Routledge
Taylor & Francis Group

Maritime Policy & Management

The flagship journal of international shipping and port research

ISSN: 0308-8839 (Print) 1464-5254 (Online) Journal homepage: www.tandfonline.com/journals/tmpm20

Enhancing maritime supply chain security and efficiency: a review of Zero-Knowledge Proofs in blockchain applications

Joel Curado Silveirinha, Manila Bhandari, João Carlos Ferreira & Ana Lúcia Martins

To cite this article: Joel Curado Silveirinha, Manila Bhandari, João Carlos Ferreira & Ana Lúcia Martins (21 Nov 2025): Enhancing maritime supply chain security and efficiency: a review of Zero-Knowledge Proofs in blockchain applications, Maritime Policy & Management, DOI: 10.1080/03088839.2025.2580502

To link to this article: https://doi.org/10.1080/03088839.2025.2580502

Published online: 21 Nov 2025.

MARITIME POLICY & MANAGEMENT
https://doi.org/10.1080/03088839.2025.2580502

Routledge
Taylor & Francis Group

Enhancing maritime supply chain security and efficiency: a review of Zero-Knowledge Proofs in blockchain applications

Joel Curado Silveirinha[a], Manila Bhandari[a], João Carlos Ferreira[a] and Ana Lúcia Martins[b]

[a]ISTAR - Information Sciences, Technologies and Architecture Research Centre, University Institute of Lisbon (ISCTE-IUL), Lisbon, Portugal; [b]Iscte - Instituto Universitário de Lisboa, Business Research Unit (BRU-IUL), Lisbon, Portugal

ABSTRACT

Despite the maritime supply chain being the backbone of global trade, it faces persistent challenges in transparency, fraud prevention, shipment tracking and data privacy. Blockchain technology has emerged as a transformative solution, enhancing trust and traceability within supply chain networks. However, its limitations in data privacy and scalability necessitate advanced privacy-preserving mechanisms. Zero-Knowledge Proofs (ZKP) offers a cryptographic approach to validate data without exposing sensitive information, addressing blockchain's privacy constraints. This paper reviews the state of the art on current applications of blockchain in maritime supply chain management and explores the integration of ZKP for secure trade document verification, fraud detection, privacy-preserving traceability and regulatory compliance. Additionally, it examines computational overhead, scalability and adoption barriers while proposing future research directions. Implementing ZKP within blockchain-based port operations enables robust governance models, ensuring data verification without revealing confidential details. This approach fosters a secure and privacy-compliant trade environment, enhancing trust and collaboration among stakeholders. By optimising resource allocation and mitigating risks, integrating ZKP can significantly improve maritime supply chain efficiency. Integrating Zero-Knowledge Proofs with blockchain, maritime logistics can achieve a balance between transparency, security and operational efficiency, addressing existing challenges in data privacy and regulatory compliance, improving the sustainability of port operations.

ARTICLE HISTORY
Received 7 March 2025
Accepted 8 October 2025

KEYWORDS
Maritime supply management; blockchain technology; zero-knowledge proof; data privacy; cryptography; governance

1. Introduction

Maritime supply chain plays a pivotal role in global trade and facilitates the transportation of approximately 90% of the world's goods (Nguyen, Chen, and Du 2023), undeniably being a key driver of prosperity in the context of global economic development. However, this critical sector faces persistent challenges, including inefficiencies in

CONTACT João Carlos Ferreira joao.carlos.ferreira@iscte-iul.pt ISTAR - Information Sciences, Technologies and Architecture Research Centre University Institute of Lisbon (ISCTE-IUL), LisbonPortugal

logistics, fraud and privacy concerns regarding sensitive data trade. These challenges are ambitious to solve due to old silo approaches with separate operations, making it difficult for stakeholders to work together as networks (Liu, Zhang, and Zhen 2023).

Maritime supply chain logistics are distinct, with ports as central nodes and involving shippers, carriers, transport providers, and related services. Numerous stakeholders, including shipping lines, port operators, insurers, and payment systems, are interconnected through complex processes. The increasing complexity and global dependence on maritime logistics have intensified interactions and dependencies. Addressing these challenges is crucial to improving efficiency, security, and trust. Policymakers, industry players, and researchers are working to enhance maritime supply chains by optimising container flow, promoting paperless digitalisation, and ensuring continuous monitoring at national borders (Pu and Lam 2021).

Supply Chain Management (SCM) involves coordinating goods, information, and services across networks, requiring transparency, cooperation, and resilience (Mentzer et al. 2001). Nonetheless, physical bottlenecks like port congestion still disrupt schedules and elevate costs, affecting both shipowners and cargo stakeholders (Bai, Jia, and Xu 2024). In this context, a maritime supply chain refers to the set of interlinked logistics processes that are specific to ocean-based transportation, including port operations and shipping lines, whereas a regular supply chain typically involves inland logistics through road, rail, or air, each with distinct regulatory and infrastructural challenges (Mentzer et al. 2001).

Blockchain has emerged as a key SCM innovation (Durán et al. 2024). In 2016, Maersk projected it could reduce maritime transport costs by 20% and save $27 billion annually between East Africa and Europe. It has already decreased packaging transit time by 40% in U.S. production lines (Chen et al. 2020). Its decentralised, immutable ledger improves transparency, traceability, and accountability (Nakamoto 2008). However, adoption in maritime logistics is hindered by governance issues, intra-organisational barriers, and a shortage of specialists. Moreover, blockchain transparency may compromise confidentiality, revealing sensitive data such as financial transactions and trade terms (Balci and Surucu-Balci 2021). Scalability, decentralisation, and security remain technical challenges due to transaction validation costs (Khan, Jung, and Hashmani 2021).

Zero-Knowledge Proofs (ZKPs) offer a cryptographic solution by validating information without exposing its content (Major, Buchanan, and Ahmad 2020). ZKPs meet maritime security requirements by safeguarding privacy and verifying data provenance. They allow verification of trade compliance and document authenticity without disclosing confidential data (Sun et al. 2021), vital for handling container bills of lading and third-party information. Combined with blockchain, ZKPs balance transparency and confidentiality (Sedlmeir et al. 2022), enabling more adaptive, secure governance systems for maritime logistics and beyond.

This paper reviews state-of-the-art ZKP applications in maritime SCM, examining how they address privacy, fraud, and efficiency challenges, alongside technical and implementation barriers. It also identifies emerging trends and research gaps to guide future innovation. Findings underscore ZKPs' potential to improve security, efficiency, and transparency, supporting broader adoption in the maritime industry.

The remainder of the paper is organised as follows. Section 2 introduces the fundamental concepts of blockchain technology, with a focus on the technical components

most relevant to maritime supply chains. Section 3 explores how blockchain is currently being applied in port operations and maritime logistics, supported by illustrative case studies. Section 4 discusses the main challenges to adoption, including technical limitations, organisational resistance, and regulatory constraints. Section 5 considers the broader implications for improving efficiency and sustainability in maritime supply chains. Finally, Section 6 summarises the key findings and outlines potential directions for future research.

2. Theoretical background

This section aims at disclosing the fundamental knowledge necessary to understand ZKP integration and blockchain in the maritime supply chain. This section addresses (1), the broader context and challenges outlined in maritime supply chain management and (2), the explanation of key technological concepts, such as blockchain and ZKP, which underpin this research. To understand the implications of integrating Zero-Knowledge Proofs (ZKPs) with blockchain in maritime supply chains, it is essential to establish a theoretical foundation that reflects both the generic architecture of these technologies and their cross-sectoral applications. Blockchain, originally conceptualised for digital currencies, has evolved into a foundational technology with wide applicability across domains such as finance, healthcare, manufacturing, and public governance. Each of these sectors presents distinctive challenges, ranging from data confidentiality and regulatory compliance to scalability and interoperability, that blockchain seeks to address through decentralisation, transparency, and automation.

2.1. Blockchain technology and consensus mechanisms

Blockchain technology enables secure storage, utilisation, and sharing of information through a decentralised, peer-to-peer distributed ledger (Uddin et al. 2021). Each node maintains an identical copy of the database, enhancing resilience by eliminating single points of failure. Transactions are grouped in time-stamped blocks, secured by cryptographic hash functions and public-key encryption (Wong 2021). Introduced with Bitcoin (Nakamoto 2008), blockchain's tamperproof ledger now supports applications in voting, healthcare, banking, real estate, and supply chain management (SCM). In maritime logistics, it improves transparency, secures vessel location data, and facilitates equitable pricing strategies among container lines (Gai et al. 2023). It also enables secure sharing of production, maintenance, crew, and vessel status data, thus reducing operational delays and inefficiencies (Sarfaraz, Chakrabortty, and Essam 2023).

At the heart of blockchain's operation is the consensus mechanism, which governs how agreement is reached on the validity and sequencing of transactions across distributed participants. The choice of consensus protocol influences a blockchain system's performance, security, energy consumption, and governance structure, making it a critical design consideration, especially for maritime supply chains involving multiple stakeholders with varying trust levels.

Proof of Work (PoW), pioneered by Bitcoin, requires nodes (miners) to solve computational puzzles to append new blocks (Haouari et al. 2022). Its main advantage lies in

strong tamper-resistance and Sybil attack mitigation, but these benefits come at the cost of extremely high energy use and limited throughput, making it unsuitable for most enterprise or regulatory environments (Barat et al. 2019). While secure and fully decentralized, PoW systems lack the efficiency needed for time-sensitive maritime operations such as real-time cargo monitoring or customs documentation exchange.

Proof of Stake (PoS) introduces efficiency by assigning validation rights based on the quantity of cryptocurrency staked. This reduces energy costs and increases transaction throughput while supporting hybrid public-private governance models (Hu et al. 2021). PoS systems, such as Ethereum 2.0, are increasingly favored in enterprise settings, including trade finance and shipping logistics, where sustainability and scalability are essential. However, PoS may exacerbate centralisation by disproportionately empowering wealthier validators.

Practical Byzantine Fault Tolerance (PBFT), by contrast, is tailored for permissioned networks where nodes are authenticated and known. PBFT offers fast finality and low energy use, but with limited scalability due to communication overhead that grows quadratically with node count. For port community systems, shipping alliances, or customs consortia, PBFT-based platforms like Hyperledger Fabric (Gai et al. 2023) offer practical advantages in consensus speed, legal accountability, and modular architecture.

In maritime settings, smart contracts, first introduced via Ethereum, further extend blockchain's functionality by automating rule-based transactions once pre-defined conditions are met. This reduces processing time for critical documents such as bills of lading (Shin et al. 2024), cuts administrative costs, and mitigates disputes and fraud (Irannezhad and Faroqi 2023). Frameworks like Ripple's Codius enhance smart contract interoperability across platforms, while Layer-2 decentralized applications (DApps) improve transactional throughput and user experience (Salzano et al. 2024).

From a technical standpoint, blockchain leverages Merkle trees for lightweight integrity verification, and cryptographic headers (including timestamps, nonces, and previous block hashes) to ensure tamper-evident continuity across blocks (Nakamoto 2008). Public Key Infrastructure (PKI) and cryptographic hashing secure identities and data flows, while encryption protects against unauthorized access.

Yet blockchain alone cannot preserve transactional privacy, an issue particularly acute in commercial maritime settings where confidential data such as pricing, contracts, and shipping schedules must remain protected. This gap is addressed by Zero-Knowledge Proofs (ZKPs), which allow parties to verify information without revealing the underlying data (Morais et al. 2019). As discussed in Section 2.4, ZKPs can be layered over blockchain to ensure compliance, interoperability, and auditability without compromising sensitive commercial information.

Despite blockchain's promise, scalability remains a fundamental constraint, particularly in high-volume, time-sensitive supply chains such as maritime logistics. Traditional blockchain architectures suffer from latency and throughput bottlenecks as the number of transactions and participants increases. Two key architectural strategies to address this challenge are Layer-2 solutions and sharding.

Layer-2 solutions operate off-chain, processing transactions outside the base blockchain while periodically settling state changes on-chain. Techniques such as state channels, payment channels, and zk-rollups dramatically increase throughput and reduce

transaction costs without sacrificing security. For instance, zk-rollups bundle hundreds of transactions and submit a succinct zero-knowledge proof to the main chain, verifying correctness without revealing transaction content. This is particularly relevant for maritime settings involving port call optimisations, container tracking, or customs clearance, where real-time responsiveness is essential. However, while Layer-2 architectures improve performance, they introduce new coordination and usability challenges, such as off-chain data availability and exit fraud risks, which must be carefully mitigated in operational environments.

Sharding addresses scalability by dividing the blockchain state and transaction load across multiple shards that process in parallel. Each shard maintains its own ledger and smart contracts, while a beacon chain coordinates cross-shard communication. In multi-port or multi-agency logistics, sharding enables separate processes (e.g. customs, port authority, logistics firms) to operate concurrently without overloading a single chain. Yet, sharding introduces complexities in data consistency, cross-shard atomicity, and validator assignment, especially when regulatory compliance and chain-of-custody must be preserved.

In tandem with scalability, secure interoperability across blockchain networks is critical in global trade environments where actors may use heterogeneous platforms. The Interledger Protocol (ILP) and Polkadot's Cross-Chain Message Passing (XCMP) are two leading approaches to this challenge. ILP enables value transfers across distinct ledgers without requiring each party to adopt the same blockchain, akin to a routing layer for digital assets. In contrast, Polkadot's XCMP allows secure message passing between parachains via shared security and consensus, enabling composability across decentralized applications.

While these interoperability protocols are technically promising, their maturity and deployment at scale remain limited. For example, ILP's adoption is still emerging outside Ripple-affiliated systems, and XCMP's performance and resilience have not yet been extensively validated in high-stakes, cross-border logistics networks. Thus, while these technologies represent future pathways for modular, secure maritime integration, their current utility should be viewed with measured optimism and critical scrutiny, especially when considering regulatory constraints, liability regimes, and operational reliability in global shipping.

2.2. Integration of blockchain and ZKP in maritime supply chains

ZKP is a cryptographic technique which allows one party to prove the validity of a statement to another without revealing any additional details about the identity of the individual. ZKP plays a vital role in enhancing identity sharing in the blockchain by providing a secure and privacy-preserving mechanism. There are two parties in ZKP, a prover, who demonstrates the truth to the other party, and a verifier, who verifies the truth without revealing additional information (Sun et al. 2021). A valid ZKP protocol follows three phases in the form of interactive in nature:

(1) Witness phase: The prover computes a proof that contains its statement, and then the proof is transmitted to the verifier;

(2) Challenge phase: Several questions are asked by the verifier;
(3) Response phase: The prover answers the questions, and then the verifier uses the given answer to accept or reject the generated proof.

In the phases above, no private information is public. There are two main categories of ZKP: Interactive and non-interactive;

a) Interactive ZKP (Inter-ZKP):

Interactive ZKPs are cryptographic protocols that involve the presence of both parties during the proof process, where a prover aims to convince a verifier, offering him the truth about a statement without revealing any sensitive information about it. Therefore, the interaction between both parties involves multiple rounds of communication, which can be more time-consuming and require significant computational resources.

b) Non-interactive ZKP:

Non-interactive ZKPs are cryptographic protocols with techniques that enable a prover to demonstrate the truth of a statement to a verifier without any continuous interaction between parties. However, developing a reliable non-interactive proof may be more difficult, and in certain types of statements, it may just be impossible to prove in a non-interactive manner (Kuznetsov et al. 2024). The widely used non-interactive ZKPs are: Zk-SNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge), Zk-STARK (Zero-Knowledge Scalable Transparent Argument of Knowledge) and Bulletproofs (Sun et al. 2021).

Figure 1 illustrates the non-interactive ZKP process in three stages: setup, key generation, and verification. In the setup phase, a security parameter (λ) is used to create a circuit (c) defining the proof rules. During key generation, this circuit generates a proving key (V_p) and a verification key (V_v). In the verification phase, the prover uses the proving key to construct a proof (π) for a statement (x) and witness (w), which is sent to the verifier with the statement. The verifier checks the proof using the verification key and either accepts or rejects it. The final proof is stored on a blockchain for transparency. This diagram demonstrates how non-interactive ZKPs enable proof without further interaction, aligning with protocols like Zk-SNARK, Zk-STARK, and Bulletproofs.

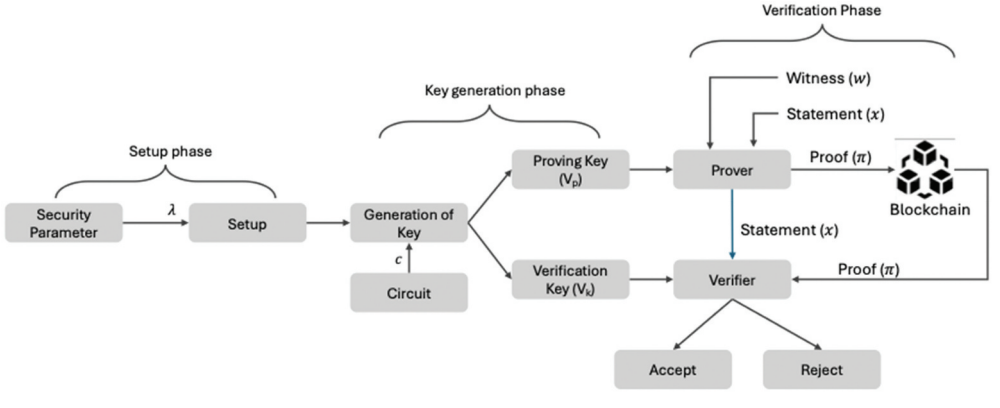

Figure 1. Schematic of non-interactive ZKP workflow.

2.3. Technical challenges of ZKP vs. conventional blockchain

Both conventional blockchains and those enhanced with Zero-Knowledge Proofs (ZKPs) offer transparency, immutability, and distributed trust; however, each faces distinct adoption hurdles in maritime supply chains.

2.3.1. Conventional blockchains

suffer from scalability and latency limits, with low transaction throughput and delayed finality in PoW systems hindering time-critical tasks like customs clearance or just-in-time port scheduling. Energy-intensive consensus raises sustainability concerns, and inherent ledger transparency can expose sensitive trade patterns or shipment volumes.

2.3.2. ZKP-enhanced systems

Mitigate privacy risks by validating transactions without revealing underlying data but add complexity. Proof generation and verification can be computationally costly, increasing latency in high-volume port operations. Some, like zk-SNARKs, require a trusted setup, creating dependencies on secure key management. Circuit design for tasks such as compliance checks without content disclosure demands specialised skills, and legacy port systems may lack APIs or cryptographic capabilities for proof verification.

In comparison, while conventional blockchains may offer higher throughput in certain setups, ZKP-enabled systems deliver stronger privacy at the cost of performance overhead. The optimal choice depends on balancing privacy, speed, sustainability, and integration requirements within regulatory and operational constraints.

3. Literature review

3.1. Cross sectorial applications of blockchain and Zero Knowledge Proofs

Blockchain technology and Zero-Knowledge Proofs (ZKPs) have gained widespread attention for their transformative potential across various industrial and institutional verticals. While initially popularised by cryptocurrencies, these technologies have rapidly evolved into tools for addressing domain-specific issues such as data privacy, operational transparency, trust management, and regulatory compliance. In the financial sector, blockchain enables decentralised finance (DeFi), allowing for real-time settlement, auditability, and programmable money through smart contracts. ZKPs are increasingly employed to preserve the confidentiality of financial transactions while maintaining compliance with anti-money laundering (AML) and know-your-customer (KYC) regulations. Projects such as Zcash and zkSync exemplify the use of non-interactive ZKPs to enable private yet verifiable exchanges on public blockchains. In healthcare, the need to share sensitive medical data across decentralised entities, such as hospitals, insurers, and regulatory bodies, makes privacy-preserving technologies critical. Blockchain has been explored for immutable health record storage and secure data sharing, while ZKPs ensure that patient data can be verified (e.g. vaccination status, medical certification) without revealing personal details, thereby aligning with data protection frameworks like the GDPR.

Supply chain management is another domain where blockchain and ZKPs are synergistically applied. Blockchain ensures end-to-end traceability, provenance verification,

and fraud mitigation in goods movement, from agriculture and pharmaceuticals to consumer electronics. ZKPs add a layer of confidentiality, enabling stakeholders to prove compliance with ethical sourcing, environmental standards, or contractual terms without disclosing sensitive business information. In the public sector, these technologies support secure identity management, verifiable voting systems, and transparent budgeting. For instance, Estonia's e-government initiatives have explored blockchain for registry management, while ZKPs are used to validate voter eligibility without compromising anonymity.

Across these verticals, a common challenge persists: the need to balance transparency with confidentiality, to scale securely without centralised control, and to interoperate across fragmented digital ecosystems. The maritime supply chain, as discussed in subsequent sections, shares many of these concerns, particularly in its reliance on cross-border, multi-stakeholder operations where trust and data security are paramount. Thus, insights from other sectors offer critical lessons and frameworks for the maritime context.

3.2. Maritime supply chain management: an overview

The maritime industry, one of the oldest in goods transportation, remains a vital link between sea and land in global trade. Its core objectives are enhancing efficiency, security, and cost-effectiveness. Maritime supply chains manage the movement of goods via sea routes, a substantial share of global commerce. This involves coordinated planning and transport of maritime containers across a network of ports, regulators, policymakers, researchers, fuel suppliers, shipbuilders, owners, operators, shippers, agents, and authorities (Vujičić et al. 2020).

A key element of this system is its information infrastructure, which manages shipment tracking and planning. It also handles sensitive data, such as bill of lading details, sender/receiver identities, and competitive information like container volumes, which can pose security risks. In recent years, blockchain technology has enabled more secure transmission and protection against tampering and misuse of data, topics explored in subsequent sections.

4. Methodology

4.1. Systematic literature review

The literature review, conducted in November 2024, focused on zero-knowledge proof and blockchain applications in the maritime supply chain. It targeted English-language journal articles from 2020–2024, sourced from Scopus and Web of Science (WOS). Duplicate articles were removed to ensure accuracy, using specific search strategies and inclusion criteria.

4.2. Research questions

The purpose of this study is to review state-of-the-art ZKP applications in maritime SCM, examining how they address privacy, fraud, and efficiency challenges, alongside technical and implementation barriers and identify key factors

affecting maritime supply chain and blockchain implementation in terms of technology usage to improve governance and maritime operations as well as its sustainability:

The research questions are the following:

- How can ZKPs be an improvement in managing container bill of ladings information and its lifecycle?
- What are the main benefits and challenges of implementing ZKPs within existing blockchain systems in the maritime supply chain?
- What are the key adoption factors of ZKPs that enable better overall governance and operations in ports?

4.3. Research strategy

The search terms were selected to find articles that addressed blockchain in the context of 'Blockchain.' Ports, maritime and containers were the population of interest, which were based on the concepts including smart logistics, supply chain, trade operations, identity management, digital identity and secure transaction. 'Blockchain' AND ('Ports' OR 'Maritime' OR 'Containers')) AND (('Smart Logistics' OR 'Supply Chain' OR 'Trade operations' OR 'Identity management' OR 'Digital identity' OR 'Secure transaction') OR ('zero-knowledge proof' OR 'ZKP' OR 'zk-SNARK' OR 'zk-STARK' OR 'bulletproof') was the search query used to identify articles that were relevant to the research. The goal was to identify a wide range of current, relevant publications on the relationship between blockchain technology and ZKP, with an emphasis on maritime supply chain management.

4.4. Study selection and evaluation

The specified query was applied to the databases mentioned in earlier sections, and 133 articles were found altogether, as per Figure 2, below. After removing 42 duplicates, 91 articles were screened. These were analysed by using the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) method, a well-respected approach that guarantees the transparent and systematic evaluation of research papers, as stated in (Page et al. 2021). PRISMA helps researchers assess the quality and relevance efficiently while upholding rigorous standards.

Figure 2 outlines the step-by-step selection process of relevant articles using the PRISMA methodology for the systematic review. The initial search yielded 133 articles from Web of Science and Scopus. After removing 42 duplicates, 91 articles remained for screening. Based on titles, abstracts, and results, 18 were excluded as irrelevant. The remaining 73 articles underwent full-text extraction and detailed review. Four papers were inaccessible and excluded. The 69 accessible full-text articles were then tabulated and categorised in MS Excel by scope and relevance. During this stage, 29 were excluded, 15 for lacking relevant information and 14 for focusing on different populations. The final analysis included 40 articles.

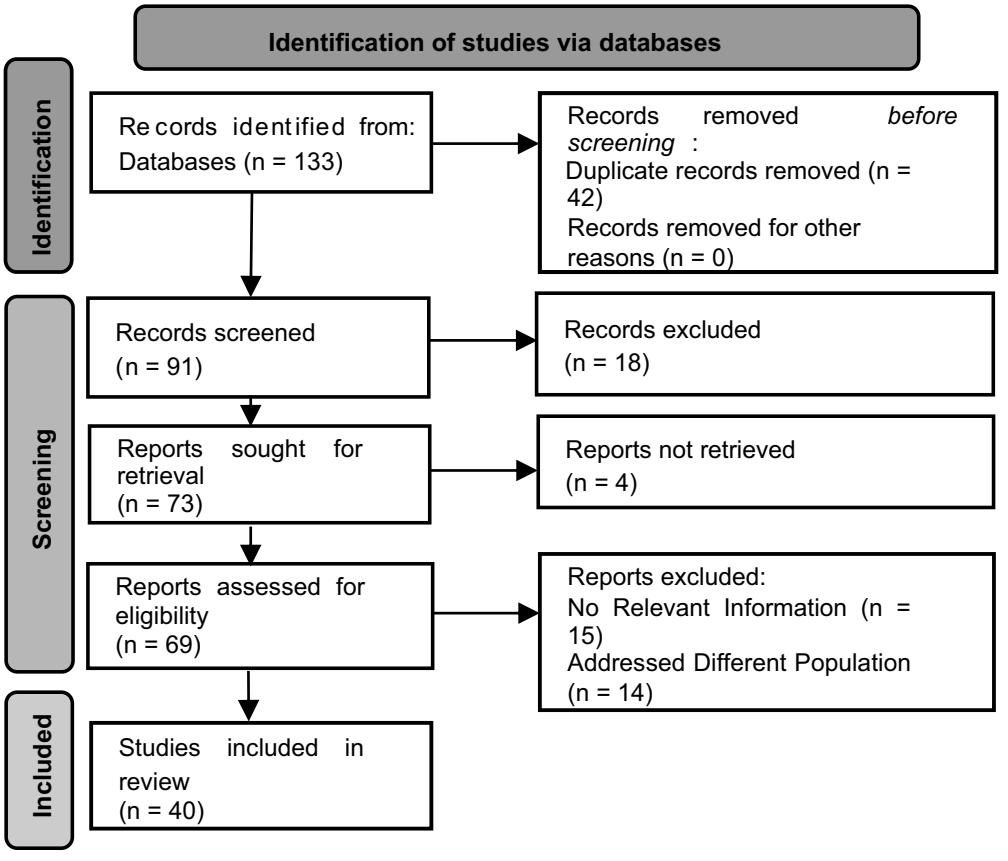

Figure 2. Systematic literature review PRISMA flow diagram.

4.5. Data extraction and synthesis

During the systematic literature review conducted using the PRISMA method, a few tools were essential for managing and storing pertinent data for the articles, namely Zotero, Microsoft Excel, Scopus and WOS. This data encompassed various aspects, including article title, author, publication year, subject area, keywords and abstract. Additionally, to facilitate comprehensive data analysis, a qualitative assessment was performed using these criteria.

5. Research findings

This section provides an overview of information regarding the retrieved articles. The analysis was detailed both in terms of application of use cases in the maritime supply chain with blockchain alone and also with blockchain with Zero Knowledge Proofs. Extended research also included container bill of lading (B/L) management, digitising and securing documentation, improving transparency, and reducing fraud. Yet its potential extends far beyond documentation.

Recent work highlights its role in maritime supply chain financing. (Lu, Lu, and Wang 2024) propose a blockchain-based port logistics finance platform integrating stakeholders for trade finance, invoice factoring, and real-time settlement (J. Li et al. 2024). shows that in perishable goods logistics, blockchain can cut spoilage losses, enhance consumer surplus, and yield net welfare gains despite high initial costs. Complementing port-finance platforms, Blockchain-based Financing Scheme (BFS) targets logistics-company financing with automated lending/repayment logic and node-level privacy controls, showing transferable design patterns for maritime finance ecosystems (Fu et al. 2022). Similarly (Zhao, Liu, and Zhang 2024), create a game model to explain how market uncertainty and blockchain services affect the three models and identify an equilibrium approach.

Contractual automation is another domain (Barahmand et al. 2019). demonstrates automated calculation of demurrage fees, real-time notifications, and conditional payments, reducing disputes and boosting transparency among shippers, carriers, and terminal operators. Understanding the operational performance of vessels provides a quantitative foundation for identifying where blockchain and Zero-Knowledge Proof integration could add the most value. For example, differences in laden ratio and port turnaround across vessel types directly impact the timeliness and predictability of cargo flows (Irannezhad and Faroqi 2023).

Other trials span port operations, bunkering, and marine insurance (Mumtaz, Bergey, and Letch 2024). reports efficiency gains in fuel quality assurance and fraud prevention in bunkering, while (Ben Farah et al. 2024) shows faster claims handling and improved sustainability compliance in marine insurance. In perishable goods traceability (Balci and Surucu-Balci 2021), finds blockchain secures cold chain integrity and offers end-to-end visibility from origin to port delivery. These studies position blockchain as a tool for financing, automation, operational optimisation, and sustainability, complementing its established documentation role.

5.1. Descriptive analysis of publications

Figure 3 depicts the distribution of published documents relevant to blockchain and ZKP applications in maritime SCM, as identified through the systematic literature review, across the years 2020 to 2024. 14% of the total relevant publications are from 2020, and the proportion decreased slightly to 12% in 2021, suggesting a minor reduction in research output focused on this area during that year. A noticeable increase occurred in 2022, with the proportion rising to 20%, indicating a growing interest in the application of these technologies within the maritime sector. This upward trend continued more significantly in 2023, reaching 26%, and peaked at 28% in 2024. This distribution highlights a progressive increase in research attention over the five-year period, reflecting the rising recognition of blockchain and ZKP as critical technologies for addressing privacy, security and efficiency challenges in maritime SCM, as explored in this review.

Figure 4 illustrates the distribution of keywords across the search results obtained during the systematic literature review on blockchain and ZKP applications in maritime SCM. The largest segment, representing 44%, corresponds to keywords related to 'Blockchain in Supply Chain,' indicating a predominant focus on the broader application of blockchain technology within supply chain contexts.

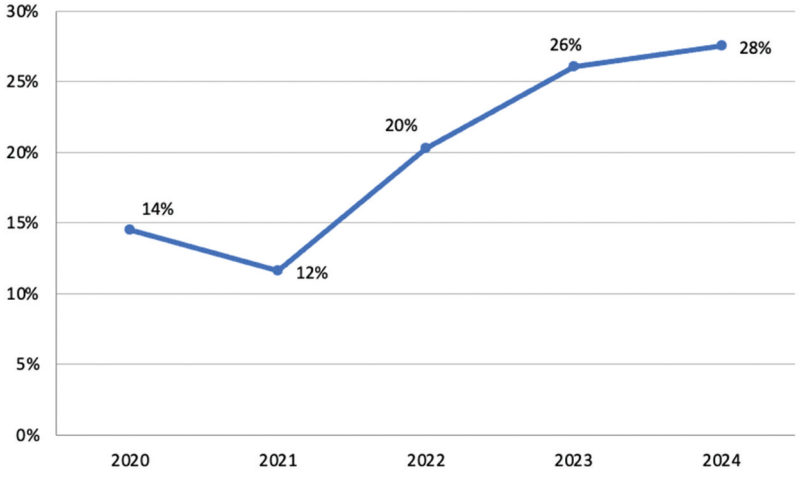

Figure 3. Distribution of published documents by year (2020–2024).

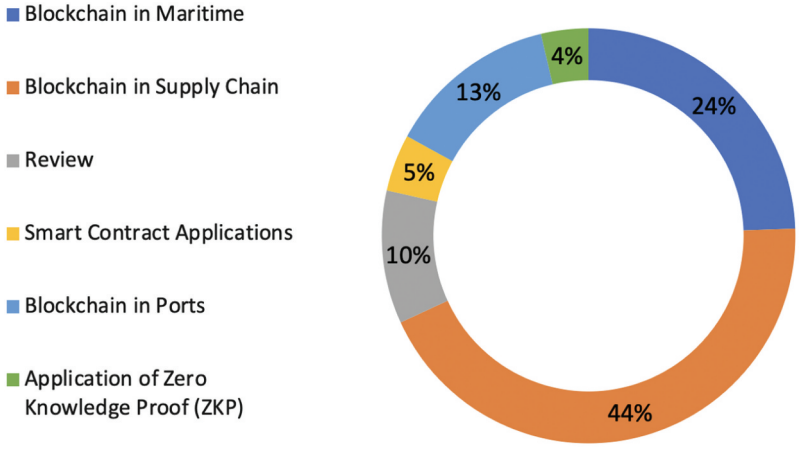

Figure 4. Distribution of keywords in search results.

The second-largest category, at 24%, is 'Blockchain in Maritime,' reflecting significant research interest specifically in maritime applications of blockchain. 'Blockchain in Ports' accounts for 13% of the keywords, highlighting the relevance of port-specific implementations. The 'Application of ZKP' category constitutes 10%, underscoring a growing but still emerging focus on ZKP within this domain. 'Review' articles make up 5% of the keyword distribution, suggesting a smaller yet notable portion of the literature dedicated to synthesising existing research. Lastly, 'Smart Contract Applications' represent 4% of the keywords, indicating a relatively limited but present exploration of smart contracts in this field. This distribution reveals the emphasis on blockchain's role in supply chain and maritime contexts, with a developing interest in ZKP and smart contract applications as complementary technologies.

5.2. Blockchain applications in maritime supply chain management with Zkp's

The analysed papers are aligned with the standard application of blockchain in maritime ports and the addon of ZKP. Table 1 shows the comparative analysis of two options. In the first one, blockchain technology is being used alone, whereas in the second one, it is being integrated with ZKP, based on the different aspects of privacy and security concerns.

As shown in Table 1, integrating ZKP into blockchain-enabled systems enhances security and performance beyond what blockchain alone offers. The proposed system must be robust and address limitations in blockchain-based MSCM, particularly in protecting confidential data and reducing on-chain operations to optimise resources and improve scalability (Sezer, Topal, and Nuriyev 2022; Sun et al. 2021). However, processing large volumes of data in real-time introduces the 'bloat' problem, an issue closely linked to scalability challenges.

Based on recent publications which contributed in the domain of blockchain technology implemented along with ZKP, the key results have been extracted in Table 2:

Blockchain remains an emerging technology with scalability limitations for handling high volumes of transactions and data. Maritime networks demand even greater data capacity, involving detailed operational and logistics information for efficient system management (Saberi et al. 2019). To address scalability, the current reliance on executing all transactions on-chain can be mitigated through ZKP implementation. ZKPs enable off-chain data verification without revealing content, only a proof of accuracy and integrity is shared on-chain, reducing computational load and enhancing scalability.

Table 1. Comparison of the use of blockchain alone and with integration of ZKP.

Aspect	Using blockchain alone	Integrating blockchain with ZKP
Data privacy	Data is transparent to all authorised participants, but sensitive data may be visible Gai et al. (2023).	ZKP ensures sensitive data remains private while still providing a way to verify the proof without revealing the actual data Zhou et al. (2024).
Data security	Provides tamper-proof records using cryptographic hashes but cannot hide specific identities or specifics Samantray and Reddy (2024).	Enhances security by adding cryptographic privacy while preserving data integrity and verification Samantray and Reddy (2024).
Operational efficiency	It manages to record and track the product movement and use the information to ensure operational efficiencies across the whole supply chain network Rasi et al. (2022).	ZKP optimises transaction verification without revealing sensitive information and improves processing time Abid et al. (2024).
Traceability	Each block is permanently connected to the past block and enables end-to-end traceability of products from source to destination, ensuring transparency and accountability across the entire supply chain Abirami Raja Santhi and Muthuswamy (2022).	ZKP enables traceability without revealing ownership or sensitive information about products or entities Zhou et al. (2024).
Data sharing	It enables transparent, secure and efficient data sharing by providing a decentralised platform for real-time Shamsan Saleh (2024).	Protect privacy during the authentication procedure of data sharing systems without revealing any confidential information Feng et al. (2022).
Scalability	High data traffic, high latency and large datasets can strain on blockchain systems Sanka and Cheung (2021).	ZKP enhances blockchain scalability by bundling multiple transactions into a single, lightweight transaction using ZKP and reducing data load on the main chain while maintaining security Sanka and Cheung (2021).

Table 2. Comparison of recent innovations in maritime industries using blockchain and ZKP.

References	Context	Proposed solution
Abid et al. (2024)	Privacy in inter organisational processes	Proposed Self-Sovereign Identity (SSI) systems to enhance privacy by avoiding sensitive data storage on-chain while enabling secure exchanges.
	Secure computations	Enables privacy-preserving operations, such as machine learning on encrypted data using FHE.
	Traceability without privacy compromised	Focusing on the balance between traceability and privacy using ZKP and fully homomorphic encryption.
	Verifiable off-chain computations	ZKP implementation for off-chain verifications, reducing on-chain computational load and preserving privacy.
	Compliance with privacy regulations	Ensure data protection and traceability align with GDPR and similar privacy laws.
	Operational costs	Proposed a private permissioned blockchain and ZKP, which reduced gas costs and maintained traceability and security.
Gai et al. (2023)	Privacy-preserving data sharing	Demonstrated the usability of privacy perseverance in positioning data using blockchain for immutability of shared information.
	Secured transaction data	Proposed Zk-SNARKS for privacy preservation of shared data and identity, which ensured fairness in data sharing and financial fairness.
	System efficiency	Demonstrated low computational costs using Zk-SNARKS, proving feasibility for real-world deployment.
	Security and fairness in transactions	Demonstrated how it protects against double-spending and fair payment mechanisms for data providers and requesters.
Sezer, Topal, and Nuriyev (2022)	Optimal resource usage	Proposed off-chain digital signing to reduce computational costs and time.
	Minimises cost of transactions	Implementation of off-chain signing reduced gas fees by minimising the number of on-chain transactions.
	Scalability	Presented the use of event-based smart contracts and minimised the number of on-chain transactions, supporting scalability features.
	Enhanced traceability	Focused on the secured traceability, achieved through exposing only required parameters.
	Anonymity and transparency	The use of cryptographic digital signatures and verification of transactions with the cryptographic hashes promotes transparency of transactions while ensuring data security.
Ben Farah et al. (2024)	Privacy preservation	Suggested ZKP use along with blockchain-based technologies can help privacy-preserving and data protection in public blockchains.
	51% attack or Goldfinger	Implementation of Proof-of-Stake (PoS) consensus mechanisms can reduce risk.
	Data injection attacks	Implementation of data validation checks and verification of accuracy and authenticity of data in off-chain can reduce resource usage with protection against false data injection.

6. Discussion

Blockchain technology has transformed information exchange by reducing reliance on central authorities through its decentralised, immutable, and distributed ledger system. Its potential to improve transparency, traceability, and trust positions it as a promising solution for addressing inefficiencies in Maritime Supply Chain Management (MSCM) (Lu, Lu, and Wang 2024). However, implementation challenges persist, including adoption barriers, governance issues, data privacy concerns, scalability limits, and high computational and financial costs (H. Li & Ariffin, 2025).

By making transactions transparent, secure, and efficient, blockchain can revolutionise MSCM (Lu, Lu, and Wang 2024). It simplifies longstanding challenges such as paperwork, lack of visibility, and port delays. Digitising key documents like bills of lading ensures tamper resistance and enables immediate sharing with port authorities, streamlining processes and reducing errors (Vujičić et al. 2020). Blockchain also

Table 3. Blockchain implemented ports and their contributions.

Port	Year of implementation and adapted technology	Role and aims	References
Port of Antwerp	2018 (Hyperledger Fabric)	Optimise efficiency in container handling logistic chain by eliminating physical paperwork and tracking hazardous goods	Kim et al. (2024)
Port of Rotterdam	2018 (Hyperledger Fabric)	Use blockchain for logistics and cargo tracking, integrating a paperless network of physical, administrative and financial streams within international shipping and distribution	Kim et al. (2024)
Port of Abu Dhabi	2018	Providing seamless and secure link between stakeholders across the trade community with encrypted documentation in shipping and trade industries	Ben Farah et al. (2024; Shin et al. (2024)
Port of Singapore	2018 (Ethereum)	Establish custom clearances and cargo certificates	Kim et al. (2024); Shin et al. (2024)
Port of Valencia	2018 (Hyperledger Fabric)	Improving supply chain traceability and enhancing data sharing among stakeholders	Kim et al. (2024)

fosters trust among stakeholders by verifying data authenticity, supports real-time shipment tracking, and automates payments through smart contracts, cutting costs and delays (Wang et al. 2022).

Nonetheless, transparency presents a major constraint. Since all network nodes can access stored data, privacy of trade secrets and sensitive business information may be compromised. This poses a challenge for stakeholders who need to protect proprietary data while contributing to a shared ledger (Gai et al. 2023). Zero-Knowledge Proofs (ZKPs) offer a solution by allowing compliance verification without revealing underlying data. This aligns with ESG-driven investor expectations, where auditability is critical but full data disclosure is commercially sensitive (Sedlmeir et al. 2022). ZKPs enable validation of shipment authenticity and customs compliance without exposing pricing, routes, or container details. As per Table 3, we can see diferent Port implementations, its year of implementation and aims, associated to the respective references.

Blockchain implementation also faces challenges such as legacy system integration, high implementation costs, scalability issues and proper availability of skilled professionals (Sun et al. 2021). As stated in research works, implementation of ZKP enables the minimisation of use of computing resources, as they inherit the characteristics of verification and privacy perseverance, hence, the system may operate with low processing costs and better efficiency (R, Chirakarotu Nair, and Kumar Panakalapati 2025).

By implementing blockchain, the collaboration of port terminals and shipping liners can lower costs and improve operational efficiency and economic sustainability. Ports around the world are increasingly adopting blockchain technology. Blockchain-based technologies at ports can enable bureaucracy reduction during operations, especially in developing countries, allowing better visibility of overall port traffic. It optimises operations and sailing times, reducing fuel use and emissions, therefore benefiting the environment (Shashidhara, Chirakarotu Nair, and Kumar Panakalapati 2025). The port of Rotterdam presented a new pilot project based on blockchain to handle containers more safely and efficiently by eliminating the use of a pin code, automating the process.

6.1. Addressing blockchain limitations with ZKP integration

This research explored the integration of Zero-Knowledge Proofs (ZKPs) into blockchain networks to address gaps in maritime supply chains. ZKPs allow verification of blockchain transactions, such as bills of lading, while preserving data privacy and ensuring transparency. Off-chain ZKP computations like zk-SNARKs and Layer-2 solutions (e.g. zk-rollups) reduce main chain load, cutting latency and costs. Bundling multiple verifications into a single proof can lower on-chain data by up to 90% (Sanka and Cheung 2021). This approach not only safeguards data integrity and confidentiality but also improves efficiency by reducing transaction and verification volume. Blockchain alone is insufficient for secure, end-to-end container tracking. ZKPs enhance governance and visibility without compromising sensitive user data.

6.2. Critical reflections on the literature

While the literature on blockchain and Zero-Knowledge Proof (ZKP) applications in supply chains, particularly in the maritime context, has grown considerably in recent years, several important limitations and inconsistencies warrant critical reflection. Many of the reviewed studies emphasise the potential of these technologies to enhance data security, reduce fraud, and streamline operations. However, the credibility and generalisability of these claims often remain uncertain due to methodological shortcomings, limited empirical testing, and unexamined implementation barriers (Ben Farah et al. 2024; Shin et al. 2024).

A recurring trend in the literature is the reliance on conceptual or simulation-based models rather than real-world deployments. For instance, numerous papers propose smart contract frameworks or privacy-preserving protocols using ZKPs without discussing the operational complexity, integration costs, or institutional inertia that often hinder adoption in port and shipping systems (Balci and Surucu-Balci 2021). Moreover, few studies engage with stakeholder perspectives, legal constraints, or performance data from pilot projects, leaving a gap between technological optimism and operational reality (Ben Farah et al. 2024).

Another issue concerns the overstatement of security guarantees. While blockchain and ZKPs are frequently framed as inherently secure, there is limited discussion of attack surfaces such as endpoint vulnerabilities, key management, or denial-of-service risks (Sun et al. 2021). Similarly, claims about interoperability solutions, such as those involving ILP or XCMP, often neglect to address the immature tooling, governance ambiguity, and lack of standardised auditability that complicate multi-chain integrations in fragmented regulatory environments (Jović et al. 2020; J. Li et al. 2024).

Furthermore, the scalability problem remains understated in several studies. Although Layer-2 solutions and sharding are cited as remedies, few sources examine the trade-offs involved, such as increased complexity, new trust assumptions, and off-chain data availability challenges (Durán et al. 2024; Khan, Jung, and Hashmani 2021). These limitations are particularly salient in global maritime supply chains where legal liability, compliance, and multi-jurisdictional coordination introduce unique barriers to decentralised innovation.

Finally, the review revealed a need for greater critical engagement with empirical lessons from adjacent sectors such as finance, healthcare, and manufacturing. Although these fields offer valuable precedents, their infrastructural, legal, and economic contexts differ from maritime logistics. As such, caution is required when extrapolating results from these domains without nuanced contextual analysis (Chang, Lakovou, and Shi 2019).

While the literature offers promising blueprints for blockchain-ZKP integration in maritime logistics, much of it remains conceptual, fragmented, and insufficiently validated. Future research must prioritise empirical rigor, cross-sectoral comparison, and critical realism in evaluating not only what these technologies can do in theory, but also what they have demonstrably achieved in practice.

6.3. Technical challenges and reported benefits

While much of the literature remains conceptual, a subset of studies and pilot implementations report practical insights into the deployment of blockchain and Zero-Knowledge Proofs (ZKPs) in supply chains and adjacent sectors. This section synthesises these insights, highlighting both the benefits realised in practice and the technical challenges encountered during implementation.

Across multiple case studies and technical evaluations, several recurring benefits of blockchain-ZKP integration have emerged. The most consistently cited advantage is enhanced data integrity and traceability, especially in multi-tier supply chains where product origin and movement verification are critical. Blockchain-based tracking systems have been shown to reduce verification times for cargo provenance and customs documentation, while also enhancing accountability in container handovers (Irannezhad and Faroqi 2023; Shin et al. 2024). In pilot projects, smart contracts have streamlined document processing, reducing clearance times and human error in bill-of-lading workflows.

ZKPs specifically contribute by enabling confidential verification, allowing stakeholders to prove compliance with contractual or regulatory terms without revealing proprietary or sensitive information. This has been tested in scenarios involving know-your-customer (KYC) validation, origin certifications, and audit automation, with reported success in balancing transparency with privacy, a major concern in competitive logistics environments (Major, Buchanan, and Ahmad 2020; Sun et al. 2021).

Technical and Operational Challenges. Despite these benefits, implementation efforts often encounter significant obstacles. A major concern is scalability, especially when applying ZKP-enhanced blockchains to high-frequency or data-intensive processes such as container monitoring or environmental compliance tracking. Layer-2 solutions and sharding offer partial mitigation but introduce new trust assumptions and coordination complexities (Khan, Jung, and Hashmani 2021; Sarfaraz, Chakrabortty, and Essam 2023).

Another prominent issue is interoperability. In real-world deployments, actors frequently operate on different platforms (e.g. port authorities, customs, shippers), necessitating cross-chain communication. However, technologies like ILP and XCMP, while promising, remain underdeveloped in practice and lack standardised protocols for maritime-specific integration (Jović et al. 2020; L. Li and Zhou 2025).

Furthermore, computational overhead associated with ZKP generation and verification can be substantial. For constrained devices or edge environments (e.g. onboard systems, IoT gateways), these requirements may exceed available processing capacity, raising concerns about performance and system responsiveness (Sarfaraz, Chakrabortty, and Essam 2023).

Institutional and Governance Constraints. Beyond technical barriers, several studies highlight organizational resistance, lack of regulatory clarity, and the need for clear data governance models. In particular, stakeholders often hesitate to adopt immutable ledgers without established recourse mechanisms or liability frameworks in case of data errors or fraud. Pilot failures are frequently linked to unclear ownership of digital infrastructure, fragmented stakeholder incentives, and insufficient user training (Balci and Surucu-Balci 2021; H. Lin 2024).

The literature reveals that while the benefits of blockchain and ZKP systems are tangible, particularly in enhancing transparency, automation, and privacy, successful implementation is highly contingent on contextual factors. These include the technical infrastructure of the supply chain, stakeholder alignment, legal frameworks, and sector-specific process complexity. Thus, future research and development efforts must balance technical innovation with operational pragmatism, ensuring that proposed systems are not only secure and private but also usable, scalable, and governable in real-world maritime logistics

6.4. Real world applications and key insights

Based on an in-depth evaluation of real-world applications, ZKP can act as the disrupting catalyst that this industry needs. It assures that all stakeholders acquire transparency and privacy, with assurance that such information pertaining to trade documents is genuine or in regulatory compliance matters (Ben Farah et al. 2024). Customs can clear shipments to meet regulatory standards without accessing proprietary trade information, and shipping companies can verify ownership or contractual arrangements without divulging competitive information. This is aligned with digitisation initiatives and legislation requirements in order to create a compliant solution for port authorities and its regulatory entities.

6.5. Benefits and future potential

Some real-life benefits of integrating ZKP into blockchain-based maritime supply chains include:

- Improved privacy and security: ZKP ensures confidentiality of sensitive information while still enabling verification of authenticity and compliance;
- Improved scalability: Off-chain computations that ZKP protocols provide keep the load off blockchain networks, thus improving scalability to a greater throughput of transactions with much efficiency;
- Operational efficiency: The use of smart contracts and ZKP reduces delays and intermediaries in the verification processes, making maritime logistics smoother;

- Fraud prevention and traceability: Immutability from blockchain and the privacy-preserving properties of ZKP, when put together, strengthen fraud detection and end-to-end traceability;
- Compliance: ZKP provides a means wherein systems could release select information of data; the case is GDPR.

6.6. Adoption factors

The adoption of blockchain in maritime supply chains is driven by intertwined technological, organisational, environmental, and economic factors.

Economically, significant upfront costs arise from infrastructure, training, and integration with legacy port systems. These must be balanced against long-term gains such as reduced administrative overhead, fewer documentation disputes, faster settlements, and better asset utilisation. In high-value or time-sensitive cargoes, such as perishables (J. Li et al. 2024), shows that improved visibility and automation can cut spoilage and optimise logistics, outweighing capital costs.

Cybersecurity remains a barrier. Conventional blockchains face risks like 51% attacks, smart contract flaws, oracle data injection, and metadata leakage. ZKP-enabled systems enhance privacy by validating transactions without exposing details, but add complexity through proof verification overhead, trusted setup risks, and the need for advanced cryptographic skills. Blockchain and ZKP adoption needs a multi-dimensional transformation requiring investment, governance, and enabling legal frameworks.

6.7. Challenges and the way forward

Despite their promise, implementing blockchain and ZKP in MSCM faces challenges, particularly in integrating with existing systems. Major obstacles include high computational demands, legacy system compatibility, high implementation costs, and the absence of standardised protocols. Additionally, regulatory uncertainties around smart contracts and blockchain systems must be addressed for broader adoption (H.-F. Lin 2025).

Future research should focus on optimising ZKP protocols by reducing computational complexity, employing hardware accelerators, and standardising data formats and communication protocols. Pilot projects and real-world case studies can help identify practical solutions. Collaborative efforts among transport companies, port authorities, policymakers, and technology providers are essential for innovation and standardisation.

The integration of blockchain with ZKPs represents a significant advance in tackling privacy, scalability, and efficiency challenges in maritime supply chains. It holds the potential to transform the industry through secure, transparent, and sustainable trade operations.

7. Conclusion and future direction

In Maritime Supply Chain Management (MSCM), blockchain has emerged as a key innovation to address inefficiencies, lack of transparency, and trust issues. However, its limitations, such as scalability, high computational costs, and privacy concerns, necessitate advanced privacy-preserving mechanisms. Zero-Knowledge Proofs (ZKPs) offer

a valuable complement, enabling secure data verification without disclosing sensitive information.

Drawing on real-world MSCM applications, this study highlights the potential of integrating blockchain with ZKP to optimise maritime logistics. Key use cases include privacy-preserving traceability, secure document verification, fraud prevention, and regulatory compliance. ZKP and off-chain computations reduce blockchain's computational burden through lightweight cryptographic proofs, enhancing scalability and protecting sensitive trade data.

Effective implementation of ZKP-enabled blockchain in MSCM requires stakeholder collaboration, alignment of suitable technologies, and attention to legal and regulatory frameworks. Advances in cryptography and blockchain architecture offer promising solutions for the sector.

Integrating ZKP can transform MSCM into a more secure, efficient, and privacy-compliant trade environment, reshaping governance processes. This study underlines the need to overcome technical, operational, and legal barriers for broader adoption. Future research should prioritise standardised protocols, lightweight nodes for edge networks, optimised ZKP algorithms for real-time use, and scalable deployment strategies to fully realise blockchain-ZKP potential.

While this study offers a comprehensive review of blockchain's potential in maritime supply chains, it is not without limitations. First, the absence of empirical validation restricts the ability to assess the actual performance of blockchain solutions in operational settings; however, that validation was out of scope for this research. Second, the findings are generalised across diverse global contexts, which may overlook region-specific regulatory, infrastructural, or organisational constraints. Nonetheless, with the appropriate adjustments, it can be beneficial to many different contexts. Future research could address these limitations through empirical case studies and comparative analyses across different maritime regions and work should include proof-of-concept projects to test governance models and the robustness of blockchain-ZKP systems. Although blockchain is already in use at some maritime ports, widespread adoption remains limited. Layer-2 solutions must also improve integration and user interfaces to enhance usability and adoption.

Disclosure statement

No potential conflict of interest was reported by the author(s).

References

Abid, A., S. Cheikhrouhou, S. Kallel, and M. Jmaiel. 2024. "A Privacy-Preserving Traceability System for Self-Sovereign Identity-Based Inter-Organizational Business Processes." *Computer Standards and Interfaces* 92:92. https://doi.org/10.1016/j.csi.2024.103930.

Abirami Raja Santhi, P. M., and P. Muthuswamy. 2022. "Influence of Blockchain Technology in Manufacturing Supply Chain and Logistics." *Logistics* 6 (15): 15. https://doi.org/10.3390/logistics6010015.

Bai, X., H. Jia, and M. Xu. 2024. "Identifying Port Congestion and Evaluating Its Impact on Maritime Logistics." *Maritime Policy & Management* 51 (3): 345–362. https://doi.org/10.1080/03088839.2022.2135036.

Balci, G., and E. Surucu-Balci. 2021. "Blockchain Adoption in the Maritime Supply Chain: Examining Barriers and Salient Stakeholders in Containerized International Trade." *Transportation Research Part E: Logistics & Transportation Review* 156:102539. https://doi.org/10.1016/j.tre.2021.102539.

Barahmand, S., S. Ghandeharizadeh, B. Krishnamachari, D. Lugones, R. Nambiar, and T. Slaats. 2019. "Second International Symposium on Foundations and Applications of Blockchain."

Ben Farah, M., Y. Ahmed, H. Mahmoud, S. Shah, M. Al-Kadri, S. Taramonli, X. Bellekens, R. Abozariba, M. Idrissi, and A. Aneiba. 2024. "A Survey on Blockchain Technology in the Maritime Industry: Challenges and Future Perspectives." *Future Generation Computer Systems-The International Journal of Escience* 157:618–637. https://doi.org/10.1016/j.future.2024.03.046.

Chang, Y., E. Lakovou, and W. Shi. 2019. *Blockchain in Global Supply Chains and Cross Border Trade: A Critical Synthesis of the State-of-The-Art, Challenges and Opportunities*. https://www.tandfonline.com/doi/epdf/10.1080/00207543.2019.1651946?needAccess=true .

Chen, S., S. Brahma, J. Mackay, C. Cao, and B. Aliakbarian. 2020. "The Role of Smart Packaging System in Food Supply Chain." *Journal of Food Science* 85 (3): 517–525. https://doi.org/10.1111/1750-3841.15046.

Shashidhara, R., R. Chirakarotu Nair, and P. Kumar Panakalapati. 2025. "Promise of Zero-Knowledge Proofs (ZKPs) for Blockchain Privacy and Security: Opportunities, Challenges, and Future Directions." *Security and Privacy* 8 (1): e461. https://doi.org/10.1002/spy2.461.

Durán, C., A. K. Yazdi, I. Derpich, and Y. Tan. 2024. "Leveraging Blockchain for Maritime Port Supply Chain Management Through Multicriteria Decision Making." *Mathematics* 12 (10): 1511. https://doi.org/10.3390/math12101511.

Feng, T., P. Yang, C. Liu, J. Fang, and R. Ma. 2022. "Blockchain Data Privacy Protection and Sharing Scheme Based on Zero-Knowledge Proof." *Wireless Communications and Mobile Computing* 2022 (1): 1040662. https://doi.org/10.1155/2022/1040662.

Fu, J., B. Cao, X. Wang, P. Zeng, W. Liang, and Y. Liu. 2022. "BFS: A Blockchain-Based Financing Scheme for Logistics Company in Supply Chain Finance." *Connection Science* 34 (1): 1929–1955. https://doi.org/10.1080/09540091.2022.2088698.

Gai, K., H. Tang, G. Li, T. Xie, S. Wang, L. Zhu, and K.-K. R. Choo. 2023. "Blockchain-Based Privacy-Preserving Positioning Data Sharing for IoT-Enabled Maritime Transportation Systems." *IEEE Transactions on Intelligent Transportation Systems* 24 (2): 2344–2358. https://doi.org/10.1109/TITS.2022.3190487.

Haouari, M., M. Mhiri, M. El-Masri, and K. Al-Yafi. 2022. "A Novel Proof of Useful Work for a Blockchain Storing Transportation Transactions." *Information Processing & Management* 59 (1): 102749. https://doi.org/10.1016/j.ipm.2021.102749.

Hu, Q., B. Yan, Y. Han, and J. Yu. 2021. "An Improved Delegated Proof of Stake Consensus Algorithm." *Procedia Computer Science* 187:341–346. https://doi.org/10.1016/j.procs.2021.04.109.

Irannezhad, E., and H. Faroqi. 2023. "Addressing Some of Bill of Lading Issues Using the Internet of Things and Blockchain Technologies: A Digitalized Conceptual Framework." *Maritime Policy & Management* 50 (4): 428–446. https://doi.org/10.1080/03088839.2021.1930223.

Jia, H., and R. Adland. 2019. "Smart Contracts and Demurrage in Ocean Transportation." FAB 2019 Proceedings of the International Association of Maritime Economists (IAME) Conference, 35–52. https://scfab.github.io/2019/assets/papers/FAB2019Proceedings.pdf.

Jović, M., E. Tijan, D. Žgaljić, and S. Aksentijević. 2020. "Improving Maritime Transport Sustainability Using Blockchain-Based Information Exchange." *Sustainability* 12 (21), Article 21. 8866. https://doi.org/10.3390/su12218866.

Khan, D., L. T. Jung, and M. A. Hashmani. 2021. "Systematic Literature Review of Challenges in Blockchain Scalability." *Applied Sciences* 11 (20): 9372. https://doi.org/10.3390/app11209372.

Kim, H., Z. Xiao, X. Zhang, X. Fu, and Z. Qin. 2024. *Rethinking Blockchain Technologies for the Maritime Industry: An Overview of the Current Landscape*. https://www.mdpi.com/1999-5903/16/12/454.

Kuznetsov, O., E. Frontoni, K. Kuznetsova, R. Shevchuk, and M. Karpinski. 2024. "NFT Technology for Enhanced Global Digital Registers: A Novel Approach to Tokenization." *Future Internet* 16 (7): 252. https://doi.org/10.3390/fi16070252.

Li, H., and S. B. Ariffin. 2025. "Blockchain-Enabled Supply Chain Finance: A Bibliometric Review and Literature Review *Appl. Math. Inf. Sci.* 19 (5): 1129–1140. https://doi.org/10.18576/amis/190513.

Li, J., D. Han, T. Weng, H. Wu, K. Li, and A. Castiglione. 2024. "A Secure Data Storage and Sharing Scheme for Port Supply Chain Based on Blockchain and Dynamic Searchable Encryption." *Computer Standards and Interfaces* 91. https://doi.org/10.1016/j.csi.2024.103887.

Li, L., and J. Zhou. 2025. "Blockchain Effects and Investment Strategies in the Maritime Supply Chain Under Perishable Goods Loss." *Systems* 13 (3): 196. https://doi.org/10.3390/systems13030196.

Lin, H. 2024. "Blockchain Adoption in the Maritime Industry: Empirical Evidence from the Technological-Organizational-Environmental Framework." *Maritime Policy & Management* 51 (7): 1474–1496. https://doi.org/10.1080/03088839.2023.2175063.

Lin, H.-F. 2025. "Examining the Determinants of Blockchain Technology-Enabled Maritime Supply Chain System Adoption Intention: Does Market Turbulence Play a Moderating Role?" *Marine Policy* 174:106616. https://doi.org/10.1016/j.marpol.2025.106616.

Liu, J., H. Zhang, and L. Zhen. 2023. "Blockchain Technology in Maritime Supply Chains: Applications, Architecture and Challenges." *International Journal of Production Research* 61 (11): 3547–3563. https://doi.org/10.1080/00207543.2021.1930239.

Lu, B., H. Lu, and H. Wang. 2024. "Design and Value Analysis of the Blockchain-Based Port Logistics Financial Platform." *Maritime Policy & Management* 51 (6): 1037–1061. https://doi.org/10.1080/03088839.2023.2205870.

Major, W., W. J. Buchanan, and J. Ahmad. 2020. "An Authentication Protocol Based on Chaos and Zero Knowledge Proof." *Nonlinear Dynamics* 99 (4): 3065–3087. https://doi.org/10.1007/s11071-020-05463-3.

Mentzer, J. T., W. DeWitt, J. S. Keebler, S. Min, N. W. Nix, C. D. Smith, and Z. G. Zacharia. 2001. "Defining Supply Chain Management." *Journal of Business Logistics* 22 (2): 1–25. https://doi.org/10.1002/j.2158-1592.2001.tb00001.x.

Morais, E., T. Koens, C. van Wijk, and A. Koren. 2019. "A Survey on Zero Knowledge Range Proofs and Applications." *SN Applied Sciences* 1 (8): 946. https://doi.org/10.1007/s42452-019-0989-z.

Mumtaz, U. U., P. Bergey, and N. Letch. 2024. "Assessing the Role of Blockchain Technology for Marine Bunkering Operations – a Case Study of Task Technology Fit." *Marine Policy* 159:105909. https://doi.org/10.1016/j.marpol.2023.105909.

Nakamoto, S. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System." Retrieved from: https://bitcoin.org/bitcoin.pdf.

Nguyen, S., P. Chen, and Y. Du. 2023. "Blockchain Adoption in Container Shipping: An Empirical Study on Barriers, Approaches, and Recommendations." *Marine Policy* 155. https://doi.org/10.1016/j.marpol.2023.105724.

Page, M. J., J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, L. Shamseer, et al. 2021. "The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews." *BMJ* 372:n71. https://www.bmj.com/content/372/bmj.n71.short.

Pu, S., and J. S. L. Lam. 2021. "Blockchain Adoptions in the Maritime Industry: A Conceptual Framework." *Maritime Policy & Management* 48 (6): 777–794. https://doi.org/10.1080/03088839.2020.1825855.

Rasi, R. Z., U. S. B. Rakiman, R. Z. R. M. Radzi, N. R. Masrom, and V. P. K. Sundram. 2022. "A Literature Review on Blockchain Technology: Risk in Supply Chain Management." *IEEE Engineering Management Review* 50 (1): 186–200. https://doi.org/10.1109/EMR.2021.3133447.

Saberi, S., M. Kouhizadeh, J. Sarkis, and L. Shen. 2019. "Blockchain Technology and Its Relationships to Sustainable Supply Chain Management." *International Journal of Production Research* 57 (7): 2117–2135. https://doi.org/10.1080/00207543.2018.1533261.

Salzano, F., L. Marchesi, R. Pareschi, and R. Tonelli 2024. "Integrating Blockchain Technology within an Information Ecosystem." *Blockchain: Research and Applications* 5 (4). https://doi.org/10.1016/j.bcra.2024.100225), 100225.

Samantray, B. S., and K. H. K. Reddy. 2024. "A Novel Secure Supply Chain for Smart Healthcare Systems: An Approach to Leverage Blockchain, Keccak-256, and ZKP for Drug Safety Assurance." *Peer-to-Peer Networking and Applications* 18 (1): 16. https://doi.org/10.1007/s12083-024-01832-6.

Sanka, A. I., and R. C. C. Cheung. 2021. "A Systematic Review of Blockchain Scalability: Issues, Solutions, Analysis and Future Research." *Journal of Network and Computer Applications* 195:103232. https://doi.org/10.1016/j.jnca.2021.103232.

Sarfaraz, A., R. K. Chakrabortty, and D. L. Essam. 2023. "The Implications of Blockchain-Coordinated Information Sharing within a Supply Chain: A Simulation Study." *Blockchain: Research and Applications* 4 (1): 100110. https://doi.org/10.1016/j.bcra.2022.100110.

Sedlmeir, J., J. Lautenschlager, G. Fridgen, and N. Urbach. 2022. "The Transparency Challenge of Blockchain in Organizations." *Electronic Markets* 32 (3): 1779–1794. https://doi.org/10.1007/s12525-022-00536-0.

Sezer, B. B., S. Topal, and U. Nuriyev. 2022. "TPPSUPPLY: A Traceable and Privacy-Preserving Blockchain System Architecture for the Supply Chain." *Journal of Information Security & Applications* 66:66. https://doi.org/10.1016/j.jisa.2022.103116.

Shamsan Saleh, A. M. 2024. "Blockchain for Secure and Decentralized Artificial Intelligence in Cybersecurity: A Comprehensive Review." *Blockchain: Research and Applications* 5 (3): 100193. https://doi.org/10.1016/j.bcra.2024.100193.

Shin, S., Y. Wang, S. Pettit, and W. Abouarghoub. 2024. "Blockchain Application in Maritime Supply Chain: A Systematic Literature Review and Conceptual Framework." *Maritime Policy & Management* 51 (6): 1062–1095. https://doi.org/10.1080/03088839.2023.2234896.

Sun, X., F. R. Yu, P. Zhang, Z. Sun, W. Xie, and X. Peng. 2021. "A Survey on Zero-Knowledge Proof in Blockchain." *IEEE Network* 35 (4): 198–205. https://doi.org/10.1109/MNET.011.2000473.

Uddin, M., A. Khalique, A. K. Jumani, S. S. Ullah, and S. Hussain. 2021. "Next-Generation Blockchain-Enabled Virtualized Cloud Security Solutions: Review and Open Challenges." *Electronics* 10 (20): 2493. https://doi.org/10.3390/electronics10202493.

Vujičić, S., N. Hasanspahić, M. Car, and L. Čampara. 2020. "Distributed Ledger Technology as a Tool for Environmental Sustainability in the Shipping Industry." *Journal of Marine Science and Engineering* 8 (5), Article 5. 366. https://doi.org/10.3390/jmse8050366.

Wang, Y., P. Chen, B. Wu, C. Wan, and Z. Yang. 2022. "A Trustable Architecture Over Blockchain to Facilitate Maritime Administration for MASS Systems." *Reliability Engineering and System Safety* 219:108246. https://doi.org/10.1016/j.ress.2021.108246.

Wong, D. 2021. *Real-World Cryptography*. Simon and Schuster.

Zhao, H., J. Liu, and G. Zhang. 2024. "Blockchain-Driven Operation Strategy of Financial Supply Chain Under Uncertain Environment." *International Journal of Production Research* 62 (8): 2982–3002. https://doi.org/10.1080/00207543.2023.2190816.

Zhou, L., A. Diro, A. Saini, S. Kaisar, and P. C. Hiep. 2024. "Leveraging Zero Knowledge Proofs for Blockchain-Based Identity Sharing: A Survey of Advancements, Challenges and Opportunities." *Journal of Information Security & Applications* 80:103678. https://doi.org/10.1016/j.jisa.2023.103678.