. [16] developed a rice supply chain system using blockchain technology to ensure food safety and improve the distribution of rice. Their study demonstrated the effectiveness of blockchain in maintaining the integrity and traceability of food products. An immutable and transparent history of the rice's journey is established by recording and storing transactional data at each stage using the blockchain's decentralized ledger. This includes secure storage of the information about the origin, treated techniques, transportation circumstances, and storage. The outcomes showed the effectiveness of blockchain technology in improving supply chain efficiency towards food safety, as well as maintaining the traceability and transparency of the information. Moreover, the collected data can be accessed in real time, enabling prompt actions to possible safety issues. The blockchain's tamper-proof feature reduced the possibility of fraudulent activity, which enhanced consumer confidence.

The integration of Digital Supply Chain (DSC) operations through blockchain has also garnered attention. Korpela et al. [17] discussed the acceleration of business-to-business (B2B) operations and the integration of DSC using blockchain. Their work highlighted the potential of blockchain to enhance supply chain efficiency through secure and transparent data exchange. This use case highlights the communication and transactions exchanged between businesses within the supply chain, ensuring a responsive and responsible network. Similarly, Gurtu

Table 1
List of acronyms.

Acronyms	Description
IoT	Internet of Things
DSC	Digital Supply Chain
B2B	Business-to-Business
IBM	International Business Machines
SCM	Supply Chain Management
CAP	Climate Action Plan
BD	Big Data
APBA	Algeciras Bay Authority
WLAN	Wireless Local Area Network
HPA	Hamburg Port Authority
AIS	Automatic Radar Identification of Ships
RFID	Radio Frequency Identification
LEO	Low Earth Orbit
LoRaWAN	Long Range Wide Area Networks
WAN	Wide Area Network
DLT	Digital Ledger Technology
DAO	Distributed Autonomous Organization
GDPR	The European Data Protection Regulation
IMO	International Maritime Organization
UNCLOS	United Nations Law of the Sea Convention
EC	European Commission
SMS	Safety Management Systems
NIS	Network and Information Systems
MASS	Maritime Autonomous Ship Systems
GPS	Global Positioning System
Mt Gox	Magic: The Gathering Online eXchange
RQ	Research Question
SC	Smart Contract
5G	5th generation mobile network
SCM	Supply Chain Management
DDoS	Distributed Denial of Service
NoSQL	Not only SQL
HSM	Hardware Security Module
ECDIS	Electronic Chart Display and Information Systems
IMO	International Maritime Organization
ENISA	The European Union Agency for CyberSecurity
MASS	Maritime Autonomous Ship Systems
AML	The Anti-money Laundering
KYC	Know Your Customers
EC	The European Commission
EPIRB	Emergency Position Indicating Radio Beacon
RQ	Research Question

et al. [18] analyzed the trends in blockchain technology within the context of DSC. It analyzed the advantages of utilizing blockchain for DSC, including enhanced data security, reduced financial and banking risks, and its mitigation against fraudulent activities. Tracking ownership and maintaining the integrity of quantity along the supply chain are two areas discussed where blockchain contributed to adaptability and increased operational efficiency. The complex implementation of blockchain and the requirements for further extension technologies are two limitations of blockchain within DSC, and there is a need for further examination to achieve a mature robust system.

In the healthcare sector, Clauson [19] addressed the integration challenges and potential benefits of adopting blockchain technology. The study emphasized the significance of blockchain in enhancing data security, interoperability, and patient privacy in healthcare supply chains. To ensure that patient information is kept confidential but accessible to authorized parties only, it is practical to establish a framework that is both secure and interoperable for managing sensitive healthcare data. Blockchain technology is being used in healthcare supply chains to improve the security and efficiency of healthcare data management while also addressing interoperability issues.

Blockchain technology has also gained prominence in the maritime sector. For example, Maersk, one of the largest shipping companies, collaborated with International Business Machines (IBM) to develop the TradeLens platform. This platform offers real-time access to shipping data and documents, including IoT and sensor data, utilizing blockchain technology [20,21]. This collaborative effort demonstrates the application of blockchain technology to improve transparency and efficiency in maritime logistics. Moreover, it ensures the security and transparency of the data exchanged, maintaining the collaboration among different stakeholders in the shipping ecosystem.

Irannezhad et al. [22] investigated the opportunities and challenges of blockchain technology in logistics and transportation. Their study highlighted how blockchain can enhance process coordination, information sharing, and data security through encryption. The integration of blockchain technology in logistics and transportation processes results in improved efficiency, fewer inconsistencies, and increased security when critical data is transferred along the supply chain.

In [23–25], authors examined the potential adoption of blockchain technology in global sea-borne containerized logistics. The study emphasized the benefits of blockchain for trading partners and shipping companies, highlighting the need for widespread adoption of blockchain technologies in the maritime industry. The application of blockchain technology to improve supply chain efficiency, traceability, transparency, and cost-effectiveness. This is especially by emphasizing digital bills of lading that represent the practical side. The blockchain's tamper-proof nature reduces paperwork fraud, despite drawbacks including high energy consumption and regulatory issues.

Authors in [26–28] conducted a study on blockchain in maritime logistics, focusing on trust issues within Digital Supply Chains (DSC). The study identified four trust issues: lack of communication, opportunistic behavior, distrust in information, and high interdependence between actors. The authors proposed a proof-of-concept blockchain experiment to address these challenges. This means leveraging blockchain technology to improve DSC's trust and transparency while addressing problems that limit effective communication and coordination between supply chain parties.

Loklindt et al. [29] assessed the adoption of blockchain for exchanging shipping information. Their study demonstrated how blockchain can reduce transaction costs and advance global trade by improving the efficiency and security of data exchange.

Tijan et al. [30] proposed a decentralized data storage solution based on blockchain technology in the maritime sector. Their work outlined the advantages and disadvantages of using blockchain technology in this context.

As shown in Table 2, four key maritime blockchain applications have emerged: ship operations, marine insurance, and ship finance. This review examines the platform being used, the type of network, as well as the advantages and disadvantages of the platform. It offers many advantages, including transparency, traceability, security, efficiency, supply chain automation, cost reduction, and paperless systems. The implementation of this technology continues to face several challenges, including high energy consumption, complex cost integration, scalability, interoperability issues, and privacy and data protection issues.

Maritime blockchain use cases identified in the literature include bills of lading, ship operations, marine insurance, and ship finance. Of these, 13 studies emphasize digital bills of lading. As a result, maritime systems can enhance transparency, traceability, efficiency in the supply chain, cost reduction, and environmental friendliness. Despite this, these technologies pose many challenges, such as high energy consumption, complexity, scalability, interoperability, regulatory concerns, and issues related to data security [31–33]. Yet, their tamper-proof nature minimizes documentation fraud. PU and Lam [34] highlight the key use-cases in maritime using blockchain, which are bills of lading, ship operations, marine insurance, ship finance and warehouse management.

Sixteen studies have investigated ship operations as a potential blockchain use case, emphasizing the potential of this technology for improving transparency, real-time traceability, and supply chain automation. Moreover, five studies have explored blockchain's impact on

Table 2
Comparison of Blockchain-based Maritime; C: Corda, E: Ethereum and H: Hyperledger Fabric, R: Ripple.

Ref.	Use-cases						Benefits				Disadvantages			
	Bills of lading	Ship Operations	Marine Insurance	Ship Finance	Platform Used	Network Type	Transparency and Traceability	Security	Efficient and Automation of Supply chain	Cost Reduction and paper-less system	High Energy Consumption and cost Integration	Complexity, Scalability and Interoperability	Regulatory and legal Considerations	Privacy and data protection
[38,39]	√	×	×	×	C	×	√	×	√	√	√	√	√	√
[40–43]	√	×	×	×	×	×	√	×	√	√	√	√	√	√
[44]	√	×	×	×	E	×	√	×	√	√	√	√	×	√
[45]	√	√	×	×	H	×	√	×	√	√	√	√	×	√
[46–49]	×	√	×	×	×	×	√	√	√	√	×	√	√	√
[23,50,51]	×	√	×	×	H	×	√	√	√	√	×	√	√	√
[52,53]	×	√	×	×	E	×	√	×	√	√	√	√	×	√
[54]	×	√	×	×	×	×	√	√	√	√	√	√	×	√
[55–57]	×	×	√	×	C	×	√	√	√	√	×	√	√	√
[58]	×	×	×	√	R	×	√	√	√	√	×	√	√	×
[59]	×	×	×	√	×	×	√	√	√	√	×	√	√	×
[34,60]	√	√	√	√	×	×	√	√	√	√	×	√	√	√
[61–63]	√	√	×	×	×	×	√	√	√	√	×	√	√	√

marine insurance, highlighting its ability to increase transparency, minimize errors and fraud, and streamline the claims process. Furthermore, four studies have examined ship finance, highlighting blockchain's role in ensuring a secure and efficient system that can mitigate fraud risks.

Four platforms dominate the studies: Ethereum, Corda, Hyperledger Fabric, and Ripple [35–37] (Table 2). Decentralized apps (DApps) and self-executing contracts may now be created and executed on Ethereum, a decentralized smart contract platform, revolutionizing the industry. It is frequently used for initiatives addressing non-fungible tokens (NFTs), decentralized finance (DeFi), and other topics. Contrarily, Corda is intended for use by financial organizations. This blockchain platform makes it possible to conduct private and secure transactions, which makes it perfect for the supply chain, insurance, and banking sectors. It is renowned for its emphasis on protecting data privacy and prudent sharing. The Hyperledger project, led by the Linux Foundation and mostly targeted at businesses, includes Hyperledger Fabric. It provides a flexible structure, making it appropriate for companies building blockchain applications. It is frequently used for supply chain management and identity verification.

Despite using blockchain technology, Ripple primarily serves the banking industry. It is a major participant in international remittances since it provides a real-time gross settlement system and currency exchange network, which banks and payment service providers utilize to expedite cross-border transactions. These platforms cover a wide spectrum of blockchain applications, including cross-border financial transactions, private and permissioned corporate solutions, smart contracts, and decentralized apps. Their combined effect demonstrates the adaptability and creativity built into blockchain technology. In terms of practicality, platforms are selected according to their unique advantages and suitability within maritime industry applications.

There are several survey papers [61,63]. Czachorowski et al. [61] reviewed a couple of studies with the aim of addressing maritime applications using blockchain. The review spotted there is a need in the existing maritime systems for better anti-cybercrime measures and privacy. These two are part of a number of compelling factors driving blockchain adoption in the maritime sector. These include efficient supply chain processes, visibility of time-stamped proofed data, the reduction of operational costs and intermediaries, the strengthening of security measures, and the need to meet legal requirements.

Peronja et al. [63] provides container freight and rate prices for the last few years, as well as potential future expenses if blockchain-based technology is applied. The study's findings show that incorporating blockchain technology into the Shanghai-US West Coast route reduces costs by 6%, highlighting blockchain's potential to revolutionize maritime trade. Furthermore, the scope of the analysis went beyond this route, including other important freight markets such as Shanghai-Northern Europe, Shanghai-Mediterranean, and others.

It can be demonstrated that Several of the issues the shipping industry has faced for a long time can be mitigated by blockchain technology. The delays in shipping, which are often the result of slow administrative processes, have caused some logistical and emergency preparedness issues for cargo companies. There is often a high cost associated with these delays. Every day, hundreds of billions of dollars are left unpaid as payments take an average of 42 days to reach the invoicing organization. Since the transportation industry still relies heavily on manual handling of documents, processing and administration costs can account for nearly a fifth of total transportation costs. Companies, especially in the maritime industry, benefit from blockchain technology because it eliminates these burdens and speeds up business processes.

Finally, several pilot projects have been launched since 2016, with fifteen ports or businesses aiming to improve the efficiency of maritime supply chains, as illustrated in Table 3.

These studies contribute to understanding blockchain technology's potential in supply chain management and maritime logistics. They highlight the benefits of blockchain, such as enhanced data security, traceability, transparency, and process efficiency, while acknowledging

Table 3
Blockchain Pilot projects in sea-port.

Port/Business	Year	Description	Benefits
Netherland port [64]	2016	Tracing a container of flowers	Real-time tracing, 90% reduction gas emissions
Cargochain [65]	2016	It aims to track originality	Traceability, and transparency
Rotterdam Port [66]	2018	It aims to propose container tracing system	It provides traceability and visibility
Port of Antwerp [67]	2018	Bill of Lading of Cargo documentation	Reduction of cost and time, Genuine documentation
Southern Transport Corridor port [68]	2018	Enhancing shipping operations	Transparent and Trustworthy logistics process. Real-time track and trace.
Abu Dhabi Port [69]	2018	Silsal intends to leverage shipment operations	Maintain a seamless and secure shipping network
Port of Koper [70]	2018	CargoX aims to provide a smart bill of lading solution	Provide safety and reliability of the document transfer.
Marine Transport International Limited [61]	2018	TrustMeTM Provide Bill of lading	Tracing and visibility of goods
Ernest and Young and Guardtime Ltds [71]	2018	Marine insurance platform	Secure storage.
Port of Singapore [72]	2018	Novazyme aims to establish customs clearance and cargo certificate	Automation of customs procedures
Orient Overseas International Ltd [73]	2018	It aims to digitalis confirmations and fasten communication between different parties	Automation of communication between supply chain.
CargoLedger [74]	2019	It aims to facilitate payment and container tracking	Security, traceability and transparency
Port of Hamburg [75]	2019	ROboB explores enhancing the efficiency of import message platform	Enhance automation, and operation time and cost.
Port of Malmo, Copenhagen [76]	2019	Portchain aims to better coordinate good's arrival.	Reduction of coordination cost and time
Indonesian Port [77]	2019	It aims to automate customs approvals	Automation of customs procedures.
Port of Rotterdam [78]	2020	Automate and maintain safe and efficient maritime operations.	Secure, efficient and smarter Maritime Operations.
CargoSmart [79]	2020	It aims to automate customs approvals.	Automation of customs procedures.

the challenges and trust issues that must be addressed for successful implementation.

2.1. Blockchain applications in real-world maritime operations

This section summarizes and breaks down real-world uses of blockchain in maritime operations based on the literature review. These can bring improvements in transparency, efficiency, security, and automation. These practical applications highlight the revolutionary impact of blockchain technology in addressing real-time challenges and optimizing maritime processes. This includes five real-world use cases which are digital bills of lading, supply chain automation, transparent and secure ship operations, marine insurance and ship finance transactions. First, digital Bills of Lading for Enhanced Transparency: Blockchain ensures a more transparent and effective process by easing the switch from traditional paper-based bills of lading to digital ones [40]. For example, Maersk deployed digital bills of lading in partnership with IBM's TradeLens technology [64]. By enabling real-time tracking and ownership verification of shipments, this greatly lowers the possibility of mistakes, fraud, and delays brought on by the actual paperwork process. This real-world example demonstrates how blockchain technology can protect and expedite important areas of maritime operations. Second, supply Chain Automation through Smart Contracts: The implementation of smart contracts on blockchain platforms such as Ethereum is revolutionizing supply chain automation in the maritime industry [80]. Self-executing smart contracts were used to automate and validate several shipping process steps, from cargo loading to customs clearance, in a case study published by a significant shipping business. Maritime operations are made more economical and efficient by this automation, which also guarantees accuracy and compliance while cutting down on administrative costs.

Third, transparent and secure ship operations: Transparency and security can be established in ship operations through the use of blockchain [81]. The use of blockchain technology to securely store and communicate real-time data on vessel movements, maintenance records, and fuel consumption was illustrated in a case study including the deployment of Hyperledger Fabric in a marine fleet. Transparency offers an immutable and verifiable record of ship activities, which helps fleet managers make better decisions and fosters confidence among stakeholders. Fourth, efficient Claims Processing in Marine Insurance:Blockchain makes maritime insurance easier to navigate by streamlining the claims process [82]. Smart contracts that automate the payment of claims in accordance with predetermined criteria were demonstrated in a case study involving a group of insurers using Corda's blockchain technology. The marine industry's insurers and insured parties eventually gain from this automation since it reduces errors, accelerates the claims procedure, and guarantees transparency. Fifth, securing ship finance transactions: Blockchain technology offers a solution for ship finance transactions, which are frequently vulnerable to fraud threats [83]. Real-time gross settlement methods improve the efficiency and security of financial transactions, as this case study on the application of Ripple's blockchain technology in maritime finance showed. A solid basis for safe ship financing is provided by the tamper-proof nature of blockchain, which also reduces fraud risks and assures the integrity of financial records.

2.2. Limitations of blockchain uses of real-world maritime operations

This section summarizes the limitations of the real-world uses of blockchain in maritime operations based on the literature review.

High Energy Consumption: Blockchain networks are known to use a lot of energy, particularly those that use proof-of-work (PoW) consensus techniques such as Ethereum [84]. There is an environmental risk associated with the processing power needed for transaction validation and mining.

Complex Cost Integration: There are infrastructural, training, and implementation costs associated with integrating blockchain technology into current maritime systems [85]. For systems with fewer resources, the complexity of cost integration may actually be an obstacle to implementation. This makes the adoption of blockchain not feasible for some businesses which can be decided based on a transparent cost–benefit study.

Scalability: As more users and transactions occur on blockchain networks, scalability issues may arise [86,87]. Making sure the blockchain network can scale efficiently without sacrificing efficiency is a practical constraint that needs to be carefully considered in marine operations. Moreover, cross-blockchain is another essential problem where multiple blockchains may need to communicate with each other.

Interoperability: Diverse stakeholders utilizing various platforms and technologies make up the maritime process [88]. It can be difficult to ensure smooth communication between these outdated systems and recently developed blockchain solutions. To be widely adopted and effective, blockchain apps must be able to interact with traditional systems.

Privacy and Data Protection Concerns: Blockchain guarantees data transparency and immutability, however, it presents difficulties for privacy and data protection laws to be enforced [84]. It is essential to maintain a balance between transparency and preserving sensitive information, particularly in the maritime industry where the security and confidentiality of specific data are essential.

Regulatory Compliance: Blockchain regulations as they relate to maritime operations are evolving [89]. It is a realistic difficulty to ensure compliance with both present and future regulations. To make sure that blockchain implementations comply with regulatory standards, navigating legal frameworks, particularly in the context of international marine trade, it requires constant monitoring and adaptation.

2.3. *Environmental impacts of maritime transport and sustainability*

Throughout the past century, maritime transport has stood as the predominant means of facilitating global trade, engaging a multitude of stakeholders [90]. As indicated by [91], the surge in international trade and economic globalization has elevated maritime transportation to a pivotal role as the primary conduit for the movement of goods between nations. Sustainability in maritime transport is characterized by the capability to offer transport infrastructure and services that are accessible, affordable, reliable, socially inclusive, and environmentally friendly [25]. Achieving efficiency and sustainability in shipping is crucial for fostering global economic growth, with a simultaneous emphasis on safeguarding the environment, ensuring cost-effectiveness, and delivering secure and energy-efficient worldwide transportation of goods [92].

While exploring the key pillars of sustainability, the research group in [93] outlined crucial management criteria for sustaining seaport businesses. Within the environmental management criteria, considerations encompass environmental policy, the reduction of environmental risks, and fostering collaboration with stakeholders [93]. Economic management criteria involve adopting cost-saving measures through the utilization of cleaner technologies. Social management criteria include enhancements in welfare and working conditions, educational and training initiatives, and support for economic and social activities [93]. Regarding economic sustainability, key parameters may encompass connectivity, market access, trade competitiveness, infrastructure capacity, and transportation costs, which constitute a significant segment of overall logistics expenses for numerous organizations [94]. Presently, the focus extends beyond economic considerations to ecological aspects of transportation, aiming to mitigate the detrimental impact on the environment [95]. In maritime transport, there is a growing emphasis on the environmental facet of sustainability due to tightening emission regulations and stakeholder expectations. Failure to comply with or address environmental sustainability may result in unforeseen costs for companies [96]. As for the social dimension of sustainability, factors such as safety and security, health, employment, employee engagement, and working conditions should be taken into account [78]. Seaports serve as crucial nodes within the logistics and transportation networks, playing a central role in both national and regional economies [97]. To attain sustainability in seaports, the integration of environmentally friendly approaches into the activities, operations, and management of seaports is essential. The efficiency of seaport activities, particularly loading and unloading, is impeded by unnecessary delays in cargo processing caused by outdated document exchange methods, contributing to increased CO2 emissions [98]. The reliance on paper documents and the need for physical presence during "coordination meetings" result in slower business processes and elevated costs. Additionally, bottlenecks and truck congestion within and outside container terminals can give rise to significant local environmental challenges, including noise pollution and harmful emissions, as well as inefficiencies in various operations [99]. Recognition of the environmental dimension of seaport sustainability is growing among port authorities, users, policymakers, and local communities. Despite the potential environmental advantages offered by innovations, resistance to change is a common occurrence [100].

3. Methodology

This section discusses the scope and survey method used in this paper. Only blockchain and the maritime industry challenges are considered to ensure scope focus.

3.1. *Motivation*

This survey is motivated by the realization that Blockchain technology can be the solution for the next decade in the maritime industry. Blockchain can benefit supply chain management, cargo tracking, trade finance, and payment. It can protect ports and vessels from cyber attacks and accelerate supply chain transactions. The survey is written based on these research questions:

- **RQ1**: What is the impact of Maritime Blockchain on Supply Chain Management?
- **RQ2**: How can we integrate Blockchain in the Maritime Industry?
- **RQ3**: What is the current network infrastructure in Ports/Vessels?
- **RQ4**: What are Blockchain cyber-security challenges in the Maritime industry?

3.2. *Literature review protocol*

The PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-analyses) [101] protocol was used to choose the papers reviewed for this investigation. The PRISMA selection procedure is depicted in Figure 2.

3.3. *Eligibility criteria*

- Based on the scope of the survey, papers published between January 2016 and December 2023 were chosen.
- Thirty-seven websites are used in this survey.
- The keyword search was conducted using Google Scholar. The keywords used were:
  - Cyber attacks in the maritime industry
  - Blockchain and maritime industry

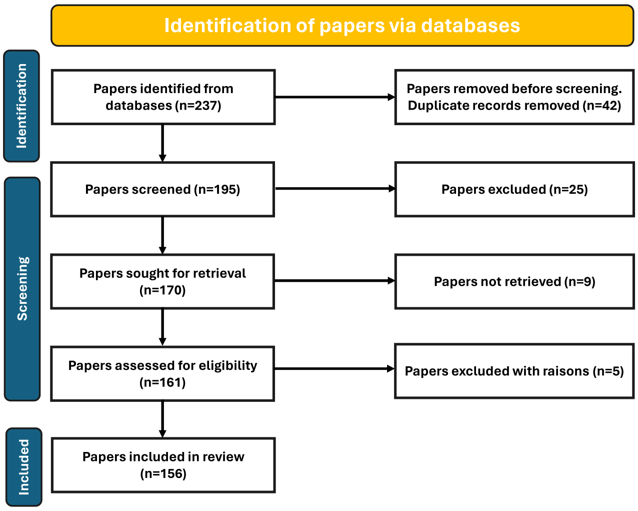

Identification of papers via databases
Identification
Screening
Included
Papers identified from databases (n=237)
Papers removed before screening. Duplicate records removed (n=42)
Papers screened (n=195)
Papers excluded (n=25)
Papers sought for retrieval (n=170)
Papers not retrieved (n=9)
Papers assessed for eligibility (n=161)
Papers excluded with raisons (n=5)
Papers included in review (n=156)

Fig. 2. Survey snapshot: Unveiling the paper filtration dynamics.

- Blockchain in Supply Chain Management
- Connectivity in the maritime industry
- Maritime international law
- GDPR and Blockchain

- We also used Mendeley Reference Manager's suggestions with backward and forward snowballing [102] to collect all pertinent references.
- Considering the topics addressed in this review, papers were included or excluded by reading the abstract, introduction and conclusion. The final collection of papers was chosen so that each taxonomy category contained at least one, and ideally several, representative papers.

3.4. Risk of bias

In this paper, Google Scholar was chosen as the web search tool. It helps avoid bias towards any particular publisher [102]. The only papers that were considered were those that were written in English. Thus, this work may have missed out on some significant work due to these limitations.

4. Blockchain in supply chain management

Supply Chain Management (SCM) is a set of approaches to sharing data across suppliers, manufacturers, and warehouses in order to produce goods or provide a service. The main aim of SCM is to minimize the overall costs of production while maximizing customer satisfaction. SCM represents a complex and large network of stakeholders, which includes many intermediaries from the production process to the distribution process [103]. Hence, communication between different parties is difficult and may lead to several problems such as:

- Inefficiency
- Uncontrolled costs
- Limited visibility of the product or items
- Traceability
- Access to information
- Provenance

Based on the aforementioned problems, SCM should explore new technologies to overcome current challenges. Fig. 3 shows the shift from a traditional supply chain to a digital supply chain and how technology can connect the supply chain more effectively, tackling the problems listed above [61].

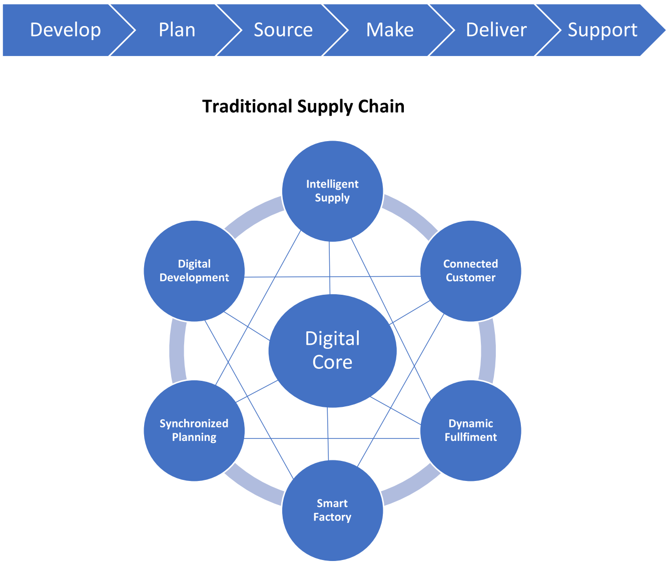


Fig. 3. Traditional and digital supply chain.

With the use of blockchain technology in SCM, processes have improved to ensure competitiveness, optimization of productivity and increased control. Blockchain also, facilitates the different operations and transactions of SCM, allowing companies to have a digital database to store all transactions and movement of goods, facilitating the tracking. The data recorded inside the blockchain is achieved in near real-time and shared and owned by everyone who is a part of the network. Due to the immutability, the data is unchangeable, hence, it is impossible for a user to modify it [30]. In this way, the probability of counterfeiting is minimized. The transactions or operations of SCM will be recorded in the blockchain and tracked continuously [104]. Therefore, transparency is ensured and the records are published and read by every party in the SCM. Fig. 5 demonstrates how data are collected, against the financial and material flow (see Figs. 4 and 6).

Several industries have used blockchain technology to reinforce the visibility of their transactions and to reduce costs [61]. In the following subsections, the importance of blockchain in the Maritime industry is highlighted.

4.1. Blockchain in maritime logistics

The maritime industry is one of the oldest means of transporting goods and is considered a crucial connection between sea and land based on the traditional way of doing business. The objectives of this industry are based on efficiency, effectiveness and cost reduction.

For international shipment, the process requires the involvement of several parts such as customs agents, providers of land transport services, freight forwarders and port management [22,105–107]. All these parts need timely logistic information (like transit, departure and arrival times, the weight of cargo, type of goods, etc.) and appropriate contractual information related to the shipment. The information required at every stage is substantial and requires numerous paper documents (commercial invoices, delivery notes, bills of lading, letters of credit, transport documents, payment notices, etc.) to be generated. Given many documents are paper-based, it is difficult to trace the shipments or components parts of the shipment after it has been delivered to the end customer. Furthermore, paper-based documents increase costs and reduce traceability.

Generally, the Maritime industry transactions are time-consuming, slow and relatively expensive.

To alleviate these limitations, an innovative blockchain solution can be integrated at the core of the maritime industry as proposed in

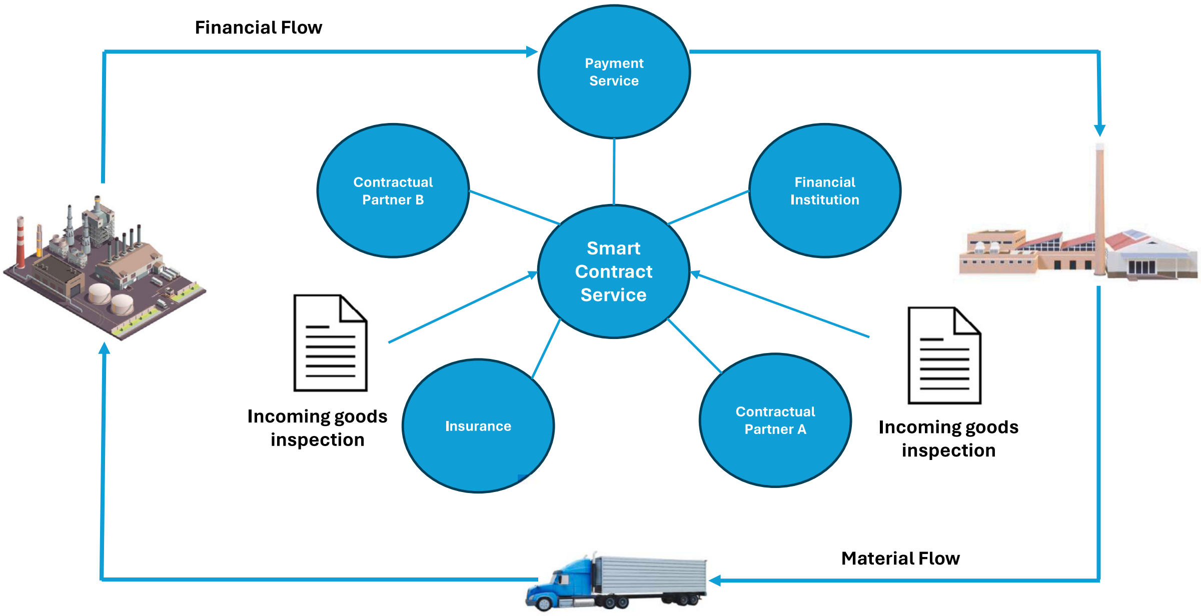


Fig. 4. Blockchain in supply chain management.

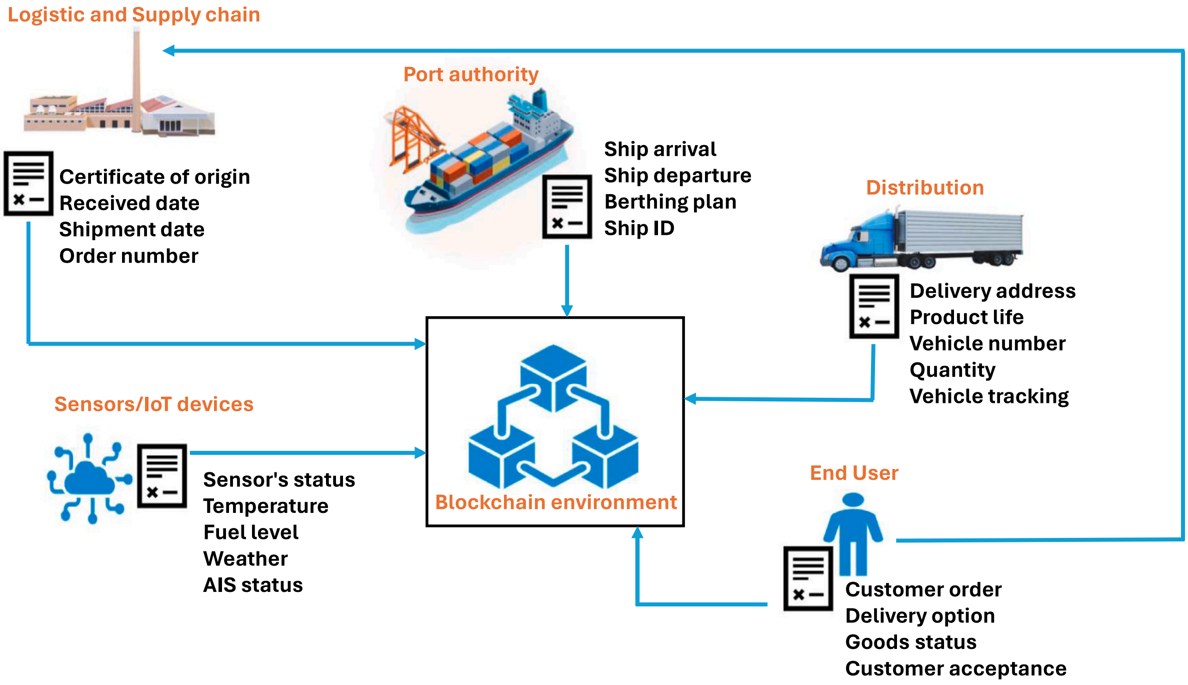


Fig. 5. Maritime blockchain.

the literature. Blockchain can minimize the complexity and volume of point-to-point communications between different parties [108]. Added to this, blockchain can help to reduce the costs and time related to the documentation and administrative processing of the shipments by automating the different transactions. Blockchain can also ensure traceability and, thus, increase visibility and situational awareness along maritime logistics.

Based on the key features of blockchain, a comparison between the current maritime industry shipping management and the benefits of adopting a blockchain-based approach is reported in Table 4.

Blockchain has shown effectiveness in solving shipping problems and is especially used for faster and leaner logistics in global trade, improved transparency and traceability in supply chains, and automation of commercial processes in logistics as demonstrated in Fig. 7.

4.2. Faster and leaner logistics in maritime global trade

It is worth noting that using blockchain in the maritime industry has a clear and reported impact on the global economy and trade [31]. Shipping is considered a key engine of the global economy, as it makes up approximately 90% of world trade. The benefits of these digital

Table 4
Before and after blockchain in Maritime industry.

Key features	Before Blockchain	After Blockchain	Ref
Visibility	• Transactions are time-consuming and slow. • Documents are paper-based, fail to provide real-time visibility.	• Automating all transactions. • Providing a digital platform for information sharing.	[31]
Traceability	• Documents fail to ensure real-time traceability.	• Tracking and tracing information. • Providing real-time shipping information. • Ensuring information sharing among different parties.	[109]
Immutability	• Any part of the maritime network can modify transaction information. • With a centralized database, high risk of fraud.	• Transactions are timestamped. • Providing a single source of data, an immutable database.	[30]
Smart contracts	• Postponement between delivery times and payment terms when dealing with multiple parties.	• Automatically adjusting marine insurance.	[110]

Table 5
IoT at Seaports.

Port's name	Technology	Year	Ref
Port of San Diego	Adopt climate action plan (CAP): The CAP provides a long-term strategic vision for the Green Port program. IoT and smart sensors: to detect and stop wasted energy (energy efficiency digitization program).	2013–2014	[111], [112]
Port of Rotterdam	• 3D Printing: use 3D printing to repair damaged ship parts. • Managing Big Data (BD) to share information. • Portbase: created by a merger between Rotterdam's Port Infolink and Amsterdam's Port Net: Portbase facilitates the exchange of data between companies and the exchange of information with government authorities. • Sensors, machine learning, simulation and modeling, predictive analytics: these technologies are used for maintenance planning, cargo flow analysis, and port planning. • Port of Rotterdam implemented the 'Digital Dolphins' smart quay and sensor technology-equipped buoys that support ship-to-ship cargo transfer and generate timely data about cargo status based on IoT technology.	2009–2017	[113], [114]
Port of Amsterdam	• App Iamport: provides the ability to follow ship movements in real-time. • Application Port Data: shows the historical market shares of the throughput of cargo to promote the idea of data sharing. • Managing Big Data: to share information.	2016–2020	[114], [115]
Port of Antwerp	• Drone–boat: to guarantee the safe passage of container ships on arrival and departure. • Collecting and translating data using Cloud connectivity (New cloud-based IoT) provides a platform for IoT operating systems, allowing for communication within and between ports. • The port is exploring the use of blockchain for container collection.	2017–2018	[116], [117]
Port of Algeciras	• The Port of Algeciras Bay Authority (APBA) is driving an innovation program called Algeciras Brain Port 2020 (ABP 2020). Phase 1 Algeciras Brain port [2014–2015], focused on infrastructure and innovation frameworks, has been created as the core for the digital transformation journey. Phase 2 Algeciras Brain Port [2020] improves collaboration and synergies among the whole port and logistics community. • Digital platform: using IoT and sensors to collect data from the operational situation of the port.	2014–2020	[118]
Port of Hamburg	• HPA (Hamburg Port Authority) aims to transform this seaport into an intelligent port based on three key areas: infrastructure, traffic flows, and trade flow. • Using Bluetooth, hotspots or Wireless Local Area Network (WLAN) cloud, mobile devices, IoT, and Big Data. • HPA embedding sensors and communicative capacities in the port's main tangible assets. Smart meters can monitor and control energy. • Automatic radar identification of ships (AIS Technology) and RFID (Radio-Frequency identification): port authorities know at all times what is moving around in the port. • GPS (Global Positioning System) and geo-referencing: monitoring the movements of trucks. • HPA launched an IoT pilot project to record the emissions of sulfur dioxide, nitrogen dioxide, and fine dust at various locations in the port of Hamburg using sensors. • HPA, Deutsche Telekom, and Nokia completed a 5G field trial at the port of Hamburg, which can be used to support use cases for traffic light control and IoT sensors mounted on mobile barges.	2014–2019	[119], [120]

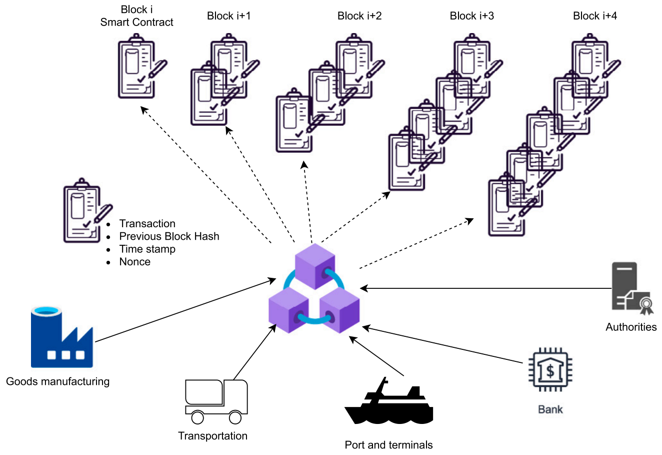


Fig. 6. Smart contract in maritime supply chain.

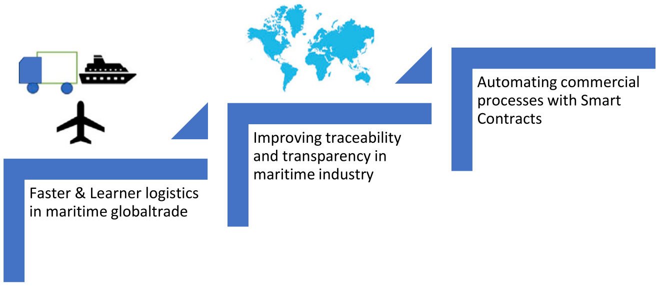

Faster & Learner logistics in maritime globaltrade
Improving traceability and transparency in maritime industry
Automating commercial processes with Smart Contracts

Fig. 7. Blockchain in maritime logistics.

platforms create novel opportunities for ports to have added value for the economy. blockchain integrated into the maritime industry creates a communication channel between the different parties by pooling and sharing resources. This may lead to maximizing gain and efficiency [121].

4.3. Improving traceability and transparency in maritime

Blockchain improves tracking and traceability of cargo and the different shipping transactions [81,122,123]. This way, the shipping conditions are respected and assure customer satisfaction in long and complex supply chains. This is because, for each transaction, the related information is recorded on a distributed ledger. Thus, the data is collected throughout the supply chain [109]. Moreover, if a problem occurs, the blockchain-based system can send a warning automatically to the different parties. The maritime industry's transport environment could also be monitored by combining blockchain and the Internet of Things by integrating a sensor device within products.

4.4. Smart contracts in blockchain logistics

In the maritime industry, digitized blockchain contracts, known as Smart Contracts, are revolutionizing logistics operations. These sets of code automate and regulate transactions digitally between parties, significantly enhancing efficiency in maritime logistics [124]. By ensuring timely delivery and adherence to payment terms once a contract is signed, smart contracts help avoid delays and discrepancies that are common in traditional maritime operations [52,110].

The implementation of smart contracts on platforms like Ethereum, Hyperledger Fabric, or Ripple's Codius is particularly beneficial for the maritime industry. For example, Ethereum's smart contracts can be used to automate the verification of cargo receipt at ports, triggering actions such as sending delivery confirmations and generating invoices [125]. This not only streamlines financial transactions but also ensures continuous tracking of cargo in real-time, a critical requirement in maritime logistics.

Hyperledger Fabric offers a modular and flexible approach, suitable for creating permissioned blockchain networks in the maritime sector [126]. Its chaincode (smart contracts) can be customized to meet the specific needs of maritime logistics, offering enhanced privacy and scalability. This is particularly useful for enterprises in the maritime industry that require a controlled and customizable blockchain environment.

Ripple's Codius platform, though primarily known for payment solutions, provides smart contract capabilities that enable interoperability between different blockchain networks. This feature is invaluable in the maritime industry, where logistics operations often involve multiple stakeholders and systems.

Incorporating smart contracts in maritime logistics leads to more efficient, transparent, and secure operations. The contracts are auto-executed based on predefined algorithms and protocols, allowing involved parties to approve outcomes instantaneously. This is especially crucial in the maritime industry, where complex supply chains and international regulations necessitate a high degree of accuracy and reliability.

5. Integration of blockchain in the maritime industry

This section discusses the possibilities of integrating Blockchain into IoT maritime networks. Several approaches and algorithms were discussed in the literature proposing blockchain network models by combining the registration algorithm proposed in [127] and the proof-of-authentication proposed in [128].

5.1. Iot at seaports

IoT technology has been used in several ports to enhance the quality of service. Table 5 highlights some seaports and their technology.

There is no doubt that several ports have used a combination of technologies to reduce energy consumption, combat pollution, share information, follow ship's movement in real and near real-time, and several other goals. The Port of San Diego, for example, used IoT technology and sensors to detect and stop wasted energy and, as a result, reduce fuel consumption. To share information such as shipping movements or arrivals and departures of a ship, Amsterdam's port created a free application named "Iamport". This application can be installed on a computer or smartphone. Additionally, Amsterdam's port used a second application named "Port Data" to show the throughput of cargo's market shares. Antwerp's port created an IoT platform, allowing communication within and between ports. Furthermore, the port of Antwerpen uses blockchain for container collection. While IoT technology integration is essential to modernize services and prepare for the next generation of the maritime industry, most lack traceability information. Hence seaports are moving towards blockchain technology [61,62,129,130].

5.2. Connectivity in maritime ecosystem

The success of Blockchain technology in the maritime industry hinges on the availability of wireless broadband access throughout the various points of operations, at sea and onshore. However, land-based wireless networking solutions such as 4G/5G, LoRaWAN, LoRa, Zigbee, BLE and WiFi rely on fast copper cables, light-speed fiber optic technology and high bandwidth wireless broadband backhaul connectivity to reach the internet [131]. The wired infrastructure is a combination of fixed physical underground and overhead cabling networks, which are unavailable for water-isolated mobile objects such as ships and ocean liners. Efforts were made to add base stations in strategic islands along popular sea routes, supplied by broadband undersea cables from nearby sources [132], but these remain limited studies pointing to potential obstacles such as extreme climatic conditions and orientation factors [133,134].

On the other hand, seafloor cabled networks connecting continents and countries are often a single line laid down to form the shortest path between two gateways, not developed for distributed systems and do not necessarily follow the path of popular ships lines [135]. Furthermore, the human population on ships and vessels is not expected to offer opportunities or profitability for innovative solutions or tempt network operators to straddle optical transit lines, which means the maritime industry, at least for the foreseeable future, will rest on sub-optimal, backhaul satellite links that up to now are relatively slow and lack reliability [136]. One might assume that as we are witnessing a renewed space race in the earth's lower orbit, with projects such as those funded by SpaceX and Blue Origin [137], building internet satellite constellations will lead to a transformation in connectivity everywhere, including oceans. However, these solutions are not tailored specifically to provide backhaul access links. Rather they are built to offer an interface to domestic consumers such as homes and small businesses, limiting the potential to transcend into industrial-scale applications [136]. Casting further doubts on the success of Low Earth Orbit (LEO), these systems are optimized for fixed antennas on rooftops with a clear line of sight to orbiting satellites. They are also limited to bandwidth and number of available channels, utilizing a combination of Ku-band and Ka-band frequencies, operating on a non-interference basis [138].

What might provide stable backhaul links to vessels and ships is mesh networks, connecting ships near the shores to those in the deep ocean regions through ship-to-ship connectivity as proposed in [139,140]. Mesh topology has its own challenges. For example, high bandwidth point-to-point communications are typically built on mmWave spectrum technology using multi-input-multi-output (MIMO) directional antennas. Slight misalignment between transceivers utilizing mmWave and MIMO technologies can cause severe outages. Keeping such directional links stable is challenging if deployed on moving vessels, even if dynamic beamforming techniques are employed. There are other challenges related to channel behavior in maritime communications as detailed in [141].

Combining the above solutions might offer better prospects and higher reliability of improved backhaul connectivity [142]. However, this will increase the complexity, cost and of network maintenance activities, which are difficult to provide given that ships spend most of their life cycles offshore, leading to substantial delays in services.

In addition to backhaul issues, there is another holding back factor, which is inherent in heavily steel environments, adding another challenge for network distributions onboard ships [143]. Radio waves suffer the most when faced with steel and metal-reinforced concrete, causing traditional local networking solutions to fail, particularly under higher modulation schemes [144,145]. Multi-hop communications utilizing mesh and tree topologies are proposed to tackle the propagation issues locally. However, due to the shared bandwidth nature of local wireless technologies, interference can in some scenarios present further delay, impeding real-time performance [144]. While real-time communications are not a functional requirement for all Blockchain communications, enabling low latency communications helps in propagating transactions quickly and efficiently throughout the network [146].

In summary, connectivity shortcomings offshore and onboard ships increase outages and latency, adding challenges to Blockchain adoption in the maritime industry. Blockchain is a peer-to-peer network topology protocol, but the networking stack elements equate to infrastructure-based systems. While central servers and central authority are bypassed, access to the public internet through gateways is essential for the Digital Ledger Technology (DLT) operation to connect to respective nodes in different networks [147]. In addition, search protocols which underpin Blockchain technologies generate high traffic. For example, Futurepia, a blockchain application developed to help businesses, enterprises, and startups move to the blockchain, performs 300,000 transactions per second [148]. High traffic demand can put a strain on other essential communication within ships and ocean liners across the world's waters, adding latency and variability to network performance.

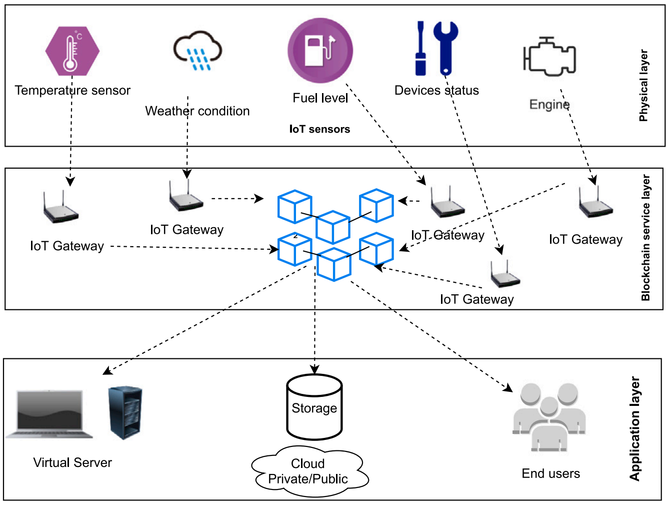


Fig. 8. Innovating seaports — IoT layers explored.

Regional diversity in terms of technology availability as well as spectrum regulation adds another layer, which limits hybrid and fallback approaches designed to support shore-to-ship connectivity, particularly at seaports and around coastlines. For example, it is widely recognized that different sea ports offer varying networking technology capabilities depending on location, investment and strategic priorities. While ports within the developed countries offer advanced network infrastructure such as 5G and fiber, many economically disadvantaged regions lack the high-speed capability, supporting only legacy networking technologies such as 3G and WiMAX [149,150]. There are also constraints associated with proprietary systems and a lack of interface standards across connected ports, limiting interoperability and creating a lock-in effect [151]. In addition, establishing a secure and successful network incorporating heterogeneous technologies is significantly challenging as discussed in [152].

5.3. Blockchain implementation in the maritime domain

Blockchain offers a partial solution enabling security and traceability issues of IoT and IoS networks in the maritime industry. The integration of IoT and IoS in digital ships and smart ports is becoming essential for the integration of the next generation to the maritime industry. Most IoT and IoS architectures are infrastructure-based systems, making them prone to existing cyber-attacks. This section presents the implementation of blockchain for IoT and IoS networks in the maritime industry.

The architecture is based on three layers (Fig. 8):

(1) Physical layer: containing the IoT sensors, such as for temperature, pressure, weather conditions and fuel level.
(2) Blockchain service layer: the data is received by IoT Gateways and sent to the blockchain network.
(3) Application layer: consists of using the virtualisation technique and cloud storage.

A layered approach has been proposed for the blockchain-based IoT network's cost-effective deployment to simplify the hardware and software implementation. With the progress in hardware technologies, low-cost implementation can be considered. The layered architecture,

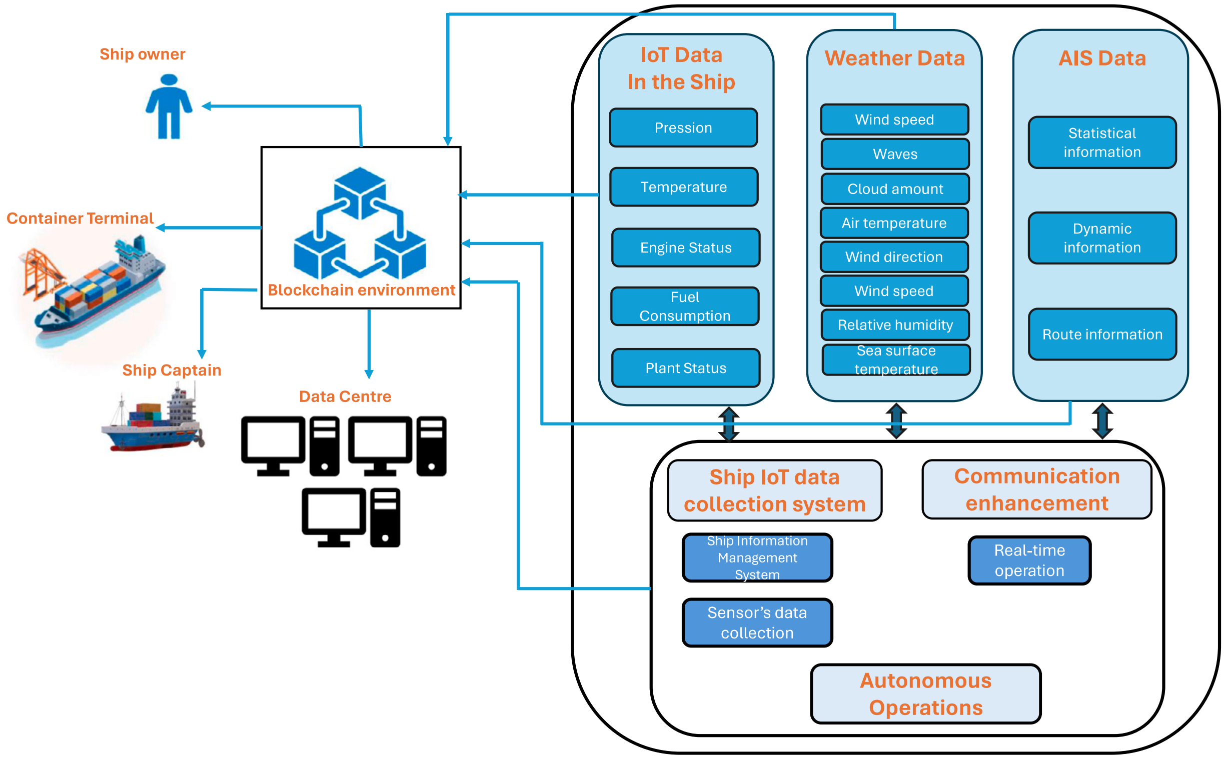


Fig. 9. Data flow in maritime environments.

as presented in Fig. 8, allows extension flexibility. Besides, developers can replace or create any new component without interrupting modules of the infrastructure. Fig. 9 provides an overview of the type of data shared by ships and ports.

The implementation of blockchain in maritime supply chain operations entails various cost considerations. Notably, recent advancements in hardware technologies contribute to the potential for cost-effective deployment. Figs. 8 and 9 suggest progress in hardware technologies, allowing for low-cost implementation, and highlight the layered architecture of blockchain, providing extension flexibility. However, implementing smart contracts for all the data mentioned in the statements involves costs related to the development of smart contracts, Blockchain transaction fees, IoT and IoS infrastructure costs, security measures and ongoing maintenance [153].

The blockchain's layered architecture enhances its adaptability, allowing for flexible extensions without disrupting the underlying modules. Developers can seamlessly replace or introduce new components within the infrastructure. When considering the execution of smart contracts for the specified data, costs are incurred in development, transaction fees, hardware and infrastructure, security measures, and ongoing maintenance. Additionally, the ability to replace or create components without interrupting modules enhances the overall adaptability of the system.

NoSQL databases, including MongoDB, offer cost-effective solutions for data storage and retrieval and are straightforward to implement compared to blockchain [154]. The decision between using blockchain or a NoSQL database should be based on the specific needs of the supply chain in the maritime. If the primary goal is to secure and transparently record transactions, and if there is a need for decentralized trust, then blockchain could be a suitable choice. However, if the emphasis is on efficient data storage, retrieval, and simplicity, a NoSQL database may offer a cost-effective alternative. A comparative cost analysis with NoSQL databases, such as MongoDB, reveals that the choice between blockchain and a NoSQL solution relies on specific use case requirements and the required balance between security, transparency, and operational simplicity.

5.4. Blockchain in maritime payment management

In maritime supply chain operations, payment management plays a pivotal role in ensuring seamless and transparent transactions. The integration of blockchain technology in this domain offers transformative solutions for enhancing payment processes. This includes the automated execution of payments through smart contracts, and borderless transactions, facilitated by crypto wallets [155]. These advancements collectively contribute to the evolution of payment systems, fostering transparency, security, and efficiency throughout the maritime supply chain.

The adoption of cryptocurrency wallets, commonly referred to as crypto wallets, further contributes to the evolution of payment systems in maritime logistics [156]. These digital wallets, built on blockchain technology, provide a secure and decentralized means of managing financial transactions [157]. In scenarios involving international shipments, crypto wallets offer the advantage of borderless payments, eliminating the need for traditional banking intermediaries and associated delays.

In the context of blockchain in maritime logistics, the integration of crypto wallets becomes particularly relevant for scenarios such as cross-border transactions, where conventional payment methods may encounter inefficiencies [158]. Blockchain facilitates real-time tracking of shipments, ensuring that payment milestones are met, and smart contracts automatically trigger payments upon fulfillment of predetermined conditions [159]. This not only accelerates payment cycles but also reduces the administrative burden associated with manual verification processes.

The implementation of blockchain in digital ships amplifies the importance of secure and efficient payment mechanisms [160]. By leveraging the decentralized and tamper-resistant nature of blockchain, payment data in digital ships is safeguarded against unauthorized alterations. Smart contracts, as integral components of this framework, automate the payment processes based on predefined data parameters and delivery milestones. The utilization of smart contracts within the maritime supply chain facilitates the automated and secure execution of

Table 6
Blockchain cybersecurity risks and possible countermeasures.

Risks	Causes	Countermeasures
51% attack or Goldfinger	In a blockchain network, if a single entity or group of entities controls more than 50% of the network's computing power, they can potentially manipulate the blockchain and its transactions.	Proof of Stake (PoS) can reduce the risk. Additionally, diversifying the blockchain network's participants can make it more robust.
Double-spending attack	A malicious actor attempts to spend the same cryptocurrency units (e.g., Bitcoin) more than once, essentially creating counterfeit money.	Employ blockchain analysis tools and services to trace and identify potential double-spending activities and help prevent them.
Vulnerabilities in smart contracts	Smart contracts are self-executing code on the blockchain that can be vulnerable to coding errors or exploits. These vulnerabilities can lead to unauthorized access or manipulation of contract terms.	Use of formal verification method, use of tools to detect bugs: OYENTE, Securify, SmartCheck [163].
Data injection attacks	Malicious actors may attempt to inject false data into the blockchain, leading to erroneous records.	Implement data validation checks and oracles to verify the accuracy and authenticity of data before it is recorded on the blockchain. Employ off-chain sources to cross-verify critical data [164].
Private key security	The security of private keys used to access and sign transactions on the blockchain is crucial. If private keys are compromised, malicious actors can gain unauthorized access.	Hardware security modules (HSMs) and multi-signature wallets. Regularly update and rotate keys and use strong authentication methods [165,166].
Private forks	Private forks and a subgroup of network participants create a new blockchain with different rules (e.g., changes in consensus mechanisms, rules, or protocol) while still using the existing blockchain's transaction history up to a certain point.	Hard Fork Signal: Implement mechanisms requiring a supermajority or broad consensus for significant protocol changes. This can prevent contentious hard forks by ensuring that changes are widely accepted.
Pool attacks	Centralization of Hash Power: When a few mining pools or validators control a significant portion of the network's hash power, they can collude to control the network's consensus rules or execute malicious activities.	Using the trusting pool, multiple confirmations for large transactions, SMARTPOOL. Also, encourage decentralization by using mining algorithms or consensus mechanisms resistant to centralization, such as Proof of Stake (PoS) or other alternatives [167].
Privacy risks	Some blockchain networks, such as public blockchains, may expose transaction data to the public, which can be a privacy concern for sensitive maritime industry data.	Implementing private or consortium blockchains can restrict access to authorized participants, ensuring that sensitive data remains private. Zero-knowledge proofs or other privacy-preserving technologies can also protect data on public blockchains.
Regulatory and compliance risks	Depending on the jurisdiction and the use of blockchain technology in the maritime industry, compliance with legal and regulatory requirements may be challenging.	Work closely with regulatory authorities and legal experts to ensure compliance with applicable laws and regulations. Transparently document blockchain operations to facilitate compliance reporting.
Social engineering attacks	Human elements remain vulnerable to social engineering attacks, such as phishing or insider threats.	Implement employee training and awareness programs to educate staff about social engineering risks. Use multi-factor authentication (MFA) and access controls to restrict unauthorized access.

payment terms based on predefined conditions. This not only mitigates the risk of fraud but also streamlines the financial aspects of shipping operations.

6. Blockchain and cyber-security risks

Recent studies and reports have shown that even blockchain is susceptible to various cybersecurity attacks and suffers several vulnerabilities [161,162]. Table 6 illustrates possible risks, causes and countermeasures that may help protect the network from cyberattacks.

6.1. GDPR and blockchain

The European Data Protection Regulation (GDPR) was created to harmonize the data protection laws within the EU member states. GDPR implementation has matured over the years, but introducing Blockchain technologies has introduced new dynamics to GDPR compliance and requirements. A key consideration will be to understand the security and privacy risks of Blockchain technologies and how data protection requirements can be met.

In GDPR, specific requirements are placed on the data processors and controllers. For example, the data controller is responsible for ensuring mechanisms for the accuracy of personal data. The compliance requirements become more challenging with the implementation of Blockchain. The key challenge in Blockchain is knowing how the data is exchanged between the nodes and who has access to the confidential information that was generated [168]. There should be a granular audit trail that can account for the permission and level of access. Data is replicated across the participating computers in Blockchain based on trust, and no centralized validation exists. This replication could make it difficult to invoke the right to be forgotten, stipulated under Article 17 of the GDPR and Article 16, which provides the right to amend following a submission by the data subject. GDPR requires data collection to be minimized, and only be used for the intended purpose. Still, in Blockchain, the participating nodes keep growing, and the scope increases gradually, making implementing this clause and data retention policies challenging. In the context of the maritime industry, data sources span multiple nodes and the underlying services. Such sources might be from the logistics, supply chain, port authority, and sensor devices. Blockchain can conflict with GDPR in the above-mentioned scenarios relating to clauses 16 and 17. Although some researchers and industry figures have floated ideas such as deleting the encryption key to make data inaccessible, we believe this area needs further research.

6.2. Blockchain technology's impact on maritime industry regulation and compliance

The adaptation of blockchain technologies to the maritime industry offers opportunities for innovations, but it also introduces complex compliance and regulatory issues that need to be considered. Navigating these challenges requires careful consideration of the regulatory impact of these technologies. It is necessary to adhere to security best practices and give serious thought to the ongoing effects of these technologies to navigate these challenges. Establishing a partnership between the regulatory agencies and the maritime sector will create a platform where the opportunities of blockchain can be maximized while maintaining compliance. The maritime industry requires a unified strategy for dealing with compliance and regulatory risks emanating from the implementation of blockchain technologies.

The infrastructure will need to be designed with regulatory and compliance issues in mind. The vessels transverse the vast ocean and often visit several countries which have different regulatory requirements, but the overarching principle is the security and privacy of the data and safety of the vessels and those within it. These different jurisdictions and lack of standardized frameworks pose a challenge to the implementation of a unified strategy for managing the risk and complying with the legal requirements. To overcome these challenges, the companies must be up to date with the laws in the various jurisdictions, apply security best practices and create a compliance culture within the organizations. The maritime industry will need to lead on this front to ensure these changes are addressed to achieve compliance. Next, some areas where regulatory requirements and blockchain technology overlap in the context of the maritime industry.

The General Data Protection Regulation (GDPR) mandates the protection of personal data and therefore the data processed and stored in the blockchain platforms must be protected. The maritime industry collects vast amounts of data which need to be protected. Such data includes confidential information relating to their customers and data relating to business transactions which are susceptible to data breaches should a successful cyber-attack take place. Vessels adhere to regulations imposed by their vessel flag state [169]. GDPR cover anyone who is dealing data from EU subjects regardless of their location [170] which might introduce compliance complications.

GDPR provides provisions to data subjects such as the right to be forgotten [171] but this can pose a compliance challenge due to the decentralized nature of blockchain unless there is a mechanism in place to fulfill the requirement of the provision. One of the main advantages of implementing blockchain technologies is transparency but this conflicts with some of the requirements of GDPR such as limiting the data that is collected and ensuring it is only used for the purpose it was collected for. A cornerstone to complying with GDPR is the implementation of robust risk management strategies, consent mechanisms, security audits and data impact analysis. A data controller has a vital role in data management and the Data Protection Officer (DPO) provides oversight and leads the data protection strategy.

Many countries have strengthened their financial regulations to fight money laundering. The Anti-money Laundering (AML) regulations and the requirements to Know Your Customers (KYC) apply to all sectors including the maritime and require them to process and collect information and share the data when dictated by the law [172] . The maritime industry needs to consider the implications before implementing blockchain technologies to ensure it does not impede compliance and regulatory requirements. Other regulations mandate ships to share travel information and comply with the reporting requirements. Blockchain technologies must align with the requirements of the regulatory bodies to avoid potential conflicts.

Smart contracts and their compliance with regulations raise some legal issues. While smart contracts serve to automate and uphold contractual agreements within blockchain systems, ensuring their enforcement across various jurisdictions can be challenging. Therefore, there may be a need for a framework to reconcile the legal requirements established by different jurisdictions to accommodate smart contracts based on blockchain technology.

Navigating the intricate legal and regulatory landscape in the maritime industry requires close collaboration among various stakeholders, including vessel owners, regulatory bodies, policymakers, and legal experts. It is essential to stay up to date with laws and regulatory requirements to comply with multiple jurisdictions in the maritime industry and implement security best practices. Such efforts contribute to fostering compliance while harnessing the opportunities provided by blockchain technologies.

6.3. *Maritime international law and regulations*

The maritime sector is a lifeline for global trade. According to the International Maritime Organization (IMO), 80% of world trade goes through the sea [173]. The traditional threats to shipping included piracy and smuggling, amongst others. Most of the current maritime laws were designed to counter such threats, but the digitization of the maritime industry has amplified the existing threats and created new ones. The digitization and spread of IoT devices have improved the communication and efficiency of maritime services. However, the sensors and connected devices also introduce cyber threats that never existed in the pre-digitization era. The existing laws, such as the United Nations Law of the Sea Convention (UNCLOS) [174] established in 1982, defined a legal framework to govern the sea and oceans. However, they were not designed with cybersecurity in mind at the time. The European Commission (EC) introduced regulation No 725/2004 [175] for enhancing ship and port security.

To address these new challenges, international organizations have developed regulations and guidelines to prevent and mitigate risks from these threats. For example, the IMO adopted resolution MSC.428(98) on maritime cyber risk management in Safety Management Systems, which mandated operators to comply with the specified guidelines and requirements [176]. IMO released further guidelines on Resolution MSC.429(98), encouraging countries to address pre-existing requirements and ensure cyber risk issues are adequately addressed [177]. In 2020 the EC adopted the EU Direction on the security of Network and Information Systems (NIS) to modernize existing frameworks by taking into account digitization and new threats emanating from these technologies [178]. The European Union Agency for CyberSecurity (ENISA) released further guidance on cyber risk management for ports, which allowed operators to manage risk from new and emerging technologies [179].

Individual countries have their own guidelines and regulations for dealing with cyber threats. For example, the United Kingdom (UK) recently updated the guidelines for the Maritime Autonomous Ship Systems (MASS) due to the significant pace of change in maritime autonomy [180]. Given the global nature of maritime trade and the continuous adoption of new technologies, global regulations and guidelines must be regularly updated and harmonized to create maritime cyber laws that are fit to address the new challenges and span across countries and jurisdictions. Such challenges will deter potential cybercriminals, while the guidelines will help the maritime sector secure its assets to preempt potential attacks.

6.4. *Security concerns of maritime related payments*

Integrating cryptocurrency wallets for data storage, payments, and shipment-related payments in blockchain-based maritime supply chain scenarios raises significant security concerns. The primary challenge lies in the risk of unauthorized access and hacking attempts, which can lead to the theft or loss of digital assets stored in these wallets. As highlighted in [181], the maritime supply chain involves a complex network of transactions and sensitive data, making the security of cryptocurrency wallets paramount.

The digital nature of these wallets makes them vulnerable to cyberattacks, including phishing, malware, and other forms of digital fraud, as discussed in [182]. Furthermore, the decentralized and often pseudonymous characteristics of blockchain transactions can complicate the tracking and recovery of lost or stolen assets. The immutable

Table 7
Examples of previous cyberattacks in Maritime Industry.

Port/Business	Year	Attack type	Description
Sembcorp Marine [183]	2022	Unauthorized access	An unauthorized user exploited third-party software to access the IT network. Even while the organization said the breach would not have a big financial impact, it nevertheless shows how important the implementation of cybersecurity measures to stop cyberattacks.
Voyager Worldwide [184]	2022	DDoS	Voyager Worldwide is a marine IT solutions provider with activities supporting over 25% of shipping companies globally, located in Singapore. The company's network was victim to a cyberattack that brought all systems down. . DSLAB said that the hacker used the IT service providers to spread the cyberattack to shipping businesses.
Port of Lisbon [185]	2022	Ransomware	LockBit said that its ransomware took down the port's internal computer systems and website. They have reportedly published samples of the stolen material such as financial reports, audits, contracts, cargo information, ship logs, and port documents, among other crucial port-related data. They asked for $1.5 million as a ransom.
DNV (Det Norske Veritas)-Maritime [186]	2023	Ransomware	DNV stated that 70 customers operating around 1000 vessels were impacted by a ransomware attack, close to 15% of its total fleet. The attack was reported to the Norwegian National Security Authority, the Norwegian Data Protection Authority and the German Cyber Security Authority.
Ports of Halifax, Montreal, and Quebec [187]	2023	DDoS	The hackers successfully brought down the ports' websites and overwhelmed their communication networks, making them temporarily offline for customers. In response to the detected threat, the ports' IT officers, cybersecurity experts, and authorities launched an investigation into their network systems to gauge the severity of the attack and identify viable solutions to solve it. Simultaneously, they refrained from using electronic devices and decided to shut down all network operations to mitigate the impact.
Port of Nagoya [188]	2023	Ransomware	Staff found themselves unable to turn on their computers. Shortly after, they received a message from hackers who had infiltrated the network, asking for a ransom for the restoration of the port's loading systems. The port authorities and operators chose not to accept the offer.

nature of blockchain, while beneficial for transparency and data integrity, also means that any unauthorized transaction or error cannot be easily reversed, adding another layer of risk.

These security concerns necessitate stringent measures to protect the integrity of maritime supply chain transactions and maintain the trust of all involved stakeholders.

7. Challenges and future trends of blockchain in the maritime industry

Based on a recent study by law firm HFW (Holman Fenwick Willan) and maritime cyber-security company CyberOwl, 14% of the maritime industry in the word had paid a ransom in 2023 to unlock computer network, up from 3% in 2022 [189]. Cyberattacks that target critical ship equipment—such as the ship mail systems, GPS, Automatic Identification System (AIS), Electronic Chart Display and Information System (ECDIS), and Emergency Position Indicating Radio Beacon (EPIRB)–pose serious risks to navigation safety, especially when they target important components on the bridge. The integrity and dependability of navigation systems are threatened by these attacks, which could have catastrophic effects including crashes, groundings, or navigational errors. Table 7 summarize previous cyberattacks that happened in the last two years. We have noticed that the majority of attacks are Ransomware and Distributed Denial of Service (DDoS) attacks, which are the most severe cyber threats in the maritime industry. Ransomware encrypts critical data or systems until a ransom is paid, thus disrupting operations, and services, and compromising safety. DDoS attacks, on the other hand, flood ship systems with excessive amounts of traffic, causing system overload and inevitable failures targeting the availability of the system. Consequently, the maritime industry urgently needs strong cybersecurity measures and backup plans as these cyberattacks threaten not only the safety of crew members and vessels but also marine transportation, trade, and environmental security.

By offering decentralized and impenetrable solutions, blockchain technology presents an effective way to reduce cyber threats in the marine industry. By implementing blockchain, essential ship equipment such as GPS, AIS, and ECDIS can be significantly less vulnerable to ransomware and DDoS attacks. The capacity of blockchain to improve transparency and traceability is one of the technology's primary benefits for the marine sector. Every transaction and event may be accurately and securely documented using blockchain, establishing a visible and auditable information trail. Lowering fraud, strengthening compliance with rules, and raising stakeholder trust may considerably help the sector.

Additionally, blockchain may automate and streamline several procedures in the marine sector, increasing productivity and lowering costs. Smart contracts, self-executing contracts with predetermined rules stored on the blockchain, can, for instance, automate and enforce contractual agreements between many parties. This can decrease paperwork, eliminate the need for middlemen, and hasten transaction settlement. Blockchain technology may also improve the security of data and transactions. It can guard private data from unauthorized access and modification by utilizing cryptographic methods and decentralized consensus processes. This is especially important in a sector where cyber risks and data breaches are a recurring worry.

Several initiatives and projects have already been initiated to investigate the possibilities of blockchain in the marine sector. For instance, the Maritime Blockchain Labs (MBL) consortium, comprised of businesses like BLOC and Lloyd's Register, wants to provide blockchain solutions for maritime use cases, such as vessel registration, cargo tracking, and port management [190,191]. Similarly, IBM and Maersk's TradeLens platform uses blockchain technology to digitize and automate international trade procedures [192–194]. Blockchain technology has much potential for the marine sector, but difficulties and impediments to its wider implementation exist. These include the necessity for industry-wide cooperation, regulatory uncertainty, and interoperability problems. Close collaboration between industry players, regulatory authorities, and technology suppliers will be necessary to meet these difficulties.

In conclusion, the marine sector has a bright future for blockchain technology. The sector may overcome long-standing obstacles and usher in a new age of digitalization and collaboration by using blockchain technology's transparency, effectiveness, and security. The marine sector is positioned to gain from greater efficiency, lower costs, and improved stakeholder confidence as more initiatives and projects research and adopt blockchain technology.

8. Conclusion

This comprehensive survey paper has outlined the numerous potential consequences of using blockchain technology across various domains within the maritime industry, including supply chain management, maritime logistics, smart contracts, and the Internet of Things (IoT). The inherent attributes of blockchain, such as its capacity to record, encrypt, sign, share, and verify transactions among different users, offer a robust framework for ensuring security, and authenticity within maritime operations.

Nevertheless, there is a growing concern about security as a result of the increasing integration of IoT sensors into port operations. Blockchain shows great promise in protecting the data integrity produced by IoT devices and reducing vulnerabilities in port infrastructures. However, despite its potential, the paper critically addresses the prevalent cyber-security issues within blockchain systems.

Considering these insights, it becomes evident that while blockchain technology holds immense promise for revolutionizing the maritime sector, there exists a pressing need for robust measures to improve its security framework against sophisticated cyberattacks. Moving forward, these efforts must be directed towards the implementation of an advanced security standard to improve the integrity and resilience of blockchain systems within the maritime industry.

CRediT authorship contribution statement

Mohamed Ben Farah: Conceptualization, Data curation, Formal analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, Software, Supervision, Validation, Visualization, Writing – original draft, Writing – review & editing. **Yussuf Ahmed:** Methodology, Resources, Writing – review & editing. **Haithem Mahmoud:** Investigation, Resources, Writing – review & editing. **Syed Attique Shah:** Methodology, Writing – original draft, Writing – review & editing. **Sandy Taramonli:** Investigation, Methodology, Validation. **Xavier Bellekens:** Conceptualization, Investigation, Resources, Supervision. **Raouf Abozariba:** Investigation, Methodology, Supervision, Writing – original draft, Writing – review & editing. **Moad Idrissi:** Investigation, Visualization, Writing – review & editing. **Adel Aneiba:** Funding acquisition, Supervision, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no competing interests.

Data availability

Data will be made available on request.

References

[1] Satoshi Nakamoto, Bitcoin: A peer-to-peer electronic cash system, Decentralized Bus. Rev. (2008).

[2] Matthias Mettler, Blockchain technology in healthcare: The revolution starts here, in: 2016 IEEE 18th International Conference on E-Health Networking, Applications and Services, Healthcom, IEEE, 2016, pp. 1–3.

[3] Chin-Ling Chen, et al., A blockchain-based intelligent anti-switch package in tracing logistics system, J. Supercomput. 77 (2021) 7791–7832.

[4] Shahbaz Siddiqui, et al., Smart contract-based security architecture for collaborative services in municipal smart cities, J. Syst. Archit. 135 (2023) 102802.

[5] Alexandre Dolgui, Dmitry Ivanov, Semyon Potryasaev, Boris Sokolov, Marina Ivanova, Frank Werner, Blockchain-oriented dynamic modelling of smart contract design and execution in the supply chain, Int. J. Prod. Res. 58 (7) (2020) 2184–2199.

[6] Michael Crosby, Pradan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman, et al., Blockchain technology: Beyond bitcoin, Appl. Innov. 2 (6–10) (2016) 71.

[7] Saurabh Singh, Pradip Kumar Sharma, Byungun Yoon, Mohammad Shojafar, Gi Hwan Cho, In-Ho Ra, Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city, Sustainable Cities Soc. 63 (2020) 102364.

[8] Thippa Reddy Gadekallu, et al., Blockchain for edge of things: Applications, opportunities, and challenges, IEEE Internet Things J. 9 (2) (2021) 964–988.

[9] Yanling Chang, et al., Blockchain in global supply chains and cross border trade: a critical synthesis of the state-of-the-art, challenges and opportunities, Int. J. Prod. Res. 58 (7) (2020) 2082–2099.

[10] Stefan Wunderlich, David Saive, The electronic bill of lading, in: International Congress on Blockchain and Applications, Springer, 2019, pp. 93–100.

[11] Hichem Mrabet, et al., A survey of IoT security based on a layered architecture of sensing and data analysis, Sensors 20 (13) (2020) 3625.

[12] Pankaj Dutta, et al., Blockchain technology in supply chain operations: Applications, challenges and research opportunities, Transp. Res. E 142 (2020) 102067.

[13] Maria A. Lambrou, et al., Ambient intelligence technologies in support of shipping markets' operations, Telemat. Inform. 25 (2) (2008) 72–83.

[14] Anne H. Gausdal, Karen V. Czachorowski, Marina Z. Solesvik, Applying blockchain technology: Evidence from Norwegian companies, Sustainability 10 (6) (2018) 1985.

[15] Patrizia Serra, Gianfranco Fancello, Roberto Tonelli, Lodovica Marchesi, Can the blockchain facilitate the development of an interport community? in: International Conference on Computational Science and Its Applications, Springer, 2021, pp. 240–251.

[16] M. Vinod Kumar, N.C.S. Iyengar, A framework for blockchain technology in rice supply chain management, Adv. Sci. Technol. Lett. 146 (2017) 125–130.

[17] Kari Korpela, Jukka Hallikas, Tomi Dahlberg, Digital supply chain transformation toward blockchain integration, in: Proceedings of the 50th Hawaii International Conference on System Sciences.

[18] Amulya Gurtu, Jestin Johny, Potential of blockchain technology in supply chain management: a literature review, Int. J. Phys. Distrib. Logist. Manage. (2019).

[19] Kevin A. Clauson, Elizabeth A. Breeden, Cameron Davidson, Timothy K. Mackey, Leveraging blockchain technology to enhance supply chain management in healthcare: an exploration of challenges and opportunities in the health supply chain, Blockchain Healthc. Today 1 (3) (2018) 1–12.

[20] Christine A. McDaniel, Hanna C. Norberg, Can blockchain technology facilitate international trade? in: Mercatus Research Paper, 2019.

[21] Louise Fjord Kjærsgaard, Blockchain technology and the allocation of taxing rights to payments related to initial coin offerings, Intertax 48 (10) (2020).

[22] Elnaz Irannezhad, Is blockchain a solution for logistics and freight transportation problems? Transp. Res. Procedia 48 (2020) 290–306.

[23] Ashraf Shirani, Blockchain for global maritime logistics, Issues Inf. Syst. 19 (3) (2018).

[24] Luigi Morra, Application of Blockchain Technologies To Logistics and To Container's Transportation Industry, Luiss Guido Carli, 2019.

[25] Olakunle Oloruntobi, Kasypi Mokhtar, Adel Gohari, Saira Asif, Lai Fatt Chuah, Sustainable transition towards greener and cleaner seaborne shipping industry: Challenges and opportunities, Clean. Eng. Technol. (2023) 100628.

[26] Niklas Andersson, Johannes Leander, Replacing Trust: A Study of Blockchain Applicability in Maritime Logistics (B.S. thesis), 2019.

[27] Gülçin Büyüközkan, Gizem Tüfekçi, Deniz Uztürk, Evaluating blockchain requirements for effective digital supply chain management, Int. J. Prod. Econ. 242 (2021) 108309.

[28] Mohsen Attaran, Digital technology enablers and their implications for supply chain management, Supply Chain Forum Int. J. 21 (3) (2020) 158–172.

[29] Christopher Loklindt, Marc-Philip Moeller, Aseem Kinra, How blockchain could be implemented for exchanging documentation in the shipping industry, in: International Conference on Dynamics in Logistics, Springer, 2018, pp. 194–198.

[30] Edvard Tijan, Saša Aksentijević, Katarina Ivanić, Mladen Jardas, Blockchain technology implementation in logistics, Sustainability 11 (4) (2019) 1185.

[31] Yusheng Zhou, Ying Shan Soh, Hui Shan Loh, Kum Fai Yuen, The key challenges and critical success factors of blockchain implementation: Policy implications for Singapore's maritime industry, Mar. Policy (2020) 104265.

[32] Rim Abdallah, Jérôme Besancenot, Cyrille Bertelle, Claude Duvallet, Frédéric Gilletta, An extensive preliminary blockchain survey from a maritime perspective, Smart Cities 6 (2) (2023) 846–877.

[33] Elnaz Irannezhad, The architectural design requirements of a blockchain-based port community system, Logistics 4 (4) (2020) 30.

[34] Shuyi Pu, Jasmine Siu Lee Lam, Blockchain adoptions in the maritime industry: A conceptual framework, Marit. Policy Manag. 48 (6) (2021) 777–794.

[35] Martin Valenta, Philipp Sandner, Comparison of ethereum, hyperledger fabric and corda, Frankf. Sch. Blockchain Cent. 8 (2017) 1–8.

[36] Brenn Hill, Samanyu Chopra, Paul Valencourt, Narayan Prusty, Blockchain Developer's Guide: Develop Smart Applications with Blockchain Technologies-Ethereum, JavaScript, Hyperledger Fabric, and Corda, Packt Publishing Ltd, 2018.

[37] Chinmay Saraf, Siddharth Sabadra, Blockchain platforms: A compendium, in: 2018 IEEE International Conference on Innovative Research and Development, ICIRD, 2018, pp. 1–6.

[38] GT Review, Sanne Wass, Banks pilot new electronic bill of lading capability on voltron blockchain platform, Glob. Trade Rev. (GTR) (2019).

[39] Accenture, Blockchain technology for digital contracting, 2023, https://www.accenture.com/sg-en/case-studies/about/blockchain-contracts-harnessing-new-technology.

[40] Elnaz Irannezhad, Hamed Faroqi, Addressing some of bill of lading issues using the internet of things and blockchain technologies: A digitalized conceptual framework, Marit. Policy Manag. 50 (4) (2023) 428–446.

[41] Huiru Liu, Blockchain and Bills of Lading: Legal Issues in Perspective, Maritime Law in Motion, Springer, 2020, pp. 413–435.

[42] Koji Takahashi, Blockchain technology and electronic bills of lading, J. Int. Marit. Law 22 (2016) 202–211.

[43] Elson. Ong, Blockchain bills of lading, in: NUS Law Working Paper, 2018.

[44] CargoX, Reshaping the future of global trade with world's first blockchain bill of lading, 2018.

[45] IBM, IBM Introduces TradeLens Blockchain Shipping Solution, IBM Newsroom, 2018, https://newsroom.ibm.com/2018-08-09-Maersk-and-IBM-Introduce-TradeLens-Blockchain-Shipping-Solution.

[46] Kunpeng Li, et al., Blockchain in maritime supply chain: A synthesis analysis of benefits, challenges and limitations, J. Supply Chain Oper. Manag. 18 (2) (2020) 257.

[47] Robert Philipp, et al., Blockchain and smart contracts for entrepreneurial collaboration in maritime supply chains, Transp. Telecomm. J. 20 (4) (2019) 365–378.

[48] Manos-Nikolaos Papadakis, Evangelia Kopanaki, Innovative maritime operations management using blockchain technology & standardization, J. ICT Stand. (2022) 469–508.

[49] Johannes Schnelle, et al., Framework for the adoption of blockchain in maritime cold chains, in: Changing Tides: The New Role of Resilience and Sustainability in Logistics and Supply Chain Management–Innovative Approaches for the Shift To a New Era–Proceedings of the Hamburg International Conference of Logistics, Vol. 33, HICL, epubli GmbH, Berlin, 2022, pp. 121–148.

[50] Person, PIL, PSA and IBM To Collaborate on Innovative Blockchain Technology, Supply Chain Magazine, 2020, https://supplychaindigital.com/technology/pil-psa-and-ibm-collaborate-innovative-blockchain-technology.

[51] N. Morris, Kuehne+Nagel, largest freight forwarder adopts blockchain, 2020.

[52] Feruz K. Elmay, et al., Using NFTs and blockchain for traceability and auctioning of shipping containers and cargo in maritime industry, IEEE Access 10 (2022) 124507–124522.

[53] Johannes Hinckeldeyn, Jochen Kreutzfeldt, (Short paper) Developing a smart storage container for a blockchain-based supply chain application, in: 2018 Crypto Valley Conference on Blockchain Technology, CVCBT, 2018, pp. 97–100.

[54] Lei Xu, et al., Binding the physical and cyber worlds: A blockchain approach for cargo supply chain security enhancement, in: 2018 IEEE International Symposium on Technologies for Homeland Security, HST, IEEE, 2018, pp. 1–5.

[55] Nicky Morris, EY Maersk Blockchain Marine Insurance Platform Goes Live, Ledger Insights - Blockchain for Enterprise, 2018, https://www.ledgerinsights.com/blockchain-marine-insurance/.

[56] Radboud Vlaar, Banking Giant ING Is Quietly Becoming a Serious Blockchain Innovator, Passle, 2018, https://news.finchcapital.com/post/102euxn/banking-giant-ing-is-quietly-becoming-a-serious-blockchain-innovator.

[57] Nicky Morris, Riskblock Confirms R3 Corda Switch, Partners with Accenture, Ledger Insights - Blockchain for Enterprise, 2020, https://www.ledgerinsights.com/riskblock-confirms-r3-corda-accenture-blockchain/.

[58] Filip Caron, The evolving payments landscape: Technological innovation in payment systems, IT Prof. 20 (2) (2018) 53–61.

[59] Bo Lu, et al., Design and value analysis of the blockchain-based port logistics financial platform, Marit. Policy Manag. (2023) 1–25.

[60] Jiaguo Liu, et al., Blockchain technology in maritime supply chains: Applications, architecture and challenges, Int. J. Prod. Res. (2021) 1–17.

[61] Karen Czachorowski, Marina Solesvik, Yuriy Kondratenko, The application of blockchain technology in the maritime industry, in: Green IT Engineering: Social, Business and Industrial Applications, Springer, 2019, pp. 561–577.

[62] Chung-Shan Yang, Maritime shipping digitalization: Blockchain-based technology applications, future improvements, and intention to use, Transp. Res. E 131 (2019) 108–117.

[63] Ivan Peronja, Kristijan Lenac, Roko Glavinović, Blockchain technology in maritime industry, Pomorstvo 34 (1) (2020) 178–184.

[64] Maersk, (2020). https://www.maersk.com/news/articles/2022/09/21/from-kenya-to-the-world-flowers-by-ocean.

[65] FreightWaves Staff, Unchained: Cargochain To Ease Supply Chain Data Sharing, Port Technology International, 2019, https://www.freightwaves.com/news/blockchain/cargochain-launch-of-business.

[66] Port Technology Team, Port of Rotterdam Introduces Quay Connect Blockchain Technology, Port Technology International, 2021, Available online: https://www.porttechnology.org/news/port-of-rotterdam-introduces-quay-connect-blockchain-technology/.

[67] SCOR, (2018). https://www.scor.com/en/expert-views/b3i-blockchain-insurance-industry-initiative-scor-annual-conference-2018.

[68] LLoyds, (2020). https://lloydslist.maritimeintelligence.informa.com/LL110930/PIL-and-PSA-jump-on-the-blockchain-bandwagon-with-IBM, Lloyd's List.

[69] Supplychain-digital, (2020). https://supplychaindigital.com/technology/abu-dhabi-ports-launches-blockchain-platform-imports-and-exports, Supply Chain Magazine.

[70] CargoX, (2020). https://cargox.io/press-releases/first-ever-blockchain-based-cargox-smart-bl-has-successfully-completed-its-historic-mission/.

[71] Valentina Gatteschi, et al., Blockchain and smart contracts for insurance: Is the technology mature enough? Future Internet 10 (2) (2018) 20.

[72] Port Technology International Team, Singapore Launches Maritime Blockchain, Port Technology International, 2019, https://www.porttechnology.org/news/singapore_launches_maritime_blockchain/.

[73] Oocllogistics.com, https://www.oocllogistics.com/eng/newsandmedia/news/2022/Pages/20220419.aspx.

[74] ondernemen010, Cargoledger, Blockchain Solutions for the Supply Chain, Rotterdam Innovation City, 2019, https://www.startuprotterdam.com/News/cargoledger/.

[75] Niels Hackius, et al., The privacy barrier for blockchain in logistics: First lessons from the port of hamburg, in: Logistics Management: Strategies and Instruments for Digitalizing and Decarbonizing Supply Chains–Proceedings of the German Academic Association for Business Research, Halle, 2019, Springer, 2019, pp. 45–61.

[76] Reza Karimpour, et al., Circular economy approach to facilitate the transition of the port cities into self-sustainable energy ports—A case study in copenhagen-Malmö Port (CMP), WMU J. Marit. Aff. 18 (2019) 225–247.

[77] Muhammad Iqbal Hafizon, Adhi Wicaksono, Fabian Nur Farizan, E-toll laut: Blockchain port as the key for realizing Indonesia's maritime fulcrum, in: Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance, 2019, pp. 36–45.

[78] Marija Jović, Edvard Tijan, Dražen. Žgaljić, Saša Aksentijević, Improving maritime transport sustainability using blockchain-based information exchange, Sustainability 12 (21) (2020) 8866.

[79] Port Technology Team, CargoSmart, Cosco, SIPG and Tesla Launch Cargo Blockchain Pilot, Port Technology International, 2020.

[80] Mohammed Ali Alqarni, Mohammed Saeed Alkatheiri, Sajjad Hussain Chauhdary, Sajid Saleem, Use of blockchain-based smart contracts in logistics and supply chains, Electronics 12 (6) (2023) 1340.

[81] Raja Wasim Ahmad, Haya Hasan, Raja Jayaraman, Khaled Salah, Mohammed Omar, Blockchain applications and architectures for port operations and logistics management, Res. Transp. Bus. Manag. 41 (2021) 100620.

[82] Cahyono Budy Santoso, Harjanto Prabowo, Harco Leslie Hendric Spits Warnars, Ahmad Nurul Fajar, Smart insurance system model concept for marine cargo business, in: 2021 International Conference on Data Science and Its Applications, ICoDSA, IEEE, 2021, pp. 281–286.

[83] Yang Wang, Peng Chen, Bing Wu, Chengpeng Wan, Zaili Yang, A trustable architecture over blockchain to facilitate maritime administration for MASS systems, Reliab. Eng. Syst. Saf. 219 (2022) 108246.

[84] Payam Rahimi, Nasir D. Khan, Chrysostomos Chrysostomou, Vasos Vassiliou, Babar Nazir, A secure communication for maritime iot applications using blockchain technology, in: 2020 16th International Conference on Distributed Computing in Sensor Systems, DCOSS, IEEE, 2020, pp. 244–251.

[85] Jiaguo Liu, Huimin Zhang, Lu Zhen, Blockchain technology in maritime supply chains: Applications, architecture and challenges, Int. J. Prod. Res. 61 (11) (2023) 3547–3563.

[86] Trung-Viet Nguyen, et al., PenChain: A blockchain-based platform for penalty-aware service provisioning, IEEE Access (2023).

[87] Warlley Paulo Freire, Wilson S. Melo Jr., Vinicius D. do Nascimento, Paulo R.M. Nascimento, Alan Oliveira de Sá, Towards a secure and scalable maritime monitoring system using blockchain and low-cost IoT technology, Sensors 22 (13) (2022) 4895.

[88] Ziaul Haque Munim, Okan Duru, Enna Hirata, Rise, fall, and recovery of blockchains in the maritime technology space, J. Mar. Sci. Eng. 9 (3) (2021) 266.

[89] Marko Perkušić, Šime Jozipović, Damir Piplica, The need for legal regulation of blockchain and smart contracts in the shipping industry, Trans. Marit. Sci. 9 (02) (2020) 365–373.

[90] Srdjan Vujičić, Nermin Hasanspahić, Maro Car, Leo Čampara, Distributed ledger technology as a tool for environmental sustainability in the shipping industry, J. Mar. Sci. Eng. 8 (5) (2020) 366.

[91] Marija Jović, Edvard Tijan, Rebecca Marx, Berit Gebhard, Big data management in maritime transport, Pomorski zbornik 57 (1) (2019) 123–141.

[92] John Steffen, Hyodae Seo, Carol Anne Clayson, Suyang Pei, Toshiaki Shinoda, Impacts of tidal mixing on diurnal and intraseasonal air-sea interactions in the maritime continent, Deep Sea Res. II Top. Stud. Oceanogr. 212 (2023) 105343.

[93] Saeyeon Roh, Vinh V. Thai, Hyunmi Jang, Gi-Tae Yeo, The best practices of port sustainable development: A case study in Korea, Marit. Policy Manag. 50 (2) (2023) 254–280.

[94] Koasidis Konstantinos, A. Nikas, V. Daniil, E. Kanellou, H. Doukas, A multi-criteria decision support framework for assessing seaport sustainability planning: The case of Piraeus, Marit. Policy Manag. 50 (8) (2023) 1030–1056.

[95] Oskari Lähdeaho, Olli-Pekka Hilmola, Business models amid changes in regulation and environment: The case of Finland–Russia, Sustainability 12 (8) (2020) 3393.

[96] Changping Zhao, Yecheng Wang, Yu Gong, Steve Brown, Rui Li, The evolution of the port network along the maritime silk road: From a sustainable development perspective, Mar. Policy 126 (2021) 104426.

[97] Chengpeng Wan, Yinxiang Zhao, Di Zhang, Tsz Leung Yip, Identifying important ports in maritime container shipping networks along the Maritime Silk Road, Ocean & Coastal Management 211 (2021) 105738.

[98] Nazir Imran, Muhammad Shujaat Mubarik, Navaz Naghavi, Sharfuddin Ahmed Khan, An application of multi-criteria data management approach for prioritisation of unwarranted causes of delay in international shipments, Int. J. Integr. Supply Manag. 15 (3) (2022) 233–252.

[99] Tommi Inkinen, Esa Hämäläinen, Reviewing truck logistics: Solutions for achieving low emission road freight transport, Sustainability 12 (17) (2020) 6714.

[100] Alaa Othman, Sara El Gazzar, Matjaz Knez, Investigating the influences of smart port practices and technology employment on port sustainable performance: the Egypt case, Sustainability 14 (21) (2022) 14014.

[101] Alessandro Liberati, Douglas G. Altman, Jennifer Tetzlaff, Cynthia Mulrow, Peter C. Gøtzsche, John P.A. Ioannidis, Mike Clarke, Philip J. Devereaux, Jos Kleijnen, David Moher, The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: Explanation and elaboration, Ann. Intern. Med. 151 (4) (2009) W–65.

[102] Claes Wohlin, Guidelines for snowballing in systematic literature studies and a replication in software engineering, in: Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering, 2014, pp. 1–10.

[103] Eric Lambourdiere, Elsa Corbin, Blockchain and maritime supply-chain performance: dynamic capabilities perspective, Worldw. Hosp. Tour. Themes (2020).

[104] Fran Casino, Thomas K. Dasaklis, Constantinos Patsakis, A systematic literature review of blockchain-based applications: current status, classification and open issues, Telemat. Inform. 36 (2019) 55–81.

[105] Khalid Bichou, Richard Gray, A logistics and supply chain management approach to port performance measurement, Marit. Policy Manag. 31 (1) (2004) 47–67.

[106] Antoine Frémont, Empirical Evidence for Integration and Disintegration of Maritime Shipping, Port and Logistics Activities, OECD, 2010.

[107] Yossi Sheffi, Logistics-intensive clusters: Global competitiveness and regional growth, in: Handbook of Global Logistics: Transportation in International Supply Chains, 2012, pp. 463–500.

[108] Giorgio Bavassano, Claudio Ferrari, Alessio Tei, Blockchain: How shipping industry is dealing with the ultimate technological leap, Res. Transp. Bus. Manag. (2020) 100428.

[109] Kay Behnke, M.F.W.H.A. Janssen, Boundary conditions for traceability in food supply chains using blockchain technology, Int. J. Inf. Manage. 52 (2020) 101969.

[110] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, Huaimin Wang, Blockchain challenges and opportunities: A survey, Int. J. Web Grid Serv. 14 (4) (2018) 352–375.

[111] Marija Jović, Edvard Tijan, Saša Aksentijević, Dragan Čišić, An overview of security challenges of seaport IoT systems, in: 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO, IEEE, 2019, pp. 1349–1354.

[112] 'Smart' and sustainable ports, 2021, https://www.greenport.com/news101/Projects-and-Initiatives/smart-and-sustainable-ports. (Accessed 05 January 2021).

[113] Best of 2017: Port of rotterdam uses 3D printing to repair damaged ship parts, 2021, https://worldindustrialreporter.com/port-of-rotterdam-uses-3d-printing-to-repair-damaged-ship-parts/. (Accessed 05 January 2021).

[114] Smart ports and smart infrastructure big data and simulations, 2021, http://www.dutchbss.org/wp-content/uploads/2016/11/simulations-20161208_JanEGbersten.pdf. (Accessed 05 January 2021).

[115] Ahmadhon Kamolov, Suhyun Park, An IoT-based ship berthing method using a set of ultrasonic sensors, Sensors 19 (23) (2019) 5181.

[116] Frederic Vannieuwenborg, Sofie Verbrugge, Didier Colle, Choosing IoT-connectivity? A guiding methodology based on functional characteristics and economic considerations, Trans. Emerg. Telecommun. Technol. 29 (5) (2018) e3308.

[117] Anton Esser, Christa Sys, Thierry Vanelslander, Ann Verhetsel, The labour market for the port of the future. A case study for the port of Antwerp, Case Stud. Transp. Policy 8 (2) (2020) 349–360.

[118] Alberto Rodrigo González, Nicoleta González-Cancelas, Beatriz Molina Serrano, Alberto Camarero Orive, Smart ports: ranking of spanish port system, World Sci. News 144 (2020) 1–12.

[119] Marco Ferretti, Francesco Schiavone, Majed Al-Mashari, Manlio Del Giudice, Internet of things and business processes redesign in seaports. The case of hamburg, Bus. Process Manag. J. (2016).

[120] Meisu Zhong, Yongsheng Yang, Haiqing Yao, Xiuwen Fu, Octavia A. Dobre, Octavian Postolache, 5G and IoT: Towards a new era of communications and measurements, IEEE Instrum. Meas. Mag. 22 (6) (2019) 18–26.

[121] Carlos Jahn, Sebastian Saxe, Digitalization of seaports-visions of the future, in: Fraunhofer Center for Port Operations and Services, CML, 2017, pp. 28–32.

[122] Mehrdokht Pournader, Yangyan Shi, Stefan Seuring, S.C. Lenny Koh, Blockchain applications in supply chains, transport and logistics: a systematic review of the literature, Int. J. Prod. Res. 58 (7) (2020) 2063–2081.

[123] Petri Helo, A.H.M. Shamsuzzoha, Real-time supply chain—A blockchain architecture for project deliveries, Robot. Comput.-Integr. Manuf. 63 (2020) 101909.

[124] Mizna Khalid, et al., Towards SDN-based smart contract solution for IoT access control, Comput. Commun. 198 (2023) 1–31.

[125] Konstantinos Christidis, Michael Devetsikiotis, Blockchains and smart contracts for the internet of things, IEEE Access 4 (2016) 2292–2303.

[126] Elli Androulaki, et al., Hyperledger fabric: a distributed operating system for permissioned blockchains, in: Proceedings of the Thirteenth EuroSys Conference, 2018, pp. 1–15.

[127] How to represent a blockchain through a mathematical model? 2021, https://canopee-group.com/wp-content/uploads/2020/05/Blockchain-Coperneec.pdf/. (Accessed 17 January 2021).

[128] Deepak Puthal, Saraju P. Mohanty, Priyadarsi Nanda, Elias Kougianos, Gautam Das, Proof-of-authentication for scalable blockchain in resource-constrained distributed systems, in: 2019 IEEE International Conference on Consumer Electronics, ICCE, IEEE, 2019, pp. 1–5.

[129] Metin Ozturk, Mona Jaber, Muhammad A. Imran, Energy-aware smart connectivity for IoT networks: Enabling smart ports, Wirel. Commun. Mob. Comput. 2018 (2018).

[130] Karim Jabbar, Pernille Bjørn, Infrastructural grind: Introducing blockchain technology in the shipping domain, in: Proceedings of the 2018 ACM Conference on Supporting Groupwork, 2018, pp. 297–308.

[131] Wei Chen, et al., A survey of maritime communications: From the wireless channel measurements and modeling perspective, Reg. Stud. Mar. Sci. 48 (2021) 102031.

[132] Jun-Bo Wang, et al., Unmanned surface vessel assisted maritime wireless communication toward 6G: Opportunities and challenges, IEEE Wirel. Commun. 29 (6) (2022) 72–79.

[133] Saurab Rauniyar, et al., Mobile connectivity beyond the coast-line: A case study for next generation shipping, in: 2023 IEEE 98th Vehicular Technology Conference, VTC2023-Fall, 2023, pp. 1–7.

[134] Te Wei, et al., Hybrid satellite-terrestrial communication networks for the maritime Internet of Things: Key technologies, opportunities, and challenges, IEEE Internet Things J. 8 (11) (2021) 8910–8934.

[135] Christian Bueger, et al., Security threats to undersea communications cables and infrastructure–consequences for the EU, in: Report for SEDE Committee of the European Parliament, PE702, 2022, p. 557.

[136] Sami Ma, et al., Network characteristics of LEO satellite constellations: A starlink-based measurement from end users, in: IEEE INFOCOM 2023-IEEE Conference on Computer Communications, 2023, pp. 1–10.

[137] Tyler Przybylski, et al., Aircraft communication systems-topologies, protocols, and vulnerabilities, J. Netw. Comput. Appl. (2023).

[138] Todd E. Humphreys, et al., Signal structure of the starlink ku-band downlink, IEEE Trans. Aerosp. Electron. Syst. (2023).

[139] Jaya Shankar Pathmasuntharam, et al., High speed maritime ship-to-ship/shore mesh networks, in: 2007 7th International Conference on ITS Telecommunications, IEEE, 2007, pp. 1–6.

[140] Ming-Tuo Zhou, et al., TRITON: high-speed maritime wireless mesh network, IEEE Wirel. Commun. 20 (5) (2013) 134–142.

[141] Jue Wang, et al., Wireless channel models for maritime communications, IEEE Access 6 (2018) 68070–68088.

[142] Wencai Du, et al., Integrated wireless networking architecture for maritime communications, in: 2010 11th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, IEEE, 2010, pp. 134–138.

[143] Hussein Kdouh, et al., Wireless sensor network on board vessels, in: 2012 19th International Conference on Telecommunications, ICT, 2012, pp. 1–6.

[144] Hussein Kdouh, et al., Performance analysis of a hierarchical shipboard wireless sensor network, in: 2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC, 2012, pp. 765–770.

[145] Brecht De Beelde, et al., 60 GHz path loss modelling inside ships, in: 2020 14th European Conference on Antennas and Propagation, EuCAP, 2020, pp. 1–5.

[146] Tharaka Hewa, et al., The role of blockchain in 6G: Challenges, opportunities and research directions, in: 2020 2nd 6G Wireless Summit, 6G SUMMIT, 2020, pp. 1–5.

[147] Bitcoin, S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2008.

[148] Laphou Lao, et al., A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling, ACM Comput. Surv. 53 (1) (2020) 1–32.

[149] Author's Name, Title of the Article, 2023, https://www.theregister.com/2023/04/27/singapores_maritime_5g/. (Accessed 7 February 2024).

[150] Port of Antwerp Bruges, Its own 5G network in zeebrugge ready for the future, 2024, https://www.portofantwerpbruges.com/en/news/its-own-5g-network-zeebrugge-ready-future. (Accessed 7 February 2024).

[151] Sheraz Aslam, et al., Internet of ships: A survey on architectures, emerging applications, and challenges, IEEE Internet Things J. 7 (10) (2020) 9714–9727.

[152] Kan Zheng, et al., Heterogeneous vehicular networking: A survey on architecture, challenges, and solutions, IEEE Commun. Surv. Tutor. 17 (4) (2015) 2377–2396.

[153] Shuai Wang, et al., Blockchain-enabled smart contracts: architecture, applications, and future trends, IEEE Trans. Syst. Man Cybern. A 49 (11) (2019) 2266–2277.

[154] Yaser Mansouri, et al., An automated implementation of hybrid cloud for performance evaluation of distributed databases, J. Netw. Comput. Appl. 167 (2020) 102740.

[155] Hau-Ling Chan, et al., The SMARTER framework and real application cases of blockchain, Technol. Forecast. Soc. Change 196 (2023) 122798.

[156] Mehmet Baygin, et al., A blockchain-based approach to smart cargo transportation using UHF RFID, Expert Syst. Appl. 188 (2022) 116030.

[157] Ahto Buldas, et al., An ultra-scalable blockchain platform for universal asset tokenization: design and implementation, IEEE Access 10 (2022) 77284–77322.

[158] Yassine Maleh, et al., Blockchain for cyber–physical systems: Challenges and applications, in: Advances in Blockchain Technology for Cyber Physical Systems, 2022, pp. 11–59.

[159] Tianyi Liu, Diansheng Li, Study on the new implementation mode of cross-docking based on blockchain technology, Comput. Ind. Eng. 180 (2023) 109249.

[160] Xu Xin, et al., Investment strategy for blockchain technology in a shipping supply chain, Ocean & Coastal Management 226 (2022) 106263.

[161] Mohamed Amine Ben Farah, Elochukwu Ukwandu, Hanan Hindy, David Brosset, Miroslav Bures, Ivan Andonovic, Xavier Bellekens, Cyber security in the maritime industry: A systematic survey of recent advances and future trends, Information 13 (1) (2022) 22.

[162] Mohamed Ben Farah, M. Omar Al-Kadri, Yussuf Ahmed, Raouf Abouzariba, Xavier Bellekens, Cyber incident scenarios in the maritime industry: Risk assessment and mitigation strategies, in: 2023 IEEE International Conference on Cyber Security and Resilience, CSR, 2023, pp. 194–199.

[163] Huru Hasanova, Ui-jun Baek, Mu-gon Shin, Kyunghee Cho, Myung-Sup Kim, A survey on blockchain cybersecurity vulnerabilities and possible countermeasures, Int. J. Netw. Manage. 29 (2) (2019) e2060.

[164] N. Anita, M. Vijayalakshmi, Blockchain security attack: A brief survey, in: 2019 10th International Conference on Computing, Communication and Networking Technologies, ICCCNT, 2019, pp. 1–6.

[165] Om Pal, Bashir Alam, Vinay Thakur, Surendra Singh, Key management for blockchain technology, ICT Express 7 (1) (2021) 76–80.

[166] Huaqun Guo, Xingjie Yu, A survey on blockchain technology and its security, Blockchain Res. Appl. 3 (2) (2022) 100067.

[167] Fahad Saleh, Blockchain without waste: Proof-of-stake, Rev. Financ. Stud. 34 (3) (2021) 1156–1190.

[168] A.K.M. Bahalul Haque, A.K.M. Najmul Islam, Sami Hyrynsalmi, Bilal Naqvi, Kari Smolander, GDPR compliant blockchains–A systematic literature review, IEEE Access 9 (2021) 50593–50606.

[169] Kriangsak Kittichaisaree, Jurisdiction and Attribution of State Responsibility in Cyberspace, Public International Law of Cyberspace, Springer, 2017, pp. 23–44.

[170] W. Gregory Voss, Cross-border data flows, the GDPR, and data governance, Wash. Int'l LJ 29 (2019) 485.

[171] Eugenia Politou, Efthimios Alepis, Maria Virvou, Constantinos Patsakis, The right to be forgotten in the GDPR: implementation challenges and potential solutions, in: Privacy and Data Protection Challenges in the Distributed Era, Springer, 2022, pp. 41–68.

[172] Ilaria Zavoli, Colin King, The challenges of implementing anti-money laundering regulation: An empirical analysis, Mod. Law Rev. 84 (4) (2021) 740–771.

[173] International Maritime Organization (IMO), (2019). https://www.imo.org/en/About/Pages/Default.aspx.

[174] International Maritime Organization (IMO), (2019). https://www.imo.org/en/OurWork/Legal/Pages/UnitedNationsConventionOnTheLawOfTheSea.aspx.

[175] European Commission, (2004). https://www.legislation.gov.uk/eur/2004/725/data.pdf.

[176] International Maritime Organization (IMO), (2017). https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.428(98).pdf.

[177] Maritime Executive, (2022). https://maritime-executive.com/editorials/the-imo-2021-cyber-guidelines-and-the-need-to-secure-seaports.

[178] Enisa Europe, Cybersecurity in the maritime sector: ENISA releases new guidelines for navigating cyber risk, 2020, https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-maritime-sector-enisa-releases-new-guidelines-for-navigating-cyber-risk.

[179] Enisa Europe, Guidelines: Cyber risk management for ports, 2020, https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports.

[180] Maritime UK, MASS UK industry conduct principles and code of practice 2021, 2021, https://www.maritimeuk.org/priorities/innovation/maritime-uk-autonomous-systems-regulatory-working-group/mass-uk-industry-conduct-principles-and-code-practice-2021-v5/.

[181] Md Rafiqul Islam, et al., A review on blockchain security issues and challenges, in: 2021 IEEE 12th Control and System Graduate Research Colloquium, ICSGRC, IEEE, 2021, pp. 227–232.

[182] Iuon-Chang Lin, Tzu-Chun Liao, A survey of blockchain security issues and challenges, IJ Netw. Secur. 19 (5) (2017) 653–659.

[183] Sembcorp Marine, Sembcorp marine reports cyber incident; moves to address incident and support affected stakeholders, 2022, https://www.sembmarine.com/stock-exchange-announcements/sembcorp-marine-reports-cyber-incident-moves-to-address-incident-and-support-affected-stakeholders.

[184] Riviera News, Voyager fleet insight platform hit by cyber-security incident, 2022, https://www.rivieramm.com/news-content-hub/news-content-hub/voyager-fleet-insight-unavailable-after-cyber-security-incident-74229.

[185] Rakin Rahman, Cyber-attack threatens release of Port of Lisbon data, 2023, https://www.porttechnology.org/news/cyber-attack-threatens-release-of-port-of-lisbon-data/.

[186] Jamey Bergman, DNV: 'all users back online' two months after ShipManager cyber attack hit 1,000 vessels, 2023, https://www.rivieramm.com/news-content-hub/news-content-hub/dnv-reports-cyber-attack-on-its-shipmanager-software-74466.

[187] Chalermpong Senarak, Port cyberattacks from 2011 to 2023: a literature review and discussion of selected cases, Marit. Econ. Logist. (2023) 1–26.

[188] Jamey Bergman, Critical infrastructure cyberattack on Japan's biggest port, 2023, https://techwireasia.com/07/2023/critical-infrastructure-cyberattack-on-japans-biggest-port/.

[189] Martyn Wingrove, 14% of maritime industry hit by ransomware payments, 2023, https://www.rivieramm.com/news-content-hub/news-content-hub/cyber-security-solution-unveiled-as-maritime-incidents-rise-78685.

[190] Daniel Adam, Dante Benjamin Matellini, Anna Kaparaki, Blockchain: Research and Applications.

[191] Nexhat Kapidani, Intelligent Use of Maritime Info-Communication Systems in Developing Environments (Ph.D. thesis), 2023.

[192] Friedrich Lorenz-Meyer, Vitor Santos, Blockchain in the shipping industry: A proposal for the use of blockchain for SMEs in the maritime industry, Procedia Comput. Sci. 219 (2023) 807–814.

[193] Helmi Hannila, Utilizing blockchain technology in sustainable supply chain management: Benefits, challenges, and motivations, 2023.

[194] Son Nguyen, Peggy Shu-Ling Chen, Yuquan Du, Blockchain adoption in container shipping: An empirical study on barriers, approaches, and recommendations, Mar. Policy 155 (2023) 105724.

Further reading

[1] Niels Hackius, Moritz Petersen, Blockchain in logistics and supply chain: trick or treat? in: Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment. Proceedings of the Hamburg International Conference of Logistics, Vol. 23, HICL, epubli GmbH, Berlin, 2017, pp. 3–18.

Dr Mohamed Ben Farah (BEng, M.Sc., Ph.D., HDR) is currently a Lecturer in Networks and Cyber-Security at Birmingham City University. Dr Mohamed held a research associate position in cybersecurity at the Institute for Signals, Sensors, and Communications within the Department of Electronic and Electrical Engineering at the University of Strathclyde. Mohamed's research interests span diverse areas within cybersecurity and engineering, including pervasive security for IoT devices, machine learning techniques, blockchain, as well as privacy and encryption.

Dr Yussuf Ahmed is a Senior Lecturer in Cyber Security and Director of the BSc/MSci Cyber Security Programmes at Birmingham City University. He is a Senior Fellow of the Higher Education Academy (SFHEA) and specializes in Information Security, Cyber Assurance, Network Security, Cyber risks, and Security Governance. Yussuf is an experienced Cyber security professional with over 15 years of experience working in the industry before joining Birmingham City University and holds various industry certifications.

Dr Haitham Mahmoud is a research fellow in the Future Communication Systems research group at BCU, where he is involved in cutting-edge research projects. He is also part of the Next Generation Radio-Access Network (NGRAN) team. He has made significant contributions to numerous funded projects as a highly effective research coordinator and dedicated research assistant. Moreover, he has also served as a Teaching Assistant and Assistant Lecturer at The British University in Egypt for four years. Furthermore, he is an accomplished author, having published numerous peer-reviewed articles in prestigious journals and conferences, and has reviewed over 150 manuscripts in IEEE magazines, IEEE transactions, MDPI, and others.

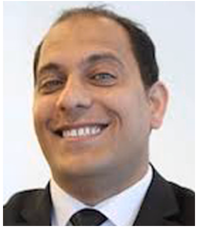
Dr. Syed Attique Shah is working as a Lecturer in Smart Computer Systems, at the School of Computing and Digital Technology, Birmingham City University, UK. Dr Shah has more than 10 years of experience in teaching and research. Previously, he was working as a Lecturer/Assistant Professor at the Data Systems Group, Institute of Computer Science, University of Tartu, Estonia. He has published more than 20 research papers in reputable Q1 journals. He has also presented several research papers at internationally renowned conferences. His research interests include big data analytics, information management, software-defined networking, and the Internet of Things

Dr M. Omar Alkadri is an Associate Professor in Cyber Security at the College of Computing and Information Technologies, University of Doha for Science and Technology. His research interests include AI Applications on Cyber Security, Intrusion Detection Systems, Network Security, Wireless Communications Protocols and Security, IoT Security, Security of CAN Networks, and Security of Healthcare Wireless Networks.

Dr Sandy Taramonli is an Assistant Professor in Cyber Security at the University of Warwick. She is a Fellow of the Higher Education Academy, and she specializes in the areas of network forensics and cryptography. Sandy was awarded a Ph.D. in Energy Conscious Adaptive Security from the University of Warwick in 2015. Her research interests are focussing on low energy encryption, stochastic log file analysis for network intrusion detection and network forensics.

Dr Xavier Bellekens (B.Sc., M.Sc., Ph.D., FHEA, MBCS, MIEEE) is the CEO and co-founder of Lupovis.io a cyber-deception spin-out of the University of Strathclyde, and a Non-resident Senior Fellow of the Scowcroft Centre for Strategy and Security at the Atlantic Council advising on critical-infrastructures, maritime and naval cyber-security and an Assistant Professor Chancellor's Fellow in the Institute for Signals, Sensors and Communications with the Department of Electronic and Electrical Engineering at the University of Strathclyde, His current research interests include critical infrastructure protection, defense as well as cyber deception and deterrence. Xavier is also the Chair of the Blockchain Group, and the Vice-Chair of Cyber-Security Group for IEEE UK and Ireland. He frequently appears in the media to provide commentary to international press on radio, TV and newspapers on major cyber-events.

Dr Raouf Abozariba (Member, IEEE) received the Ph.D. degree from Staffordshire University in 2017, and was a Senior Research Associate with the School of Computing and Communications, Lancaster University, U.K. He joined Birmingham City University, U.K., in 2019, where he is currently a Senior Lecturer with the College of Computing.



Dr Adel Aneiba received the B.Sc. degree in Computer Science from the University of Benghazi in Libya, the M.Sc. degree in e-commerce from Staffordshire University in the year 2003, and the Ph.D. degree in Computing in the year 2008. He is a professor on the Internet of Things (IoT) at Birmingham City University, UK. His research interests include IoT, computer network simulation, evaluation, optimization and blockchain. He is a Member of IET.