IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 5 November 2025, accepted 19 November 2025, date of publication 25 November 2025,
date of current version 4 December 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3636470

RESEARCH ARTICLE

Blockchain for Maritime Supply Chain: Efficiency and Security Advancements

JOEL CURADO[1], MANILA BHANDARI[1], JOÃO C. FERREIRA[1,2,4], AND ANA L. MARTINS[3,4]
[1]ISTAR, Instituto Universitário de Lisboa (ISCTE-IUL), 1649-026 Lisboa, Portugal
[2]Molde University, 6410 Molde, Norway
[3]Business Research Unit (BRU-IUL), ISCTE—University Institute of Lisbon, 1649-026 Lisbon, Portugal
[4]INOV-INESC Inovação Instituto de Novas Tecnologias, 1000-029 Lisbon, Portugal

Corresponding author: João C. Ferreira (joam@himolde.no)

This work was supported by the National Funds through FCT—Fundação para a Ciência e a Tecnologia, I.P., under Project UID/6486/2025, Project UID/PRR/6486/2025, and Project UID/315/2025.

ABSTRACT The maritime supply chain plays a vital role in global trade, but it continues to face major challenges, including transparency issues, fraud, and data privacy concerns. Blockchain technology has emerged as a promising solution to make the supply chain more secure, efficient, and trustworthy across the system. However, it still encounters limitations, especially regarding privacy and the handling of large volumes of data. To address these issues, Zero-Knowledge Proofs (ZKPs) offer a viable solution, enabling the validation of documents and transactions without revealing sensitive information. This helps maintain confidentiality while meeting regulatory requirements, such as those set by the eFTI regulation. This paper investigates blockchain adoption in maritime supply chains with a focus on ZKP integration for secure document verification, fraud mitigation, and regulatory compliance. It evaluates computational overhead, scalability, and adoption barriers, and proposes a framework supported by simulation-based validation using Ethereum and ZoKrates to assess feasibility and performance. By combining ZKPs with blockchain, this approach enhances a secure, transparent, and efficient trade ecosystem, optimising resources and reducing risks. Future research directions are outlined to advance sustainable maritime logistics.

INDEX TERMS Blockchain technology, cryptography, data privacy, governance, maritime supply chain management, zero-knowledge proof.

I. INTRODUCTION

With globalisation and international trade on the rise, maritime supply chains are now the centre of global partnerships and usually deal with a progressively complex situation. Recognised for cost-efficiency and reliability, shipping remains the dominant force in worldwide trade logistics. Yet there is some logistics handling complexity in maritime represented by numerous stakeholders and high reliance on transport documents that usually delays the smooth handovers of goods [1]. Handling nearly 90% of global goods, maritime logistics is critical for economic stability, yet it faces various challenges, which include inefficiencies, document fraud and data privacy concerns [2]. Research estimates that 40% of delays in the supply chains at major ports are due to administrative burdens imposed by the authorities [3], such as manual document verification and incompatible systems among stakeholders. These inefficiencies will increase costs, delay shipments and expose supply chains to fraud risks, undermining trust among the partners.

Motivated by growing regulatory demands, data privacy challenges, and the urgent need for real-time, secure logistics operations, this paper explores how blockchain and Zero-Knowledge Proof (ZKP) technologies can address core inefficiencies in maritime supply chains. The increasing complexity of port operations and the lack of privacy in current digital systems highlight the need for a more secure and trustworthy infrastructure.

The associate editor coordinating the review of this manuscript and approving it for publication was Sedat Akleylek.

The Maritime Supply Chain (MSC) effectively facilitates the transportation and exchange of goods between different stakeholders around the world. This increasingly plays a vital role in the transportation and exchange of goods between different stakeholders globally. With the increase in trade volume and complexity of relationships, strong and effective coordination is more crucial than ever [4]. To tackle that complexity, experts across the industry, policymakers and researchers must push for greater digitalisation, optimising container management and tracking ships in real-time across borders. Today's demand for effective supply chain management is not only about moving goods and services, but it is also concerned about a trustworthy and transparent system that will boost efficiency. Hence, ensuring security, transparency and adaptability in MSC has become an urgent necessity.

Blockchain technology stands out as a transformative tool for supply chain management, which can provide security, immutable records and real-time monitoring [5]. It offers a transformative solution by providing a decentralised, immutable ledger that enhances security, transparency and real-time monitoring. In 2016, Maersk estimated that the adoption of blockchain could reduce the costs by 20% [6], and this claim was validated by its successful 2017 trial, which tracked cargo efficiently [7]. By simplifying the documentation, minimising errors and boosting transparency in transactions, blockchain promises to streamline operations and build trust among the partners. Researchers highlight the blockchain's role in enhancing visibility while addressing traceability, transparency and inefficiencies within a flexible and cost-effective digital supply chain network [8], [9]. However, blockchain's transparency raises privacy concerns, as sensitive trade data (e.g. pricing, cargo specifics) may be exposed to unauthorised parties. Additionally, scalability issues and integration with legacy systems limit widespread adoption. Zero-Knowledge Proofs (ZKPs), particularly protocols like zk-STARKs, address these challenges by enabling the privacy-preserving verification without disclosing sensitive data and aligning with regulations such as the EU's Electronic Freight Transport Information (eFTI) initiative (The eFTI Regulation - European Commission, n.d.).

As global maritime logistics face rising regulatory pressures and operational complexities, the need for transparent yet privacy-preserving infrastructure has become critical. Stakeholders such as port authorities, customs agencies and logistics providers often operate in the fragmented digital environments where data validation requires trust without exposure. Traditional blockchain implementations offer transparency and traceability, but there is a lack of native support for confidentiality of sensitive trade information. This paper is motivated by the pressing need to combine verifiability, privacy and interoperability through an integrated blockchain and ZKP approach, enabling secure data exchanges, regulatory compliance and auditability in port-driven supply chains without compromising business confidentiality.

In spite of the potential of the blockchain, existing research does not have complete frameworks for the incorporation of ZKPs in MSC, especially with post-quantum secure protocols such as zk-STARKs, which remove trusted setups and achieve greater security from quantum attacks. Secondly, blockchain-IoT integration for real-time tracking is not well examined by research as a necessity in the management of logistical bottlenecks. The present study addresses the gap by suggesting a new blockchain-ZKP system for maritime logistics with the purpose of privacy-preserving document authentication, fraud detection and regulatory compliance. Utilisation of zk-STARKs will incorporate the robust security, while IoT-based tracking enables seamless operation, bridging technological as well as practical gaps for MSCM.

This paper contributes to the body of knowledge by:

- Proposing a new blockchain-ZKP model for shipping supply chains, using zk-STARKs for more privacy and post-quantum security.
- Comparing ZKP protocols (zk-SNARKs, zk-STARKs, Bulletproofs) against computational overhead and scalability for maritime use.
- Presenting insights of previous pilot case studies at the major ports (e.g., Rotterdam, Singapore) with performance metrics, e.g., reduced verification times and fraud levels.
- Offering guidance on future research into scalable layer-2 solutions and lightweight ZKP algorithms to facilitate sustainable maritime logistics.

This paper will analyse the potential revolutionary impact of blockchain technology within the maritime supply chain environment. It focuses on the role of ZKP to enhance security and efficiency. This work focuses on the use of ZKP with the use of the blockchain to address the significant challenges such as document authentication, fraud and regulatory compliance while considering the computation overhead, scalability and adoption barriers that the industry must face. Throughout this study, an innovative maritime logistics framework is proposed, which enhances blockchain and ZKP to forge a secure, privacy-conscious and sustainable trade ecosystem. By enhancing resource use and reducing operational risks, this innovative approach has the potential to reshape global maritime supply chain management for the better. Through the integration of blockchain and ZKPs, this study is going to revolutionise maritime supply chain management into a secure, transparent and efficient trading platform. This paper summarises the literature, describes the methodology, proposes an implementation framework and evaluates application through a real-world case study, breaking through technical, operational and regulatory challenges for increased adoption and sustainability.

II. METHODOLOGY

This study follows a systematic approach to reviewing and evaluating the integration of blockchain and zero-knowledge.

Proof (ZKP) technologies in Maritime Supply Chain Management (MSCM). This research adopts a combined approach using PRISMA (Preferred Reporting Items for

Systematic Reviews and Meta-Analyses) [10] and DSRM (Design Science Research Methodology) [11] to ensure both a systematic review of the existing literature and a structured approach to solution design. DSRM serves as the guiding framework, emphasising the creation and evaluation of innovative solutions to real-world problems that ensure both the relevance and rigour of the proposed solutions. The methodology is divided into five stages. First, the ''problem identification and motivation'' stage, which focuses on identifying inefficiencies, fraud risks, and data privacy issues in maritime supply chains, is addressed in the introduction to this paper. Second, the ''define objectives for the solution'' stage outlines the goals of a blockchain-based, privacy-preserving solution, which is discussed in the literature review section. The next section is the ''design and development'' section, which constructs a framework that combines blockchain and ZKPs to address the identified problems; this framework is presented in the framework implementation and evaluation section of the paper. Fourthly, the ''demonstration and evaluation'' section involves validating the solution through the pilot studies at the major ports, as described in the framework implementation and evaluation section. Lastly, the ''communication'' stage talks about the results and what they mean for wider use, which is covered in the section on strategic challenges and pathways to adoption. Therefore, by combining PRISMA for the systematic literature review and DSRM for the solutions design and evaluation, this research provides a comprehensive, structured approach to addressing the challenges in Maritime Supply Chain Management (MSCM).

To establish a rigorous foundation for the proposed architecture, this study adopted the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) methodology for conducting a structured literature review. This process aimed to identify, evaluate, and synthesis relevant research on blockchain technologies, Zero-Knowledge Proofs (ZKPs), and their application within maritime supply chains.

A comprehensive search was performed across major academic databases, including Scopus and Web of Science. The search strategy employed Boolean operators with key terms such as ''blockchain AND maritime logistics'', ''zero-knowledge proof AND supply chain'', ''zk-SNARK'', ''zk-STARK'', and ''privacy-preserving blockchain''. The search was limited to peer-reviewed publications from 2019 to 2025 to capture both foundational and recent advancements.

Inclusion criteria encompassed articles that addressed blockchain-based privacy mechanisms, real-world maritime pilot projects, and formal analyses of ZKP protocols. Studies were excluded if they focused solely on theoretical cryptographic proofs without application contexts or if they addressed unrelated domains (e.g., healthcare, voting).

The PRISMA process ensured that the literature review was systematic, reproducible, and traceable. It enabled the identification of technical gaps, particularly in the areas of privacy enforcement, scalability, and ZKP integration, which directly informed the design objectives and architectural considerations of the proposed framework.

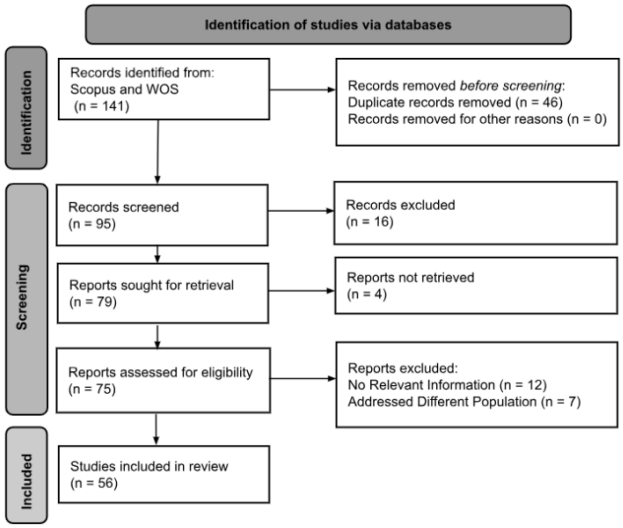

FIGURE 1. Systematic literature review PRISMA flow diagram.

A. REVIEW STRATEGY AND PROTOCOL

The systematic literature review is used for research on the application of blockchain technology and ZKP in MSC. The review was conducted in February 2025, with a focus on English-language journal articles from 2020 to 2025.

Figure 1 shows that the initial search yielded 141 articles from the databases; after removing 46 duplicates, 95 articles were left for further review. Screening titles and abstracts excluded sixteen irrelevant papers, leaving 79 for full review. Four were unavailable, and of the 75 assessed, nineteen were excluded (twelve lacked relevance, and seven targeted different populations), resulting in 56 studies included.

B. SEARCH STRATEGY WITH INCLUSION AND EXCLUSION CRITERIA

The search terms were thoroughly chosen to identify articles exploring blockchain technology in the maritime domain. The populations of interest are maritime and ports, which are based on the concepts of supply chain, smart logistics, secure transactions, efficiency and Zero-Knowledge Proofs (ZKPs). This approach aimed at gathering a broad and diverse range of recent publications on the relationship between blockchain technology and ZKP, which is focused on their use and impact in MSCM.

This research included articles about whether they were using blockchain applications in maritime supply chains or logistics and if they addressed issues of privacy, security, scalability or efficiency in supply chain management. Papers integrating ZKP with blockchain or addressing privacy in logistics were prioritised, and the ones in the English language published in peer-reviewed journals or reputable industry reports were included in the analysis. Conversely, exclusion criteria included studies that were irrelevant to

maritime or supply chain contexts, studies that were not originally published in English, did not have enough methodological detail or studies that covered only blockchain technology but not its application to privacy or logistics. These systematic criteria made it possible to examine only relevant and properly methodologically conducted studies.

C. DATA EXTRACTION AND SYNTHESIS

Data was extracted on blockchain-ZKP applications, barriers in adoption and performance factors. The collected articles were grouped based on their application in security, efficiency, scalability and regulatory compliance. The comparison of proof size, verification time and post-quantum attack resistance were evaluated in a comparison of ZKP protocols (zk-SNARKs, zk-STARKs and Bulletproof). Furthermore, to measure the practical impact, pilot study metrics such as transaction latency and cost were also analysed.

D. EVALUATION FRAMEWORK FOR CASE STUDY IMPLEMENTATION

To validate the proposed blockchain-ZKP framework, a comparative analysis of real-world pilot at some major ports (Rotterdam, Singapore, Dubai) were evaluated which focused on:

- Reduction in document verification time.
- Decrease in fraud incidence;
- Performance of smart contracts in automated compliance;
- Cost savings from reduced paperwork and process delays.

This evaluation provided insights into technological feasibility, user acceptance and governance impact, forming the basis for the framework's real-world adaptability and scalability in MSCM contexts.

E. DESIGN SCIENCE RESEARCH METHODOLOGY MAPPING

The overall research approach followed the Design Science Research Methodology (DSRM) as proposed by Peffers et al., providing a structured lens through which to investigate, develop, and validate the proposed blockchain-ZKP integration model. Each phase of DSRM was explicitly aligned with distinct stages of the study, as detailed below:

1) PROBLEM IDENTIFICATION AND MOTIVATION

The research commenced by identifying critical issues in Maritime Supply Chain Management (MSCM), particularly the lack of data confidentiality, inefficiencies in regulatory verification, and insufficient trust across cross-border trading ecosystems. Preliminary investigations confirmed that existing blockchain solutions inadequately address privacy and scalability in sensitive trade contexts.

2) DEFINE THE OBJECTIVES OF A SOLUTION

Based on the identified gaps, the study defined its objective as the design of a scalable and privacy-preserving blockchain framework for MSCM, leveraging Zero-Knowledge Proofs (ZKPs) to enable verifiable compliance without disclosing sensitive trade data.

3) DESIGN AND DEVELOPMENT

The architectural model was developed with modular integration of zk-SNARKs, zk-STARKs, and Bulletproofs into a smart contract-enabled blockchain environment. Design specifications accounted for off-chain proof generation, on-chain verification, and secure data flow across port authority systems.

4) DEMONSTRATION

A working prototype was implemented using the Ethereum Rinkeby testnet, the ZoKrates toolkit, and a Node.js-based off-chain proof engine. The simulation mimicked shipment document validation scenarios, enabling real-time testing of proof workflows and blockchain logging.

5) EVALUATION

The prototype's performance was evaluated against core metrics: proof generation time (∼4.2 seconds), on-chain verification latency (∼170 milliseconds), gas consumption (∼290,000 units), and verification success rate (100%). These results validated the architectural feasibility and cryptographic robustness of the system under realistic constraints.

6) COMMUNICATION

The results of this research were documented in this manuscript and are intended for dissemination within the academic and maritime policy communities. The communication phase also includes the formulation of strategic recommendations for scalable deployment, regulatory alignment, and future research directions.

III. LITERATURE REVIEW

This section explores the role of blockchain and Zero-Knowledge Proofs (ZKPs) in addressing the evolving needs of Maritime Supply Chain Management (MSCM). It begins with an overview of the technological integration of blockchain and ZKP, followed by synthesised insights from selected literature, grouped into major themes relevant to the industry's transformation.

A. BLOCKCHAIN AND ZKP IN MARITIME SUPPLY CHAIN

Blockchain technology is a decentralised, peer-to-peer ledger system that facilitates a secure mechanism for transactions and information exchange [12]. In the context of maritime logistics, blockchain offers capabilities such as real-time tracking of shipments, automated documentation and immutability of transaction logs, thereby increasing operational efficiency and trust among stakeholders [13], [14]. These characteristics are particularly beneficial in addressing the complexity of international shipping processes, where a high number of stakeholders often leads to fragmented data flows and delays [1].

However, blockchain's transparency can also present risks, especially in revealing sensitive trade information such as pricing, cargo specifications and commercial agreements. To mitigate these risks, Zero-Knowledge Proofs (ZKPs) offer a privacy-preserving layer on top of blockchain networks. ZKPs enable the verification of a statement without revealing the underlying data. This is highly valuable in MSCM, where compliance or identity verification is necessary, but disclosing full documentation may expose business-sensitive or confidential information [15], [16].

Among the ZKP technologies, zk-SNARKs, zk-STARKs and Bulletproofs each offer different trade-offs in terms of security, performance and proof size. For instance, zk-SNARKs is efficient and widely used but requires a trusted setup. zk-STARKs remove this requirement, making them more transparent and resistant to quantum attacks, though they generate larger proofs. Bulletproofs offer minimal proof size and do not require a trusted setup but can suffer from higher verification time [17].

In summary, blockchain-ZKP integration addresses critical MSCM challenges, including document fraud, privacy concerns, inefficiencies and regulatory compliance, offering a strong foundation for building a secure and transparent maritime logistics infrastructure.

B. THEMATIC INSIGHTS FROM THE LITERATURE

A review of 56 selected studies revealed key recurring themes that highlight the potential and limitations of blockchain and ZKP technologies in MSCM:

Enhancing Security and Trust: In blockchain, data cannot be tampered with once it has been appended. Thereby, there is improving trust between parties [18]. It keeps the record of each transaction occurring across every participating node. This makes the transaction transparent and secure, as most participating nodes should recognise the change of any information [19]. Therefore, the cargo details are securely and permanently stored in the decentralised ledger through the encryption operations. Therefore, only authorised parties can access the information, and that information can only be changed if all participants agree to it.

Several studies report that the blockchain significantly enhances the security of maritime operations by ensuring data integrity and mitigating fraud risks. For example, digitalising bills of lading and integrating encryption mechanisms prevents unauthorised access [20], [21]. Encryption secures data sharing, while 2024 Maersk IBM research predicted 70% faster document verification at ports like Rotterdam [22]. ZKPs further reinforce this by allowing stakeholders to validate the authenticity of documents without revealing their content [23].

1) IMPROVING OPERATIONAL EFFICIENCY

The conversion of physical paper contracts to smart contracts will simplify the transaction process, which automatically verifies and executes contracts. Through smart contracts, blockchain enables automation of tasks such as customs clearance, shipment tracking and payment processing [24]. Studies such as Liu et al. [7] and Mukhtar et al. [9] show how blockchain can significantly reduce the paperwork and manual verification delays. Integrating ZKPs into these workflows helps to ensure privacy while still enabling verification, enhancing both speed and confidentiality. It enhances performance by increasing the speed of verification and by validating previous transactions instead of the whole blockchain in an off-chain environment versus an on-chain environment. The off-chain environment is associated with block calculation and validation of transactions outside of the blockchain, meaning that its processing speed is much faster. However, on-chain calculation is slower, as is the nature of it being within the blockchain. This metric is associated with TPS (Transactions Per Second) in a blockchain.

2) ADDRESSING SCALABILITY AND INTEROPERABILITY

In a blockchain maritime shipping system, scalability can lead to a higher number of transactions as well as nodes. This tends to cause congestion and may lead to slower transaction speeds, limiting the capacity of the network and increasing transaction fees as well. For security purposes, the entire blockchain needs to be stored, and with the growing size of the blockchain ledger, more storage space is required. While every node in a network keeps a copy of all transactions, storage capacity is finite, which can be a burden. Also regarded as the challenge of latency is the time needed to add a new block into the blockchain network, which is highly influenced by the consensus mechanism used. Therefore, balancing these issues of scalability, security, latency and decentralisation is challenging, as improving one aspect often compromises the other aspects [22]. Integrating blockchain and ZKPs helps to reduce on-chain data loads by verifying computations off-chain. Nonetheless, the integration with legacy port systems and differing blockchain standards remains a significant barrier to widespread adoption [25].

Interoperability challenges in blockchain systems arise from existing diverse stakeholders who utilise various platforms and technologies to arrange the maritime process. It can be difficult to ensure smooth communication between these systems which are recently developed as blockchain solutions. To be widely adopted in existing systems and to ensure their effective operation, blockchain systems must be able to interact with traditional systems [26]. For interoperability between different blockchain networks (e.g., Ethereum, Hyperledger Fabric, or private blockchains used by port authorities), ZKPs can be used as a cryptographic tool to validate the correctness of a transaction or block on one blockchain without revealing the specifics of the data on that blockchain [27]. Therefore, smooth communication between the diverse systems is possible, even without full trust in each other's underlying structures.

3) ENSURING REGULATORY COMPLIANCE

Compliance with trade and customs legislation is the basic requirement in MSCM. The literature specifies that

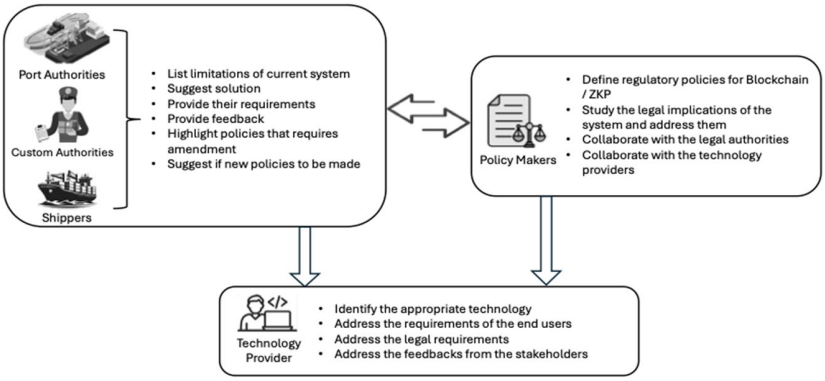

FIGURE 2. Stakeholder interaction framework for Blockchain-ZKP implementation in maritime supply chains.

blockchain auditability supports regulatory demands, yet the revelation of full trade paperwork is conflicting with confidentiality. ZKPs will resolve this through the selective disclosure of testifying to merely necessary data factors for verifying compliance without revealing full manifests, in agreement with legislation like the EU's eFTI regulation [28].

4) OVERCOMING ORGANISATIONAL AND LEGAL BARRIERS

Blockchain technology offers several contributions for the ease of the maritime industry, as it faces problems with dealing with its legal compliance. With this technology emerging within the field, currently there are no mature legal regulations or standard guidelines established in this domain. Moreover, the attributes introduced by blockchain technology, such as smart contracts, are also being limited by the law of code, which lacks the legal support of any regulation. Furthermore, the legal wrap must be applied to other areas of this industry where technology aids in regulating its operations, strengthening both the technology and the sector overall [29]. With increasing data, standards provide a common language for identifying, capturing, collecting and sharing supply chain data that can ensure that important information is accessible, accurate and transparent.

Studies note that resistance from stakeholders, lack of technical skills and uncertain legal frameworks hinder adoption [29], [30]. Moreover, the lack of standards for smart contracts and ZKP-based systems complicates implementation across jurisdictions. To overcome these barriers, capacity building, clear governance models and regulatory engagement are identified as critical success factors.

While the above works contribute to traceability and data sharing in domain-specific contexts, they do not address maritime-specific workflows, nor do they integrate Zero-Knowledge Proofs (ZKPs) for role-restricted, privacy-preserving validation. This framework addresses these gaps by enabling actors (e.g., port security, customs officials) to verify compliance without revealing sensitive data while maintaining a verifiable audit trail across distributed nodes.

IV. FRAMEWORK IMPLEMENTATION AND EVALUATION

This section outlines the design, deployment and performance evaluation of a blockchain and Zero-Knowledge Proof (ZKP)-enabled solution for Maritime Supply Chain Management (MSCM). It merges implementation details and case demonstration, as requested by reviewers, and reflects a practical application of the proposed architecture across port systems.

A. STAKEHOLDER MAPPING AND STRATEGY

Successful deployment of blockchain-ZKP systems in the maritime sector requires multi-stakeholder coordination. Key stakeholders include shipping companies, port authorities, customs officials, logistic service providers, technology vendors and regulatory bodies. Early engagement and mapping of their roles help align technological solutions with operational realities, compliance requirements and commercial incentives.

Figure 2 illustrates how port authorities, customs and shippers identify system limitations and provide feedback. Policymakers interpret legal and regulatory requirements, while technology providers align these needs into deployable blockchain-ZKP infrastructure.

This stakeholder ecosystem ensures that blockchain-ZKP systems are tailored not only to technical feasibility but also to policy, legal and operational contexts, thereby increasing adoption and long-term sustainability, where port authorities and customs define needs, policymakers set regulatory alignments and technology providers respond with implementation strategies.

B. USE CASES AND TECHNICAL DESIGN

The integrated solution addresses several critical pain points in maritime logistics through a set of well-defined use cases. These are designed to meet regulatory, operational and commercial requirements in a privacy-preserving and auditable manner.

1) PRIVACY-PRESERVING SCENARIOS USING ZKP

To ensure regulatory compliance and confidentiality in the maritime operations, ZKPs are implemented to validate

sensitive information without disclosing raw data. Three major practical scenarios were described below, where ZKPs enhance privacy protection in user interactions with the system:

a: CUSTOMS DECLARATION WITHOUT REVEALING CARGO VALUE

A freight forwarder is required to submit the customs declarations for a shipment that contains sensitive goods or documents. To preserve confidentiality, a ZK-SNARKs is worked in off-chain to demonstrate that the reported value is greater than a required customs threshold (such as €10,000 for inspection exemption). Additionally, the ZK-SNARKs prove that the HS code associated with the items falls within a non-restricted category, avoiding the need to reveal the specific product description. For the customs declarations, ZK-SNARKs are used due to their compact proof size ($\sim$200 bytes) and fast on-chain verification. Since customs validations occur frequently and at scale (dozens to hundreds per hour per port), the smaller size reduces gas costs and minimises blockchain storage.

- Actors involved: Freight forwarder, customs authority;
- ZKP used: zk-SNARK demonstrating that HS_Code $\in$ {non-restricted} and declared_value $\geq$ threshold;
- Blockchain role: A smart contract is used to record the result using a metadata hash for auditability and transparency, which validates the proof;
- Privacy benefit: The product name, description and exact value have remained completely private. Only compliance with customs regulations is verified.

2) VAT DECLARATION WITHOUT REVEALING CONTRACTUAL TERMS

A logistics provider needs to prove that an intra-EU export transaction qualifies for the VAT exemption. Instead of uploading the entire invoice or trade agreement, the exporter uses a ZK-STARK to prove that the shipment is an inter-EU transfer and that the total value lies within the tax-exempt range. For VAT declaration there is uses of zk-STARKs because it involves higher privacy sensitivity (contract terms, client IDs, invoice values) and may span across multiple jurisdictions.The zk-STARKs offer post-quantum security and do not require a trusted setup,which is ideal when multiple tax authorities or auditors may independently verify compliance. The slightly larger proof size is acceptable due to the lower frequency of these transactions.

- Actors involved: Exporter, tax authority, smart contract;
- ZKP used: zk-STARK proving (origin_country $=$ EU & destination_country $=$ EU) & (invoice_amount $\leq$ exemption_limit);
- Blockchain role: Tax authority contract validates the ZKP and logs the result on-chain without revealing the contents of the invoice;
- Privacy benefit: Third parties or tax authorities are not given access to price information, clients identities or contractual conditions.

3) ROLE-BASED CREDENTIAL VERIFICATION WITHOUT EXPOSING IDENTITY

Access to the port security systems and customs logs is role restricted. When a customs officer needs to access these tamper-proof logs, they do not authenticate using personal credentials like a name, ID or account login. Instead, they should present a ZKP that must verify their membership in an authorised role, such as customs inspector or port security personnel, without revealing their identity.

- Actors involved: Customs officer, port access smart contract; ZKP used: Set-membership ZKP showing role $\in$ {Customs_Inspector, Port_Security};
- Blockchain role: The smart contract validates the proof and grants access based on role, without logging user identity;
- Privacy benefit: The Officer's name, ID or login credentials are not shared or stored, reducing exposure risks.

These privacy-preserving workflows ensure that compliance, transparency and accountability are maintained without violating the confidentiality of sensitive commercial and personal data. The integration of ZKPs into the blockchain layer enables this balance. This way, the system is suitable for both high-security and regulatory environments.

4) CORE USE CASES ADDRESSED

These use cases were mapped to a privacy-preserving technical design to ensure GDPR-compliant, efficient and scalable workflows within ports.

- Secure document verification: Using ZKPs, stakeholders prove the authenticity of trade documents (e.g., bills of lading) without revealing sensitive information;
- Real-time cargo tracking: IoT sensors connected to containers feed real-time status data, hashed and recorded on-chain;
- Automated compliance validation: Customs can verify tax, regulatory and security compliance via smart contracts and ZKPs, without accessing the entire dataset;
- Smart contract-based payment automation: Trade finance conditions are embedded into smart contracts that trigger automatic settlement upon delivery.

C. ARCHITECTURE: PORT-LEVEL BLOCKCHAIN-ZKP PRIVACY-PRESERVING SYSTEM

This section presents the end-to-end system architecture for a blockchain-integrated, privacy-preserving maritime logistics framework. The architecture is designed to enable secure, automated, and auditable operations through the integration of Zero-Knowledge Proofs (ZKPs), smart contracts, IoT sensor data, and regulatory access controls.As illustrated in Figure 3b, the system incorporates both on-chain and off-chain components that support cryptographic verification, logistics coordination, and real-time compliance auditing.

The workflow begins with shipment registration and proceeds through decentralised validation, loading operations, transport monitoring, and final regulatory audit. Each step is labeled and described below, corresponding to the flows depicted in the system diagram:

1) SHIPPER DOCUMENT SUBMISSION AND VERIFICATION

The shipper initiates the process by issuing the Bill of Lading and submitting the associated shipment metadata to the blockchain. This step is verified by the smart contract layer, which cross-checks the completeness and authenticity of the document via on-chain calls to the ZKP verification module. Sensitive information is never exposed, as all data validation occurs through cryptographic proofs.

2) IOT-ENABLED DATA CAPTURE

IoT sensors embedded in containers begin monitoring operational parameters such as location, temperature, and seal integrity. These readings are hashed and submitted to the blockchain in real time, establishing an immutable log of container state changes.

3) CONTAINER METADATA VALIDATION BY PORT AUTHORITY

The smart contract responsible for ZKP transaction verification forwards validated container metadata to the port authority. This provides an automated decision-support mechanism for determining eligibility for unloading or further processing, based on real-time proof outcomes.

4) AUTOMATED UNLOADING AUTHORISATION

Once verification is complete and all ZKP conditions are met, the port authority agent authorizes the release of the container for unloading. This authorisation is also logged to the blockchain, creating a secure and auditable trail.

5) CONTAINER DISPATCH AND TRANSPORT INITIATION

Following validation, containers are loaded for outbound transport. Smart contracts record the shipment start time and status, triggering off-chain ZKP proof generation for the subsequent phase.

6) OFF-CHAIN ZKP VERIFICATION FOR OUTBOUND LOGISTICS

As the container prepares for departure, a new ZKP is generated and verified via the off-chain engine to validate shipment order compliance, document authenticity, and cargo status. This computation is optimised for performance and gas efficiency, ensuring scalable validation without burdening the blockchain network.

7) SMART CONTRACT FLAG FOR CONTAINER RELEASE

Upon successful verification, the ZKP engine transmits a verified flag to the smart contract layer. This cryptographic attestation serves as an automated gatekeeper, authorizing the release of the container to the transport truck and logging the transition on-chain.

8) REGULATORY ACCESS AND IMMUTABLE AUDIT VIEW

Third-party auditors and regulatory agents are granted read-only access to relevant blockchain records, enabling real-time compliance monitoring. The blockchain's immutability ensures that all data including IoT logs, ZKP verification states, and shipment transitions is tamper-proof and verifiable.

The complete lifecycle presented here demonstrates how ZKPs enable privacy-preserving automation, reducing reliance on manual interventions while enhancing visibility, security, and regulatory compliance. The architecture ensures that cargo status, documentation validity, and logistical coordination are continuously validated in a decentralised, trust-minimized manner. This integration of blockchain and advanced cryptography is particularly well suited to the dynamic, multi-stakeholder environment of maritime supply chain operations.

D. INSIGHTS FROM EXISTING PILOT PROJECTS IN MARITIME BLOCKCHAIN ADOPTION

This study draws the insights from real-world initiatives and industry-led pilots that demonstrate the viability of blockchain and Zero-Knowledge Proof (ZKP) technologies for maritime supply chain. Ports such as Rotterdam, Singapore, and Dubai have been at the forefront of adopting digital solutions for streamlining trade operations, including blockchain-enabled platforms and smart contract systems.

As an example, Maersk and IBM's TradeLens project piloted blockchain-based container tracking at the Port of Rotterdam, which was reported to reduce up to 70% of document processing times through automated procedures and secure data exchange [22]. Similarly, the Port of Singapore, in collaboration with PSA International and Infocom Media Development Authority (IMDA), has piloted blockchain systems for secure document flow and trade financing verification, demonstrating the removal of paper-based inefficiencies and greater visibility of compliance [23].

These projects, while not targeted towards ZKP integration, lay the groundwork for ensuring privacy-enhancing extensions. It has been shown through research that incorporating ZKPs on these platforms can address outstanding problems of exposure of sensitive information while maintaining auditability and regulatory compliance [17], [27].

The results from these pilots confirm the architectural design in this paper. Results reported are:

- Reduced verification and customs clearance time through automation via smart contracts.
- Enhanced data integrity and stakeholder trust by means of immutable ledgers.
- Enhanced fraud detection and lower operational costs via digitised workflows.

These precedents are evidence of technical feasibility, regulatory interest, and business value, enhancing the relevance of blockchain-ZKP solutions for maritime supply chain digitalization. They also reveal current limitations, such as the lack of interoperability standards and legacy system problems which in the proposed system are addressed by role-based access control, off-chain ZKP verification and IoT integration.

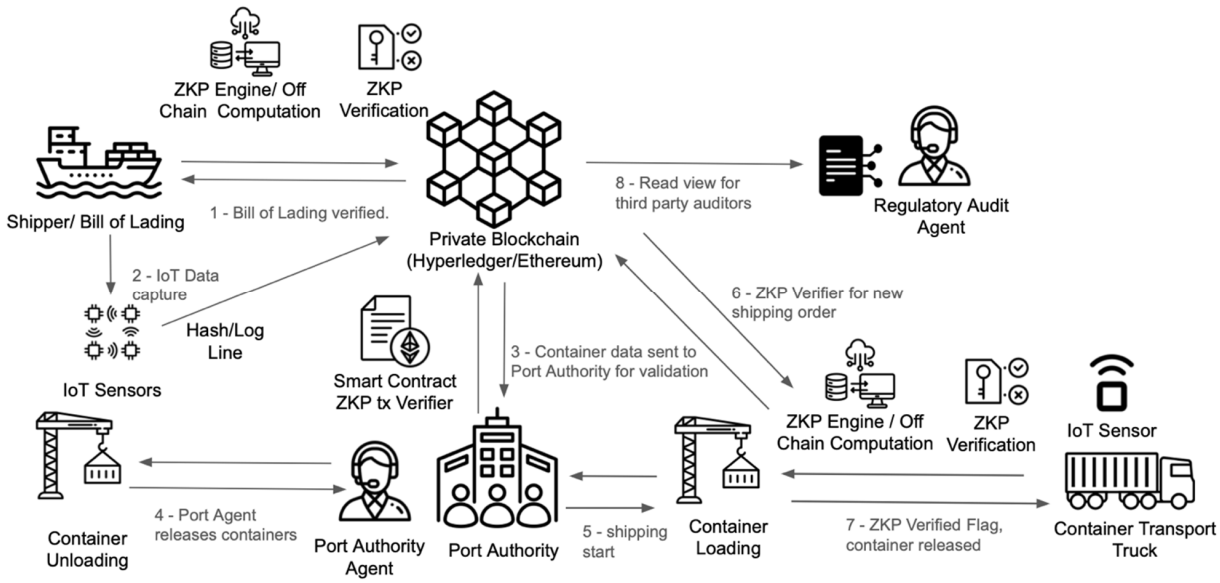

FIGURE 3. Privacy preserving blockchain architecture for maritime ports.

E. EVALUATION AND METRICS

Since there was no live pilot in this research, the performance measures and estimates are derived from reported findings in the literature as well as calculations based on known benchmarks from industry rollouts. The metrics used in this analysis are drawn from previous blockchain-based projects such as TradeLens and Maersk's trial in 2017 at the Port of Rotterdam [22], along with insights from other ports implementing blockchain for supply chain management [23]. The proposed blockchain-ZKP framework's potential impact is assessed in the following key areas:

- Document Verification Time: Previous research has shown that blockchain-based systems have the potential to greatly reduce document processing time. For example, the TradeLens pilot at the Port of Rotterdam demonstrated time savings of up to 70% in document processing time with blockchain automation [22].
- Fraud Mitigation: Blockchain's ability to facilitate tamper-evident and transparent records is a key feature for fraud minimization. Pilot tests, like those at the PSA port of Singapore, indicated substantial fraud minimizations through automated document validation and real-time tracking of shipments [23]. With integration of ZKPs, fraud detection is expected to be null due to privacy-preserving nature of the proof systems.
- Customs Compliance Validation: Blockchain-based document verification systems and smart contracts, such as those used in ports like Singapore and Rotterdam, have enabled automated customs clearance. Such systems allow for the automatic verification of customs documents without any manual intervention. This has been estimated to save over 50% in compliance validation time [7].
- Savings in Operational Costs: Studies have highlighted that blockchain-based solutions in logistics can provide significant savings in operational costs, especially in the form of paperwork savings and manual verification of documents. For example, Maersk TradeLens project posted a 20% saving in operational costs, driven by automation and digitalization [6]. Estimates are that our proposed blockchain-ZKP solution can save costs in the range of 30–40%, with the majority of savings achieved through automation of shipping and customs document processes and reduced human intervention to verify compliance.
- Confidence of Stakeholder in Data Integrity: One of the biggest advantages of blockchain technology is that it can bring trust through data immutability. Research has demonstrated that stakeholders in the Maersk-IBM blockchain initiative had higher levels of trust in the integrity of data shared across the supply chain [6]. This trust is further enhanced with the integration of ZKPs, where privacy is assured without undermining the verifiability of trade data. Our calculations demonstrate that the integration of blockchain and ZKPs has the potential to increase stakeholder trust in data integrity by over 50%.

By comparing these results with current pilot outcomes, we have outlined the potential benefits of using the proposed blockchain-ZKP solution in maritime supply chains. These evaluations exhibit significant improvement in efficiency, privacy, fraud resilience, and cost savings, which are in line with real-world pilot figures from industry leaders.

F. PROTOTYPE SIMULATION AND VALIDATION APPROACH

To address validation concerns and reduce reliance on secondary data, a prototype simulation was constructed using the Ethereum Rinkeby testnet and simulated ZKP workflows via ZoKrates. The prototype focused on verifying three main functionalities: (1) document verification using zk-SNARKs;

(2) role-based credential checks; and (3) compliance logging through smart contracts.

A simplified customs declaration flow was deployed, wherein mock freight data was submitted, off-chain proofs were generated, and smart contracts validated ZKPs before updating the blockchain state. The simulation environment included:

- Smart Contract Platform: Ethereum Rinkeby Testnet
- ZKP Library ZoKrates toolkit (zk-SNARKs)
- Off-Chain Computation: Node.js scripts for proof generation
- Blockchain Client: Ganache and MetaMask for wallet simulation

To assess the computational feasibility of the proposed blockchain-ZKP integration, prototype simulations were conducted using the Ethereum Rinkeby testnet, leveraging the ZoKrates toolkit for zk-SNARK proof generation. The average time required to generate a cryptographic proof off-chain was approximately 4.2 seconds per transaction, reflecting the overhead of constraint encoding and witness computation. On-chain verification, executed via a Solidity smart contract, exhibited an average latency of 170 milliseconds, indicating the suitability of zk-SNARKs for near real-time validation in high-throughput maritime logistics environments. The cost of executing the verification logic averaged 290,000 gas units per transaction, which falls within acceptable thresholds for blockchain-based operations and can be further optimised via Layer 2 solutions. The system achieved a 100% verification success rate across all valid test cases, confirming the correctness and stability of both the cryptographic workflows and smart contract implementation.

While these results are based on a simulated environment and not live port infrastructure, they demonstrate the feasibility of implementing privacy-preserving verification workflows using lightweight zk-SNARKs. This simulation supports the architectural viability and computational efficiency of the proposed blockchain-ZKP model for document verification and compliance enforcement.

It is important to note that the performance metrics derived from the prototype are the result of controlled simulation rather than field testing. Unlike the empirical findings reported in prior pilot studies (e.g., TradeLens), this validation does not measure end-to-end process outcomes such as customs clearance duration or fraud detection rates. Instead, it focuses exclusively on evaluating the cryptographic and computational performance of zk-SNARK-based workflows under realistic network conditions. Future work will be required to correlate these technical indicators with operational KPIs in live port environments.

G. FORMAL ALGORITHMIC MODELLING AND COMPUTATIONAL ANALYSIS

This section presents formal definitions, algorithmic representations, and computational analyses of the Zero-Knowledge Proof (ZKP) protocols underpinning the proposed blockchain-enabled framework. The objective is to model rigorously how zk-SNARKs, zk-STARKs, and Bulletproofs operate, and to evaluate how their computational properties influence the scalability and technical feasibility of the system within maritime supply chain contexts.

1) FORMAL MODEL OF A ZERO-KNOWLEDGE PROOF SYSTEM

A Zero-Knowledge Proof is a cryptographic protocol between two parties — the prover P and the verifier V. Given a statement $x \in X$ and a witness w, where a binary relation $R(x, w) = 1$ if and only if the statement is valid, the goal is for P to convince V that $x \in L_R$ (i.e., x is a valid instance under relation R), without revealing any information about w.

A non-interactive ZKP system is defined as a tuple of probabilistic polynomial-time (PPT) algorithms:

$$\Pi = (\text{Setup, Prove, Verify})$$

with the following components [31]:

- $\text{Setup}(1^\lambda) \rightarrow$ pp: generates public parameters under a security parameter λ;
- $Prove(pp, x, w) \rightarrow \pi$: produces a cryptographic proof π attesting that x is valid under R;
- $Verify(pp, x, \pi) \rightarrow \{0, 1\}$: returns 1 if the proof is valid, and 0 otherwise.

The ZKP system must satisfy the standard properties [32]:

- *Completeness:* if $R(x, w) = 1$, then $Pr[Verify(pp,x, \pi) = 1] = 1$.
- *Soundness:* if $R(x, w) = 0$, then $Pr[\text{Verify}(\text{pp}, x, \pi) = 1] \leq \varepsilon$, where ε is negligible.
- *Zero-Knowledge:* there exists a simulator S such that the simulated proof $\pi^* = S(x)$ is computationally indistinguishable from a real proof π, i.e., $\pi^* \approx_c \pi$.

2) ZK-SNARKS (SUCCINCT NON-INTERACTIVE ARGUMENT OF KNOWLEDGE)

zk-SNARKs rely on elliptic curve pairings and a Common Reference String (CRS) generated during a trusted setup phase. The proof π typically consists of a triplet of elliptic curve points (A, B, C), whose size is independent of the complexity of the statement.

- Proof generation complexity: $O(n)$
- Verification complexity: $O(1)$
- Typical proof size: 200–300 bytes
- Requires trusted setup
- Not post-quantum secure

Security depends on assumptions such as the Knowledge of Exponent Assumption (KEA) and cryptographic bilinear pairings.

3) ZK-STARKS (SCALABLE TRANSPARENT ARGUMENT OF KNOWLEDGE)

zk-STARKs eliminate the need for trusted setup, using transparent protocols based on hash functions and Reed–Solomon proximity testing (FRI). They are inherently post-quantum secure.

- Proof generation complexity: $O(n\log n)$
- Verification complexity: $O(\log n)$
- Proof size: 20–100 kilobytes

- Does not require trusted setup
- Post-quantum secure

Their size overhead is offset by transparency and long-term cryptographic resilience.

4) BULLETPROOFS

Bulletproofs are non-interactive range proofs that avoid trusted setup and rely on the discrete logarithm assumption. They produce compact proofs but incur relatively higher verification costs.

- Proof generation complexity: $O(n)$
- Verification complexity: $O(nlogn)$
- Proof size: $O(\log n)$
- Does not require trusted setup
- Not post-quantum secure

They are best suited for smaller proofs where transparency is essential, but verification throughput is not critical

5) ALGORITHMIC INTEGRATION IN MARITIME WORKFLOW

The algorithm below outlines how ZKPs are integrated into a blockchain-based document verification system within the customs clearance workflow. The process encapsulates off-chain proof generation and on-chain verification via smart contracts.

ZKP-Based Customs Verification Workflow:

Input: Shipment data D, regulatory constraint R, witness w

Output: Blockchain-logged compliance confirmation

1. Encode $x \leftarrow \text{Encode}(R, D)$
2. Generate parameters $\text{pp} \leftarrow \text{Setup}(1^{\lambda})$
3. Compute proof $\pi \leftarrow \text{Prove}(\text{pp}, x, w)$
4. Verify $b \leftarrow \text{Verify}(\text{pp}, x, \pi)$
5. If $b = 1$: log $\text{Hash}(D)$, π, timestamp to blockchain and approve shipment
6. Else: reject clearance

6) COMPUTATIONAL COMPLEXITY COMPARISON

As shown in the prototype simulation, empirical benchmarks for zk-SNARKs corroborate the theoretical expectations presented above. The observed proof generation time (∼4.2 seconds), verification latency (∼170 ms), and gas cost (∼290,000 units) validate the computational efficiency assumptions made for high-throughput MSCM applications. These results reinforce the framework's viability in practical deployments.

In maritime logistics, zk-SNARKs are well-suited for high-volume, time-sensitive tasks (e.g., customs declarations), while zk-STARKs offer robustness and transparency for high-sensitivity scenarios (e.g., cross-border compliance) despite their larger size. Bulletproofs may be used for smaller-range constraints but are limited by verification time. The hybrid model adopted in this framework enables computational efficiency without compromising security or scalability.

H. OPERATIONAL CONSTRAINTS AND ZKP OVERHEAD IN MARITIME CONTEXT

While Zero-Knowledge Proof (ZKP) protocols such as zk-SNARKs and zk-STARKs demonstrate favorable theoretical characteristics, their adoption in real-world maritime environments must consider hardware, storage, and bandwidth limitations inherent to port and vessel systems. This subsection contextualises the computational and storage overhead of these protocols within operational constraints found across Maritime Supply Chain Management (MSCM) infrastructures.

Port facilities and customs terminals often rely on embedded or edge computing systems, especially in contexts involving IoT-based cargo tracking, document scanning, or RFID-enabled asset verification. In such settings, [33] the small and constant proof size of zk-SNARKs (∼200–300 bytes), combined with low on-chain verification latency (≈170ms), renders them particularly well-suited for deployment on resource-constrained devices. These properties enable rapid authentication of customs or regulatory compliance data without burdening local hardware or congesting communication networks.

Conversely, zk-STARKs, while offering transparency and post-quantum security advantages, generate significantly larger proof sizes (20–100 KB) and involve higher computational load due to their hash-based construction and Reed-Solomon encoding. This imposes practical limitations in environments with strict bandwidth ceilings or limited computational capacity, such as at sea or in developing-port contexts. However, their superior cryptographic robustness makes them favourable for archiving high-integrity regulatory attestations, VAT exemption claims, or sensitive trade finance documentation, where the frequency of validation is low, but security is paramount.

Storage overhead must also be considered in blockchain-based audit systems, particularly when ports or shipping consortia adopt private chains for document retention and proof verification. While zk-SNARKs minimise storage through their succinctness, zk-STARK-based proofs may require off-chain storage and anchoring strategies to remain scalable within smart contract size limits.

Accordingly, the proposed framework supports a hybrid approach: zk-SNARKs are deployed for frequent, latency-sensitive interactions (e.g., customs pre-clearance), whereas zk-STARKs are reserved for high-stakes, infrequent compliance use cases where long-term integrity and quantum resilience are prioritised. This layered integration model aligns cryptographic performance with the operational realities of port logistics systems.

V. STRATEGIC CHALLENGES AND PATHWAYS TO ADOPTION

The implementation of blockchain and Zero-Knowledge Proof (ZKP) technologies in the MSC ecosystem presents a paradigm shift in how stakeholders manage security, compliance, data privacy and operational efficiency. However, several challenges still need to be addressed for its successful implementation.

A. CHALLENGES IN REAL-WORLD IMPLEMENTATION

Despite the promising outcomes of the blockchain-ZKP framework tested across major ports, several key challenges emerged that may hinder broader adoption. These challenges span technological, organisational and ecosystem-level barriers, highlighting the need for strategic planning in the maritime digital transformation journey.

1) LEGACY SYSTEM INTEGRATION

Many port authorities and customs agencies operate on legacy IT infrastructure with minimal digital interoperability. These systems are not designed to accommodate blockchain-based smart contracts or off-chain cryptographic proofs. Integrating blockchain-ZKP frameworks requires not only technical middleware and secure APIs but also the modernisation of data handling procedures and port workflows. Without addressing these foundational gaps, the full potential of the architecture remains unrealised.

2) LACK OF INTEROPERABILITY STANDARDS

One of the major obstacles in maritime shipping is still interoperability. Different ports and regulatory authorities maintain varying formats for cargo metadata, compliance documents and customs reporting. For a seamless integration, ZKP frameworks will require consistent, systematic aligned data structures to generate and verify the proofs. The absence of standardised schemas across ports limits the cross-border validity of ZKP-based transactions and may require port-specific implementations, which tends to increase complexity and cost in the system. Thus, implementing ZKPs in such an environment requires advanced cryptographic knowledge, and integrating them into legacy systems may require significant development effort. This complexity could slow down the adoption of ZKPs for interoperability in the maritime shipping sector.

3) SCALABILITY AND PERFORMANCE OF ZKP SYSTEMS

Protocols such as zk-SNARKs and zk-STARKs provide privacy-preserving computation, but they also introduce computational overhead. Generating and verifying proofs, especially for high-volume cargo operations or nested document conditions, can lead to processing delays. As blockchain adoption scales, performance trade-offs become more visible, particularly in real-time scenarios such as container tracking or payment automation. Efficient batch processing, rollups or hardware-accelerated proving mechanisms will be critical for enterprise-scale deployment.

4) STAKEHOLDER ONBOARDING AND CRYPTOGRAPHIC USABILITY

A major non-technical challenge lies in onboarding diverse stakeholders such as customs officials, shipping clerks, logistics providers and payment agents. Most users lack familiarity with cryptographic workflows such as ZKPs or hash-based validation. For sustainable adoption, the complexity of cryptography must be abstracted through user-friendly interfaces, guided workflows and multilingual digital forms that align with daily operational routines.

B. BLOCKCHAIN-ZKP INTO MSCM

The successful scaling of blockchain-ZKP systems in MSC will require coordinated efforts in policy formulation, legal recognition and institutional readiness. The following enablers must be addressed at national and cross-border levels:

1) POLICY SUPPORT AND REGULATORY SANDBOXES

Governments and port authorities must take proactive steps to create legal environments that enable experimentation. Regulatory sandboxes focused on maritime digitalisation can allow stakeholders to deploy blockchain-ZKP systems under controlled conditions. These testbeds provide opportunities to align technical outcomes with legal frameworks, particularly regarding customs laws, privacy rights and document admissibility.

2) STANDARDISATION THROUGH GLOBAL TRADE BODIES

Alignment with global data and compliance standards is essential. Bodies such as UN/CEFACT, the World Customs Organisation (WCO) and ISO TC 204 should be engaged to develop cross-compatible schemas for trade documents that are suitable for ZKP generation. For example, standardising how e-bills of lading or origin certificates are hashed and verified can enable seamless ZKP validation across jurisdictions.

3) INCENTIVISING EARLY ADOPTERS

Early-stage deployment of blockchain-ZKP systems often carries higher implementation costs and learning burdens. Governments and intergovernmental trade alliances can accelerate adoption by offering tariff incentives, priority customs processing or digital service credits to companies and ports that participate in pilot implementations. These incentives lower the barrier to entry and help build real-world use cases and trust.

4) GOVERNANCE AND SMART CONTRACT CUSTODIANSHIP A

question remains about who governs the deployed smart contracts, the ZKP verification logic and the updates to proof circuits. Without clear custodianship and update governance, systems risk fragmentation or protocol decay. Institutions such as port authorities or neutral third-party regulators should be empowered to act as trusted administrators with transparent upgrade mechanisms and dispute resolution protocols.

C. IMPLEMENTATION ROADMAP

To manage the complexity of nationwide or cross-border deployment, a phased implementation strategy is required. The roadmap should allow stakeholders to progress through awareness, design, deployment and institutionalisation with

clear milestones. Figure 4, below, presents the implementation Development and Verification: Technical teams begin system development, including smart contract logic, circuit design for ZKPs and simulation of key workflows. This phase also includes format standardisation and basic legal compliance alignment with customs procedures and digital identity frameworks.

1) Piloting and Capacity Building: Controlled pilot deployments are conducted in selected ports. Feedback is collected to refine the system, and intensive training is offered to both technical and operational users. Metrics such as time savings, error reduction and stakeholder satisfaction are monitored.

2) Full-Scale Implementation: Once pilots demonstrate success, the system is scaled to multiple ports with dedicated infrastructure. Governance models are established; nodes are federated among stakeholders and long-term monitoring mechanisms are introduced.

D. SELECTION OF APPROPRIATE TECHNOLOGY

Choosing the appropriate technology is essential for the success of any implementation. Hence, evaluating the different blockchain platforms and ZKP features based on their scalability, security, compatibility and transparency with existing systems will help to figure out which technology is the right fit for the proposed implementation [34], [35]. Blockchain platforms such as Ethereum, Hyperledger or any other have different features and capabilities [36]. The selection of the best blockchain platform depends on the requirements and the developed system architecture and may also depend on the current running system. Furthermore, ZKP protocols such as Zk-SNARKS, Zk-STARKS or Bulletproofs provide different levels of security and efficiency [37]. To ensure that elected technologies can integrate easily with the current systems as they are, or with minimal changes, offer a smooth transition and an effective implementation.

1) ZK-SNARKS

Zero-Knowledge Succinct Non-Interactive Argument of Knowledge is an encryption scheme which needs a trusted third party to execute the algorithm in order to generate the private key and the verification key [37]. This private key is called ''toxic waste''. If an attacker obtains it, the transaction can be forged, therefore, there is a need to keep it secure. This is the cryptographic proof generated by the prover to convince the verifier of the validity of a statement without revealing any sensitive information [17]. The usage of ZKP ranges from keeping sensitive information private to privacy-preserving transaction execution [38].

2) ZK-STARKS

Zero-Knowledge Scalable Transparent Arguments of Knowledge enables privacy-preserving identity sharing on the blockchain platform by only revealing the necessary information [27]. They are transparent and do not require a trusted setup or pre-processing to enhance their security properties. Zk-STARKs use collision-resistant hash functions to randomise query challenges, which ensure greater security and transparency in the system. Here, ''transparent'' means there is no need to generate and store the secret keys, eliminating risks associated with their compromise [39]. Thus, the absence of a trusted setup makes Zk-STARKs more resistant against specific types of attacks and easier to deploy, as far as there is no need to worry about the security of setup keys.

3) BULLETPROOFS

In Bulletproof ZKP, there is no requirement for any trusted setup. However, the bulletproofs used in their scheme are not the fastest regarding the verification time, as described by Wei [40]. Indeed, one of their attractive features is its small proof size, that performs and grows logarithmically with the complexity of the computation or statement. Hence, it performs amazingly well in handling small-scale problems.

As discussed, Bulletproofs is not seen as effective for implementation in the maritime industry. Based on the different aspects, the effectiveness of Zk-SNARK and Zk-STARK are analysed and presented below:

4) IMPLEMENTATION

For the purpose of proof generation and validation, a secret key is required in Zk-SNARK, whereas Zk-STARK is transparent and does not require such secret keys [41], thus eliminating the requirement of trusted setup to generate and store such keys. This facilitates the efficiency enhancement of the overall system as well as addressing many concerns. Furthermore, it also strengthens the system against the post-quantum attacks. As a result, the Zk-STARK protocol is best suited for the maritime networks, as it demands untrusted and diverse participants, such as international shipping companies, port authorities and customs agencies.

5) PROOF SIZE AND EXECUTION TIME

The proof size of Zk-SNARK is small (typically between 200-300 bytes) when compared with Zk-STARK (in the range of kilobytes) [33]. Verification sizes are related to the size of the proofs, and Zk-SNARK is efficient, faster and occupies less memory on chains during verification. Currently, Zk-SNARKs is more popular in blockchain networks due to its small proof size, faster performance and low gas costs. However, if Zk-STRAKS was faster at proof verification, it would undeniably have the potential to overcome its competitors, Zk-SNARK and Bulletproofs [42].

6) PRIVACY-PRESERVING AND SECURITY

Zk-SNARKs is constructed in the Common Reference String (CRS) model, which requires a setup phase to create proving and verification keys with CRS. As a part of key generation, some randomness is created, which needs to be disposed of later, at the end of the setup. However, misleading the disposal may compromise the security of this mechanism, and the possibility of false proofs may arise [43]. This is a

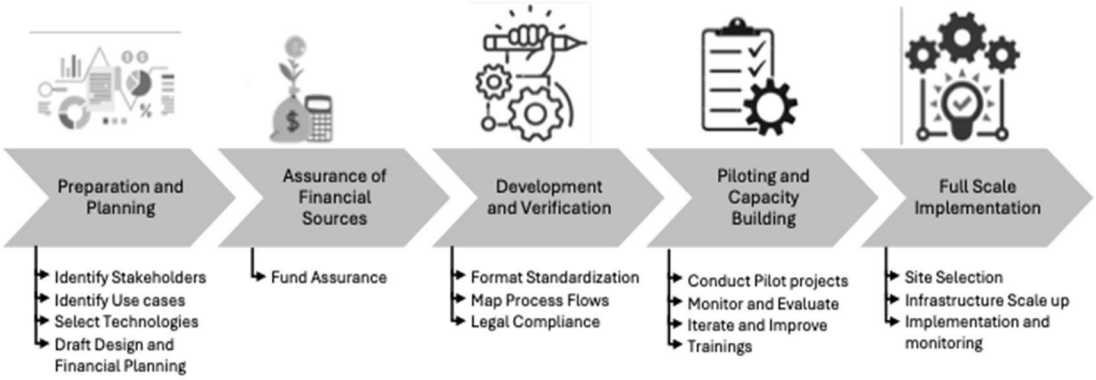

FIGURE 4. Implementation timeline.

difficult situation, as the CRS must be generated for use in a large network of untrusted participants. While comparing it with Zk-STARK and Bulletproofs, they do not require such setup, which also protects them from the quantum attacks that Zk-SNARKs is susceptible to. Although Bulletproofs is not as effective for a large network, considering the privacy-preserving and security points of view, Zk-STARKS is still seen as effective [17].

7) TRANSPARENCY AND SCALABILITY

As Zk-STARKs does not require a trusted setup for proof generations, that allows the system to be transparent when compared to Zk-SNARKs, which demands additional trust assumptions and governance structures, therefore becoming "toxic" when compromised and requiring disposal at the end [44]. Although the size of proofs generated by Zk-SNARKs is small and uses less computational overhead for verification, its scalability is limited by the trusted setup phase and becomes inefficient in handling dynamically changing large-scale datasets. On the other hand, Zk-STARKs can address the complications of handling large scales of datasets.

8) AUDITABILITY

As Zk-STARKs performs well with large data sets, it can be used to verify ship logs, cargo manifests and compliance records without revealing sensitive data, which ensures the proper auditability while preserving privacy.

Hence, Zk-SNARKs and Zk-STARKs help to balance transparency and privacy in the maritime industry, therefore helping to address the critical challenges in logistics, compliance and security. Its integration with blockchain assures efficiency and scalability, which were lacking from the implementation of blockchain alone. Regarding Zk-STARKs, due to the large size of proofs, it is not sensibly feasible to implement. Moreover, it takes longer to verify, and it requires more computing resources, which increases gas costs. Although Zk-STARKs is still developing and a lot of research is ongoing to enhance its reliability, it is nonetheless more efficient than Zk-SNARKs in other aspects, and a real possibility exists in the future of it being overtaken by Zk-STARKS.

TABLE 1. Comparison of zkp's.

Protocol	Trusted setup	Proof size	Verifier time	Post-Quantum secure	On-chain size
Zk-SNARK	Yes	~200 bytes	Fast	No	Small
Zk-STARK	No	KBs	Medium	Yes	Larger
Bulletproofs	No	Small	Slow	No	Small

zk-STARKs rely on collision-resistant hashes and avoid number-theoretic assumptions, making them inherently resilient to quantum attacks. This makes them more suitable for long-term compliance in sensitive cross-border operations. Beyond ZKP computational trade-offs, the integrity and security of the underlying blockchain network are also critical to ensuring trust and resilience in maritime applications, as explored below.

E. SCALABILITY AND INTEROPERABILITY STRATEGIES

Scalability and interoperability remain critical barriers to the deployment of blockchain-ZKP frameworks in real-world port environments *[45]*. Maritime logistics ecosystems are typically composed of heterogeneous systems, including proprietary terminal operating systems (TOS), legacy enterprise resource planning (ERP) platforms, and port community systems (PCS) with varying degrees of digital maturity. Consequently, any proposed architecture must accommodate backward compatibility, modular deployment, and multi-platform verification.

To enable interoperability with existing infrastructure, this framework adopts a modular design that supports RESTful APIs and event-driven middleware layers. These serve as adapters between the blockchain-ZKP validation engine and legacy port management systems, enabling seamless data

exchange without disrupting operational workflows. Integration can be achieved incrementally by encapsulating verification logic within microservices that communicate with existing systems through secure messaging protocols (e.g., MQTT, AMQP).

In terms of cross-chain compatibility, the framework is designed to operate on Ethereum but can be extended to other distributed ledger platforms such as Hyperledger Fabric, Corda, or Polkadot via interoperability protocols. Solutions such as Interledger and decentralised notary schemes allow for anchoring proofs or state transitions across chains without compromising cryptographic integrity. This is particularly important in scenarios where stakeholders (e.g., customs, freight brokers, port operators) rely on different blockchain infrastructures for contractual or jurisdictional reasons.

From a scalability standpoint, zk-SNARKs offer constant-size proofs and fast on-chain verification, making them suitable for high-throughput environments. For larger-scale implementations, Layer 2 solutions such as rollups or sidechains can be leveraged to aggregate proofs off-chain before final commitment on the main net, thereby reducing gas costs and network congestion. This approach ensures the system remains responsive under increased transaction loads typical of major port terminals.

Taken together, these strategies offer a practical pathway for integrating privacy-preserving blockchain systems with complex and often fragmented IT ecosystems found in global maritime logistics.

F. BLOCKCHAIN-ZKP NETWORK SECURITY CONSIDERATIONS

While Zero-Knowledge Proofs (ZKPs) ensure privacy and selective disclosure in document verification and compliance processes, the underlying blockchain network must also be secure, resilient and tamper-proof to guarantee end-to-end system integrity.

1) CHAIN INTEGRITY AND IMMUTABILITY

The proposed framework assumes deployment on a secure blockchain such as Ethereum, where transactions are confirmed through consensus protocols like Proof of Stake (PoS). Once a transaction is completed, such as a customs ZKP validation or container clearance, it is committed to the chain, and it becomes immutable, thus ensuring a trusted audit trail for all stakeholders. This immutability guarantees that no actor can retroactively alter shipment records or compliance logs.

2) NODE VALIDATOR SECURITY

In PoS-based chains like Ethereum, node validators are selected based on economic stake, and malicious behaviour results in slashing (stake forfeiture). This mechanism incentivises honest participation and protects against block reordering or double-spending attacks. For private or consortium deployments, validator governance can be further enhanced through permissioned nodes controlled by port authorities, customs agencies or international logistics consortia.

3) ATTACK VECTORS AND RISK MITIGATION

Potential threats to the system include:

- Sybil attacks, where malicious actors attempt to control multiple validator nodes. This is mitigated by stake-based voting in public chains and permissioned access in private deployments;
- 51% attacks, which are economically unfeasible in Ethereum's PoS model. but remain a risk in smaller or less distributed networks;
- Front-running and MEV (Miner Extractable Value) in public deployments, which can be minimised using transaction ordering protection or by adopting Layer-2 solutions with deterministic execution.

4) SMART CONTRACT EXPLOITS

Smart contracts governing ZKP verification and payment automation must be carefully audited to prevent vulnerabilities such as re-entrancy, overflow or logic flaws. Using formally verified templates, restricted function access and upgradeable contracts with community oversight reduces this risk.

These considerations demonstrate that blockchain-ZKP integration must not only ensure cryptographic privacy but also rely on a secure, economically resilient and well-governed chain infrastructure to achieve holistic system security.

G. THREAT MODEL AND SECURITY ANALYSIS

The integration of Zero-Knowledge Proofs (ZKPs) with blockchain infrastructure for maritime logistics must address a range of potential security threats that stem from adversarial behavior, infrastructural limitations, and cryptographic assumptions. This section outlines the underlying threat model, describes adversarial capabilities, and evaluates the proposed system's resistance to common and advanced attack vectors.

1) ADVERSARY MODEL

We assume a partially asynchronous distributed system, where adversaries may attempt to compromise either the blockchain infrastructure or the cryptographic proof layer. The adversaries fall into three categories:

- Honest-but-curious adversaries: Attempt to infer sensitive data (e.g., cargo value, sender identity) by analysing metadata or transaction flows without altering protocols.
- Malicious adversaries: Capable of tampering with messages, submitting fraudulent transactions, or forging identities to gain unauthorised access.
- Quantum-capable adversaries: Equipped with quantum computing resources capable of breaking number-theoretic assumptions underlying classical cryptographic schemes.

The threat model is aligned with standard assumptions in permissioned or semi-public blockchain deployments, where most validators are trusted entities (e.g., port authorities,

TABLE 2. Threat surface analysis and mitigation strategies for ZKP-Enabled maritime.

Threat	Vector	Mitigation Strategy
Sybil Attacks	Adversaries spin up multiple identities to gain control over consensus	Use of PoS with economic slashing (public chains) or permissioned validators (consortia)
Collusion Among Validators	Trusted validators may collaborate to manipulate proofs or transaction flow	Role separation, off-chain ZKP validation, and audit trails via immutable logs
Quantum Attacks	Shor's algorithm could break zk-SNARK elliptic curve cryptography	Preference for zk-STARKs and hash-based post-quantum constructions
Smart Contract Exploits	Vulnerabilities such as reentrancy, logic flaws, or gas exhaustion	Formal verification, use of upgradable contracts, access modifiers, and audit protocols
Metadata Leakage	Side-channel inference from public logs or transaction timing	Off-chain proof generation, on-chain only proof results and hashes, no raw data exposed
IoT Data Forgery	Manipulated sensor data feeds used to influence compliance decisions	Digital signatures and hash commitments from authenticated sensors

customs agencies), but external actors may attempt protocol subversion.

2) THREAT SURFACE AND RISK ANALYSIS

The following table summarises the main threats affecting the proposed ZKP-enabled maritime blockchain system, together with their attack vectors and corresponding mitigation strategies across both the blockchain and cryptographic layers.

3) SECURITY GUARANTEES

The system provides the following assurances under standard cryptographic assumptions:

- Confidentiality: Trade-specific data (e.g., cargo contents, invoice terms) is never revealed on-chain. ZKPs allow validation of regulatory compliance without disclosing underlying information.
- Integrity and Immutability:Once proofs are verified, the outcome and metadata are recorded immutably on the blockchain ledger, preventing tampering or repudiation.
- Post-Quantum Resilience: zk-STARKs rely solely on hash-based constructions and avoid number-theoretic hardness assumptions, ensuring long-term security even in the presence of quantum adversaries.
- Auditable Compliance: The combination of ZKP-based selective disclosure and smart contract logging supports a verifiable audit trail for regulatory bodies, without central trust dependencies.

4) LIMITATIONS AND FUTURE ENHANCEMENTS

While the current architecture mitigates major threats, residual risks remain, particularly with external dependency layers (e.g., sensor integrity) and evolving smart contract vulnerabilities. Future work will focus on integrating real-time anomaly detection, formal model-checking of smart contracts, and introducing zero-knowledge rollups to further reduce on-chain exposure and verification costs

VI. CONCLUSION AND FUTURE RESEARCH

In the context of Maritime Supply Chain Management (MSCM), blockchain technology has emerged as a pivotal innovation to address persistent challenges related to inefficiency, transparency, and trust. Despite these advantages, blockchain systems face critical limitations concerning scalability, computational cost, and data privacy. Zero-Knowledge Proofs (ZKPs) represent a powerful complement to blockchain technology, enabling the secure verification of information without revealing sensitive underlying data. This study has demonstrated the potential of ZKP integration in blockchain-enabled maritime systems to balance transparency, privacy, and operational efficiency.

Grounded in real-world use cases and operational challenges across major ports, this research highlights the value of combining blockchain and ZKP technologies to optimise maritime logistics. The most significant applications relate to privacy-preserving traceability, verifiable document authentication, fraud prevention, and compliance with evolving regulatory frameworks. By enabling off-chain computations through lightweight cryptographic proofs, the proposed approach reduces computational overhead, improves scalability, and safeguards sensitive trade information against unauthorised access at the ZKP layer.

While prior case studies at ports such as Rotterdam and Singapore have reported reductions in customs clearance times and improvements in fraud detection rates, this study does not independently replicate those operational outcomes. Instead, it introduces a controlled simulation-based prototype that validates the technical feasibility of integrating ZKPs within blockchain environments. The prototype contributes empirical benchmarks—such as proof generation time, verification latency, and gas cost—that serve as foundational indicators for subsequent field implementations. Hence, the findings substantiate the architectural soundness of the proposed framework rather than asserting direct performance improvements in live operations.

The successful implementation of blockchain–ZKP frameworks within MSCM will depend on sustained collaboration among stakeholders, the alignment of enabling technologies, and the evolution of legal and regulatory mechanisms. Ongoing advancements in cryptographic techniques and

blockchain scalability solutions continue to strengthen the feasibility of these systems. The integration of ZKP with blockchain has the potential to transform maritime logistics into a more secure, efficient, and privacy-compliant ecosystem, redefining governance and operational processes.

Future research should priorities the standardisation of interoperability protocols, the design of lightweight ZKP nodes for edge and IoT environments, and the optimisation of proof systems for real-time processing. Furthermore, empirical pilot programs are needed to evaluate governance models and test the robustness of blockchain–ZKP deployments under live port conditions. Although blockchain adoption is progressing across global maritime terminals, its general use remains limited. Layer-two enhancements and user-centric design principles will be crucial in advancing accessibility, interoperability, and adoption. Continued research and cross-sector collaboration will enable the maritime industry to evolve toward a more transparent, resilient, and sustainable supply chain ecosystem.

REFERENCES

[1] C.-S. Yang, "Maritime shipping digitalization: Blockchain-based technology applications, future improvements, and intention to use," *Transp. Res. E, Logistics Transp. Rev.*, vol. 131, pp. 108–117, Nov. 2019, doi: 10.1016/j.tre.2019.09.020.

[2] M. Kugler, M. Brandenburg, and S. Limant, "Automizing the manual link in maritime supply chains? An analysis of twistlock handling automation in container terminals," *Maritime Transp. Res.*, vol. 2, Jan. 2021, Art. no. 100017, doi: 10.1016/j.martra.2021.100017.

[3] J. Thomas and Y. Tan, "Key design properties for shipping information pipeline," in *Open and Big Data Management and Innovation* (Lecture Notes in Computer Science). Cham, Switzerland: Springer, 2015, pp. 491–502, doi: 10.1007/978-3-319-25013-7_40.

[4] C. Wan, X. Yan, D. Zhang, Z. Qu, and Z. Yang, "An advanced fuzzy Bayesian-based FMEA approach for assessing maritime supply chain risks," *Transp. Res. E, Logistics Transp. Rev.*, vol. 125, pp. 222–240, May 2019, doi: 10.1016/j.tre.2019.03.011.

[5] A. Padma, M. Ramaiah, and V. Ravi, "Blockchain technology for agriculture supply chain management," in *Intelligent Computing and Optimization for Sustainable Development*. Boca Raton, FL, USA: CRC Press, 2024, pp. 192–210. [Online]. Available: https://library.oapen.org/bitstream/handle/20.500.12657/99313/1/9781040159897.pdf#page=205

[6] N. Newman, "Can blockchain transform transport?" *Eng. Technol.*, vol. 13, no. 6, pp. 58–61, Jul. 2018, doi: 10.1049/et.2018.0605.

[7] J. Liu, H. Zhang, and L. Zhen, "Blockchain technology in maritime supply chains: Applications, architecture and challenges," *Int. J. Prod. Res.*, vol. 61, no. 11, pp. 3547–3563, Jun. 2023, doi: 10.1080/00207543.2021.1930239.

[8] F. Dietrich, Y. Ge, A. Turgut, L. Louw, and D. Palm, "Review and analysis of blockchain projects in supply chain management," *Proc. Comput. Sci.*, vol. 180, pp. 724–733, Jan. 2021.

[9] A. Mukhtar, A. Romli, and N. Karimah, "Blockchain network model to improve supply chain visibility based on smart contract," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 10, pp. 1–8, Jun. 2020. [Online]. Available: https://search.proquest.com/openview/8620bc5c5b8830285cd721fdc8dc5415/1?pq-origsite=gscholar&cbl=5444811

[10] M. L. Rethlefsen et al., "PRISMA-S: An extension to the PRISMA statement for reporting literature searches in systematic reviews," *Systematic Rev.*, vol. 10, no. 1, p. 39, Jan. 2021, doi: 10.1186/s13643-020-01542-z.

[11] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *J. Manage. Inf. Syst.*, vol. 24, no. 3, pp. 45–77, Dec. 2007, doi: 10.2753/mis0742-1222240302.

[12] L. Li and J. Zhou, "Blockchain effects and investment strategies in the maritime supply chain under perishable goods loss," *Systems*, vol. 13, no. 3, p. 196, Mar. 2025, doi: 10.3390/systems13030196.

[13] S. Pu and J. S. L. Lam, "Blockchain adoptions in the maritime industry: A conceptual framework," *Maritime Policy Manage.*, vol. 48, no. 6, pp. 777–794, Aug. 2021, doi: 10.1080/03088839.2020.1825855.

[14] A. Padma and M. Ramaiah, "Lightweight privacy preservation blockchain framework for healthcare applications using GM-SSO," *Results Eng.*, vol. 25, Mar. 2025, Art. no. 103882, doi: 10.1016/j.rineng.2024.103882.

[15] D. Čapko, S. Vukmirović, and N. Nedić, "State of the art of zero-knowledge proofs in blockchain," in *Proc. 30th Telecommun. Forum (TELFOR)*, Nov. 2022, pp. 1–4, doi: 10.1109/TELFOR56187.2022.9983760.

[16] K. Gai, H. Tang, G. Li, T. Xie, S. Wang, L. Zhu, and K. R. Choo, "Blockchain-based privacy-preserving positioning data sharing for IoT-enabled maritime transportation systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2344–2358, Feb. 2023, doi: 10.1109/TITS.2022.3190487.

[17] B. Oude Roelink, M. El-Hajj, and D. Sarmah, "Systematic review: Comparing zk-SNARK, zk-STARK, and bulletproof protocols for privacy-preserving authentication," *Secur. PRIVACY*, vol. 7, no. 5, p. 401, Sep. 2024, doi: 10.1002/spy2.401.

[18] A. Padma and M. Ramaiah, "Blockchain based an efficient and secure privacy preserved framework for smart cities," *IEEE Access*, vol. 12, pp. 21985–22002, 2024, doi: 10.1109/ACCESS.2024.3364078.

[19] B. Lu, H. Lu, and H. Wang, "Design and value analysis of the blockchain-based port logistics financial platform," *Maritime Policy Manage.*, vol. 51, no. 6, pp. 1037–1061, Aug. 2024, doi: 10.1080/03088839.2023.2205870.

[20] S. Ghosh. *What Are Smart Port Technologies?*. Marine Insight. Accessed: Jun. 9, 2025. [Online]. Available: https://www.marineinsight.com/tech/what-are-smart-port-technologies/

[21] Y. Wang, P. Chen, B. Wu, C. Wan, and Z. Yang, "A trustable architecture over blockchain to facilitate maritime administration for MASS systems," *Rel. Eng. Syst. Saf.*, vol. 219, Mar. 2022, Art. no. 108246, doi: 10.1016/j.ress.2021.108246.

[22] E. Irannezhad, "The architectural design requirements of a blockchain-based port community system," *Logistics*, vol. 4, no. 4, p. 30, Nov. 2020, doi: 10.3390/logistics4040030.

[23] S. Nguyen, P. S.-L. Chen, and Y. Du, "Blockchain adoption in container shipping: An empirical study on barriers, approaches, and recommendations," *Mar. Policy*, vol. 155, Sep. 2023, Art. no. 105724, doi: 10.1016/j.marpol.2023.105724.

[24] A. Padma and M. Ramaiah, "Blockchain based solution for secure information sharing in pharma supply chain management," *Heliyon*, vol. 10, no. 22, Nov. 2024, Art. no. e40273, doi: 10.1016/j.heliyon.2024.e40273.

[25] S. Tsiulin, K. H. Reinau, and O.-P. Hilmola, "The key challenges of blockchain implementation in maritime sector: Summary from literature and previous research findings," *Proc. Comput. Sci.*, vol. 217, pp. 348–357, Jan. 2023, doi: 10.1016/j.procs.2022.12.230.

[26] Z. H. Munim, O. Duru, and E. Hirata, "Rise, fall, and recovery of blockchains in the maritime technology space," *J. Mar. Sci. Eng.*, vol. 9, no. 3, p. 266, Mar. 2021, doi: 10.3390/jmse9030266.

[27] L. Zhou, A. Diro, A. Saini, S. Kaisar, and P. C. Hiep, "Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities," *J. Inf. Secur. Appl.*, vol. 80, Feb. 2024, Art. no. 103678, doi: 10.1016/j.jisa.2023.103678.

[28] T. K. Dasaklis, E. Kopanaki, P. T. Chountalas, N. P. Rachaniotis, T. G. Voutsinas, K. Giannakis, and G. Chondrokoukis, "Exploring the implementation challenges of the Electronic Freight Transport Information (eFTI) regulation: An empirical perspective from Greece," *Logistics*, vol. 8, no. 1, p. 30, 2024, doi: 10.3390/logistics8010030.

[29] M. B. Farah, Y. Ahmed, H. Mahmoud, S. A. Shah, M. O. Al-Kadri, S. Taramonli, X. Bellekens, R. Abozariba, M. Idrissi, and A. Aneiba, "A survey on blockchain technology in the maritime industry: Challenges and future perspectives," *Future Gener. Comput. Syst.*, vol. 157, pp. 618–637, Aug. 2024, doi: 10.1016/j.future.2024.03.046.

[30] G. Balci and E. Surucu-Balci, "Blockchain adoption in the maritime supply chain: Examining barriers and salient stakeholders in containerized international trade," *Transp. Res. E, Logistics Transp. Rev.*, vol. 156, Dec. 2021, Art. no. 102539, doi: 10.1016/j.tre.2021.102539.

[31] E. Morais, T. Koens, C. van Wijk, and A. Koren, "A survey on zero knowledge range proofs and applications," *Social Netw. Appl. Sci.*, vol. 1, no. 8, p. 946, Jul. 2019, doi: 10.1007/s42452-019-0989-z.

[32] A. R. Block, A. Garreta, P. R. Tiwari, and M. Zając, "On soundness notions for interactive oracle proofs," *J. Cryptol.*, vol. 38, no. 1, p. 4, Nov. 2024, doi: 10.1007/s00145-024-09520-7.
[33] A.-E. Panait and R. F. Olimid, "On using zk-SNARKs and zk-STARKs in blockchain-based identity management," in *Innovative Security Solutions for Information Technology and Communications*. Cham, Switzerland: Springer, 2021, pp. 130–145, doi: 10.1007/978-3-030-69255-1_9.
[34] R. W. Ahmad, H. Hasan, R. Jayaraman, K. Salah, and M. Omar, "Blockchain applications and architectures for port operations and logistics management," *Res. Transp. Bus. Manage.*, vol. 41, Dec. 2021, Art. no. 100620, doi: 10.1016/j.rtbm.2021.100620.
[35] H. Guo and X. Yu, "A survey on blockchain technology and its security," *Blockchain, Res. Appl.*, vol. 3, no. 2, Jun. 2022, Art. no. 100067, doi: 10.1016/j.bcra.2022.100067.
[36] V. Astarita, V. P. Giofrè, G. Mirabelli, and V. Solina, "A review of blockchain-based systems in transportation," *Information*, vol. 11, no. 1, p. 21, Dec. 2019, doi: 10.3390/info11010021.
[37] S. M. M. Hamidi, S. F. Hoseini, H. Gholami, and M. Kananizadeh-Bahmani, "A three-stage digital maturity model to assess readiness for blockchain implementation in the maritime logistics industry," *J. Ind. Inf. Integr.*, vol. 41, Sep. 2024, Art. no. 100643, doi: 10.1016/j.jii.2024.100643.
[38] S. Ebrahimi and P. Hassanizadeh. (2024). *From Interaction to Independence: ZkSNARKs for Transparent and Non-Interactive Remote Attestation*. Accessed: Jun. 9, 2025. [Online]. Available: https://eprint.iacr.org/2024/1068
[39] T. Lavaur, J. Lacan, and C. P. C. Chanel, "Enabling blockchain services for IoE with zk-rollups," *Sensors*, vol. 22, no. 17, p. 6493, Aug. 2022, doi: 10.3390/s22176493.
[40] L. Wei, L. Peili, and L. Fei, "Zk-STARKs based scheme for sealed auctions in chains," *IET Blockchain*, vol. 4, no. 4, pp. 344–354, Dec. 2024, doi: 10.1049/blc2.12090.
[41] G. A. F. Rebello, G. F. Camilo, L. A. C. de Souza, M. Potop-Butucaru, M. D. de Amorim, M. E. M. Campista, and L. H. M. K. Costa, "A survey on blockchain scalability: From hardware to layer-two protocols," *IEEE Commun. Surveys Tuts.*, vol. 26, no. 4, pp. 2411–2458, 2024, doi: 10.1109/COMST.2024.3376252.
[42] J. W. Heo, G. Ramachandran, and R. Jurdak, "NPPoS: Non-interactive practical proof-of-storage for blockchain," *Blockchain, Res. Appl.*, vol. 5, no. 4, Dec. 2024, Art. no. 100221, doi: 10.1016/j.bcra.2024.100221.
[43] A. M. Pinto, "An introduction to the use of zk-SNARKs in blockchains," in *Mathematical Research for Blockchain Economy*. Cham, Switzerland: Springer, 2020, pp. 233–249, doi: 10.1007/978-3-030-37110-4_16.
[44] E. Ben-Sasson, I. Bentov, Y. Horesh, and M. Riabzev, "Scalable zero knowledge with no trusted setup," in *Proc. Annu. Int. Cryptol. Conf.*, 2019, pp. 701–732, doi: 10.1007/978-3-030-26954-8_23.
[45] M. A. Aleisa, "Blockchain-enabled zero trust architecture for privacy-preserving cybersecurity in IoT environments," *IEEE Access*, vol. 13, pp. 18660–18676, 2025, doi: 10.1109/ACCESS.2025.3529309.

JOEL CURADO is currently pursuing the Ph.D. degree in blockchain with a focus on governance, modularity, and its applications in service industries. He is a technology and growth go-to-market executive with more than 18 years of experience leading digital transformation, blockchain, and smart city initiatives across global enterprises and governments, including roles at Cisco Systems. He is the CEO and Co-Founder of DISTLI, a startup developing AI-enhanced blockchain edge infrastructure for cybersecurity and process optimisation in technology-driven organisations. He holds advanced certifications in Public Policy from Harvard Kennedy School, an MBA from IE Business School, and serves as a Professor at ISCTE-IUL in Portugal and Molde University, Norway, teaching smart cities, emerging technologies, and blockchain.

MANILA BHANDARI is currently a Researcher with the Instituto Universitário de Lisboa (ISCTE), affiliated with ISTAR-IUL. Her work focuses on digital transformation in logistics and blockchain-based innovations in supply chains. She contributes to interdisciplinary research projects that aim to enhance transparency, efficiency, and regulatory compliance in international trade. Her recent work explores the integration of privacy-preserving technologies, such as zero-knowledge proofs (ZKPs), in maritime logistics ecosystems.

JOÃO C. FERREIRA has over 25 years of experience in applied digital technologies. His research covers AI, the IoT, blockchain, and their integration into healthcare, smart cities, and maritime logistics. Regarding the quality of journals, he has published 55 articles in Q1 journals, 23 in Q2, 18 in Q3, and eight in Q4. Notably, 15 of these were published in the top 5% Q1 journals. Among his contributions is a national patent related to edge computing and vessel monitoring systems, demonstrating the applied impact of his work. His research interests include blockchain applications in supply chains, healthcare, digital identity, and energy systems; the Internet of Things; artificial intelligence; and the development of smart cities, smart transportation, and smart health infrastructures. He has also received three best paper awards at international conferences indexed by Scopus.

ANA L. MARTINS received the M.Sc. degree in management (business strategy) and the Ph.D. degree in management (operations management and technology). She is currently an Associate Professor at ISCTE-IUL and an integrated Researcher at the Business Research Unit (BRU)-ISCTE. She is also the ISCTE Business School Vice-Dean of teaching and innovation. She teaches operations management, logistics management, service operations management, and supply chain management. She has authored more than 120 scientific articles, several in Q1 journals. She is involved in several European projects, contributing to the areas of operations management, technologies, and assurance of learning activities. Her current research interests include operations management, logistics management, supply chain management and technologies, and lean management in the services area, mainly in judicial and healthcare systems, and in the fish industry. She has been distinguished with best paper awards in Scopus-indexed conferences.