SECURING MARITIME OPERATIONS: ENHANCING FRAUD PREVENTION WITH BLOCKCHAIN AND NFC TECHNOLOGY

Rajendren Subramaniam[1], ***Teh Ying Wah***[2], ***Vimala Balakrishnan***[3*,4]

[1,2,3]Department of Information Systems, Faculty of Computer Science & Information Technology, Universiti Malaya

[4]Department of Computer Science and Engineering, Korea University, Seoul, Korea

Emails: rajendren@um.edu.my[1], tehyw@um.edu.my[2], vimala.balakrishnan@um.edu.my[3*] (Corresponding author)

ABSTRACT

Maritime port operations face escalating fraud risks, specifically cargo theft and document falsification, driven by fragmented paper-based processes and information silos. Conventional detection mechanisms lack real-time authentication for high-volume throughput. This study proposes an NFC-Blockchain integration framework that combines Near Field Communication with blockchain to create a digital twin for physical assets. Moving beyond descriptive analyses, this paper details a functional prototype from NFC tag initialization to smart contract execution on a Layer 1 blockchain, establishing a concrete system workflow for secure asset tracking and document verification. A mixed-methods design was utilized, combining a quantitative survey of 423 port operators with five expert interviews and case study analysis. Results reveal a significant readiness gap: while blockchain awareness is high (70%), NFC familiarity is low (35%), with adoption constrained by high implementation costs and technical expertise deficits (both 55%). The proposed architecture demonstrates that integrating these technologies automates compliance via smart contracts and provides tamper-proof real-time traceability. These findings offer actionable technical and strategic guidance for port authorities to mitigate fraud through decentralized infrastructure.

Keywords: Blockchain technology; Fraud prevention; Implementation barriers; NFC; Port operations

1.0 INTRODUCTION

1.1 Background

Fraud in port operations has emerged as a significant global concern due to its financial, security, and logistical ramifications. Traditional methods of fraud detection are proving inadequate against increasingly sophisticated schemes, including cargo theft, document forgery, smuggling, and internal collusion, which compromise supply chain integrity [1]. While the industry is turning to innovative technologies such as blockchain and NFC, the successful implementation of these tools depends on moving beyond generic adoption toward specific technical architectures [2]. Global trade's vast scale and fragmented oversight offer extensive opportunities for exploitation amid high cargo volumes [3]. Fraud mitigation is further complicated by the involvement of multiple disparate actors, including customs, shipping lines, and port operators [4], [5]. Key technical gaps such as inadequate security protocols, reliance on paper-based systems, and lack of standardized verification diminish transparency and allow fraudulent practices to persist undetected [6], [7]. Addressing these vulnerabilities requires a comprehensive digitization of documentation and the enhancement of security infrastructure to ensure operational integrity.

1.2 Blockchain Technology

Blockchain is a decentralized, cryptographically formatted immutable ledger. We utilize this highly secured database to provide a transformative tool for maritime fraud prevention by creating chronological, tamper-proof records [8]. Unlike centralized databases, its distributed architecture eliminates "single points of failure," requiring network consensus for data alterations to ensure long-term integrity. Through cryptographic hashing and digital signatures, the system secures data exchange and validates transaction authenticity via consensus mechanisms (e.g., Proof of Work/Stake), effectively mitigating document forgery [9]. Fig. 1 illustrates a decentralized workflow for handling port transactions using blockchain technology. The process begins with a Port transaction request, which is then bundled into a Port transaction block representing a group of pending data or assets [10], [11]. This block is then broadcast across a distributed network, where independent Nodes validate the port transaction to ensure its authenticity and compliance with network rules [12]. Once consensus is reached, the new block is added to the blockchain, creating a permanent and immutable record of the event. Finally, the cycle concludes with the Port transaction completed, signalling that the exchange or data update has been successfully verified and finalized [13]. These features enable transparent product provenance and utilize smart contracts to automate agreements, reducing reliance on intermediaries and minimizing contractual fraud.

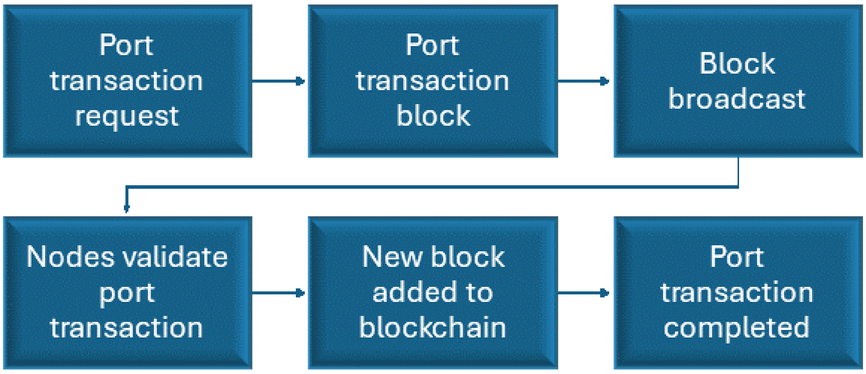

Fig. 1: Blockchain Process in Port Operation

1.3 NFC Technology

NFC is a short-range wireless connectivity technology that enables the secure exchange of data between devices in close proximity, typically within a few centimetres. In the context of port management, this technology facilitates precise real-time asset tracking and physical security enhancement [14], [15]. As illustrated in Fig. 2, embedding NFC tags on containers and vehicles allows port authorities to monitor logistical movements with high granularity, which optimizes inventory management and mitigates risks associated with theft or loss. Beyond asset tracking, NFC-based access control systems manage entry to restricted maritime zones via encrypted cards or mobile devices, significantly strengthening physical security perimeters [16]. Furthermore, the technology streamlines personnel authentication through identification badges containing digital signatures or biometric data, ensuring strict compliance with international security protocols. In cargo management, tags attached to items store critical metadata such as origin, destination, and handling instructions while enabling seamless monitoring at transit checkpoints [14]. Despite these operational benefits, successful integration requires strategic investment in NFC-enabled readers across key operational zones and the deployment of compatible software to ensure interoperability with existing port infrastructure [17].

Fig. 2: Sample NFC usage in port operation

1.4 Problem Formalization: The Security Gap in Maritime Logistics

The primary challenge in maritime security lies in systemic vulnerabilities rooted in fragmented oversight and a persistent reliance on paper-based processes [18]. This research formalizes the existing security gap into three primary technical deficiencies that facilitate fraudulent activity: the physical-digital disconnect, centralized information silos, and latency in real-time authentication [19].

First, the physical-digital disconnect refers to the lack of a cryptographic link between a digital ledger record and the actual physical cargo [20]. While existing blockchain solutions effectively secure digital data, they often fail to provide a tamper-proof mechanism to verify that the digital twin accurately represents the state of the physical asset. This results in a visibility void where cargo theft or substitution can persist undetected because the ledger remains consistent even if the physical asset has been compromised [21].

Second, centralized information silos represent a critical vulnerability in traditional port management systems (PMS) [22]. These systems rely on centralized databases that function as single points of failure, where a breach of administrative credentials can lead to unauthorized data alteration across the entire manifest. The lack of a decentralized consensus mechanism means that fraudulent changes to shipping documents can be obscured within internal records, preventing cross-party verification [23].

Third, latency in real-time authentication occurs due to the manual nature of current verification cycles. These delays create intervals of unmonitored activity within the supply chain, often referred to as operational dark windows [24]. During these periods, fraudulent activities such as smuggling or document falsification can occur without triggering system alerts, as the authentication of the goods only happens at fixed, delayed intervals rather than through continuous, automated proximity-based checks [25].

1.5 Proposed Technical Solution: NFC-Blockchain Integration

To address these challenges, this study proposes an integrated framework utilizing NFC as the physical verification layer and the Blockchain as the immutable data layer. As illustrated in the process flow in Fig. 1, blockchain provides a decentralized, tamper-proof ledger for secure transaction tracking. Complementing this, NFC facilitates real-time, secure data exchange between proximate devices; by embedding NFC tags on cargo containers, port authorities can monitor movement with high precision. This integration creates a "digital twin" for physical assets, where a unique hardware-encrypted identifier is bound to a specific smart contract, ensuring that the ledger accurately reflects the physical state of the cargo at all times [2], [26].

1.6 Research Aim and Contributions

The primary aim of this research is to investigate and validate the potential of this integrated architecture to enhance fraud prevention and operational security within port environments. Moving beyond previous descriptive studies, this paper contributes a concrete system architecture for binding physical NFC Unique Identifiers to a Layer 1 blockchain (Zetrix) [27], alongside a technical prototype validation that demonstrates the initialization and tracking of assets. Furthermore, these technical findings are supported by an empirical analysis of 423 port operators and expert interviews, providing a comprehensive view of industry readiness and the specific technical barriers to adoption.

2.0 METHODOLOGY

This research employs a mixed-methods research design, integrating empirical data collection with Design Science Research (DSR) principles to develop and validate a technical solution [23]. The methodology is structured into four phases: (i) an empirical quantitative survey to identify industry gaps; (ii) qualitative expert interviews to refine system requirements; (iii) case study analysis and (iv) the development and validation of a functional NFC-Blockchain prototype to address the formalized technical problems as summarized in Table 1.

Table 1: Methodology

Phase	Methodology	Purpose	Participants/Tools
I	Quantitative Survey	Identify fraud prevalence and tech awareness	423 Port Operators
II	Qualitative Interviews	Deepen understanding of adoption barriers	5 Industry Experts
III	Case Study Analysis	Contextualize operational challenges	3 Maritime Ports
IV	Prototype Validation	Technical feasibility & Proof of Concept (PoC) validation	NFC Hardware, Zetrix Blockchain

2.1 Research Design and Prototype Framework

This study utilizes a triangulation approach to ensure the robustness of findings by integrating empirical data with an experimental design artifact. While the quantitative survey (n=423) and qualitative interviews (n=5) establish the empirical "why" and "what" regarding maritime fraud, the Design Science Research (DSR) phase focuses on the "how" through the development of a functional technical solution. This phase involves creating a multi-layered technical architecture that maps physical assets to a digital ledger via NFC hardware [15], [28]. The integration framework is built upon the Zetrix Layer 1 blockchain, selected for its high transaction throughput and cross-border interoperability. The prototype architecture is designed to automate the verification of high-risk processes identified during the empirical phase, specifically cargo release and document authentication. The integration process follows a Hardware-to-Ledger Binding (HLB) protocol: physical NFC tags serve as the primary data source, which are then cryptographically linked to "digital twins" on the blockchain [29]. This integration ensures that any state change on the ledger, such as a change in cargo ownership or location, that requires a verified physical "handshake" via a proximity scan [30], [31]. By utilizing self-executing smart contracts, the system removes human intermediaries from the validation loop, thereby addressing the implementation complexity and human-error barriers highlighted in the survey results.

2.2 Quantitative Phase: Questionnaire Survey

The initial phase involved a questionnaire survey administered to Malaysian port operators to collect quantitative data on various aspects related to fraud and technology awareness [32], [33]. To ensure the findings reflected high-stakes operational environments, the study was conducted across three major port operators located within a prominent industrial and maritime hub in East Malaysia. To maintain strict confidentiality and protect the competitive interests of the participating entities, the specific names and precise locations of these ports have been anonymized. The survey instrument comprised questions regarding the current level of perceived fraud, familiarity with blockchain and NFC technology, and specific adoption barriers such as high implementation costs and regulatory uncertainty. This systematic gathering of data allowed for the provision of statistical evidence to support the research findings. A total of 423 respondents participated, representing a target population of logistics managers, security officers, and administrative personnel involved in cargo handling and documentation. The full survey instrument, including the Likert-scale items used to measure perceived effectiveness, is provided in Appendix A.

2.3 Qualitative Phase: In-depth Interviews

In addition to the survey, in-depth interviews were conducted with a purposive five (5) industry experts to gain qualitative insights and a contextual understanding of the research topic. These interviews allowed for a deeper exploration of key issues and perspectives that quantitative data alone could not capture, specifically focusing on the practical challenges of adopting blockchain and NFC technology in port operations. Participants were recruited based on their specialized expertise in port security, blockchain development, or maritime policy, and sessions were conducted either in-person or via secure video conferencing to ensure a wide range of expert representation [34], [35].

2.4 Case Study Analysis

Furthermore, an analysis of relevant case studies was conducted to supplement the findings from the surveys and interviews. These case studies offered real-world examples of how blockchain and NFC technology have been implemented in port operations to combat fraud, providing valuable lessons for the present study [36], [37]. By examining documented pilot projects and existing implementations, the research identified critical success factors and infrastructure requirements necessary for successful fraud prevention. This phase was crucial for validating the theoretical potential of these technologies against actual maritime operational results.

2.5 Data Analysis and Tools

Following the data collection phase, a rigorous analysis was performed using a multi-tool approach to ensure the reliability of both quantitative and qualitative results [38]. Quantitative data from the 423 survey responses were processed using statistical software to perform tests such as descriptive statistics, correlation matrices, and the calculation of composite maturity scores. These tests were used to identify relationships between technology familiarity and openness to adoption. For the qualitative data, thematic analysis was applied to interview transcripts and case study notes to identify recurring themes and barriers. Ethical approval for non-medical research involving human participants was obtained from the Universiti Malaya Research Ethics Committee (UMREC), and all participants provided informed consent prior to data collection.

2.6 Technical Validation

To move beyond descriptive analysis, the technical validity of the proposed framework was tested through a Proof-of-Concept (PoC). The prototype development followed an iterative process:

a) Requirement Definition: Based on survey results, identifying Implementation-Complexity as a major barrier.
b) System Artifact Construction: Building the NFC-to-Zetrix interface (as detailed in Section 3.0).
c) Functional Testing: Testing the cryptographic binding of NFC Unique Identifiers to the blockchain and validating real-time measurement updates.

3.0 SYSTEM ARCHITECTURE AND PROTOTYPE IMPLEMENTATION

To bridge the physical-digital gap identified in Section 1.4, we developed a technical framework that integrates NFC hardware with the Zetrix Blockchain. This section details the system architecture and the functional prototype used to validate the proposed fraud prevention mechanism.

3.1 Proposed System Architecture

The proposed system architecture is organized into a three-tier security model to maintain end-to-end cargo integrity from origin to destination, as depicted in Fig. 3. The Physical Perception Layer utilizes NTAG-series NFC chips embedded in cargo seals, storing hardware-encrypted Unique Identifiers (UIDs) that are physically tamper-evident [39]. Above this, the Edge Communication & Processing Layer serves as a gateway via mobile devices, capturing NFC payload data while appending contextual metadata such as GPS coordinates and timestamps. Finally, the Decentralized Ledger Layer, built on the Zetrix blockchain, relies on smart contracts to automate the cryptographic handshake between physical tag signatures and ledger records [30], [39].

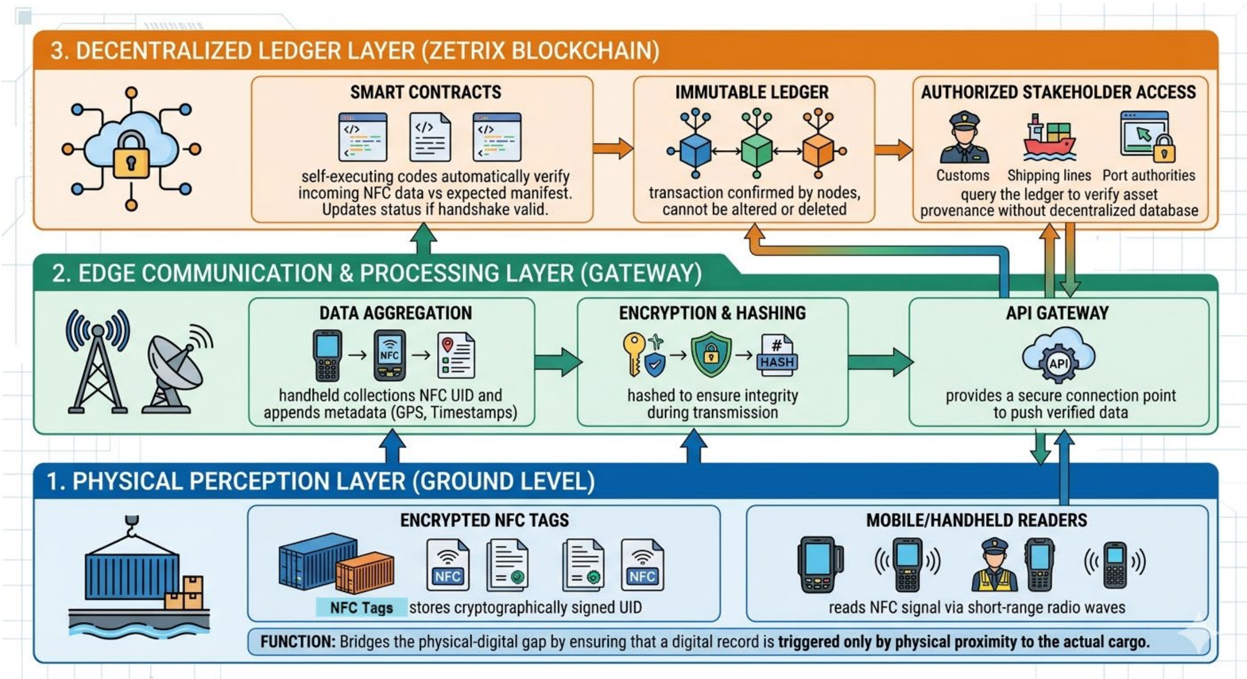

Fig. 3: Three Tier Security Model

3.2 Prototype Development and Workflow

The workflow diagram in Fig. 4 illustrates a comprehensive Hardware-to-Ledger Binding (HLB) protocol across three distinct phases, transitioning from physical asset arrival to immutable blockchain settlement [41], [42]. In Phase 1 (Asset Initialization), the process begins when a physical container is tagged with an encrypted NFC tag. A mobile device captures the chip's Unique Identifier (UID) and generates a cryptographic hash, which is then transmitted via

API to create a Digital Twin. This stage is governed by an initial smart contract that perpetually links the physical tag's identity to a new digital asset record on the Zetrix blockchain, ensuring the container cannot be spoofed.

As the cargo moves into Phase 2 (Monitoring & Verification), it passes through various port checkpoints such as warehouses or customs gates. At each location, an NFC Mobile Gateway scans the tag to aggregate real-time event data, including the hardware UID, GPS coordinates, and precise timestamps. This aggregated data is sent as a transaction request to a smart contract, which performs a cryptographic handshake by validating the current scan against the initialization data stored on the ledger. This real-time authentication allows for immutably validated events to be added as new blocks, providing full transparency via a Data Explorer and eliminating the dark windows of traditional monitoring.

The workflow culminates in Phase 3 (Blockchain Settlement) upon arrival at the final port destination. A final NFC verification scan triggers the terminal smart contract to perform an automated status update. This decentralized data anchoring updates cargo manifest and document status across the entire Zetrix network, providing authorized stakeholders such as customs, port authorities, and shipping lines with a single source of truth. By settling the transaction in a decentralized manner, the system effectively removes the single point of failure inherent in centralized Port Management Systems (PMS), thereby securing the operation against fraud and unauthorized data manipulation. The prototype screenshots are provided in Appendix B.

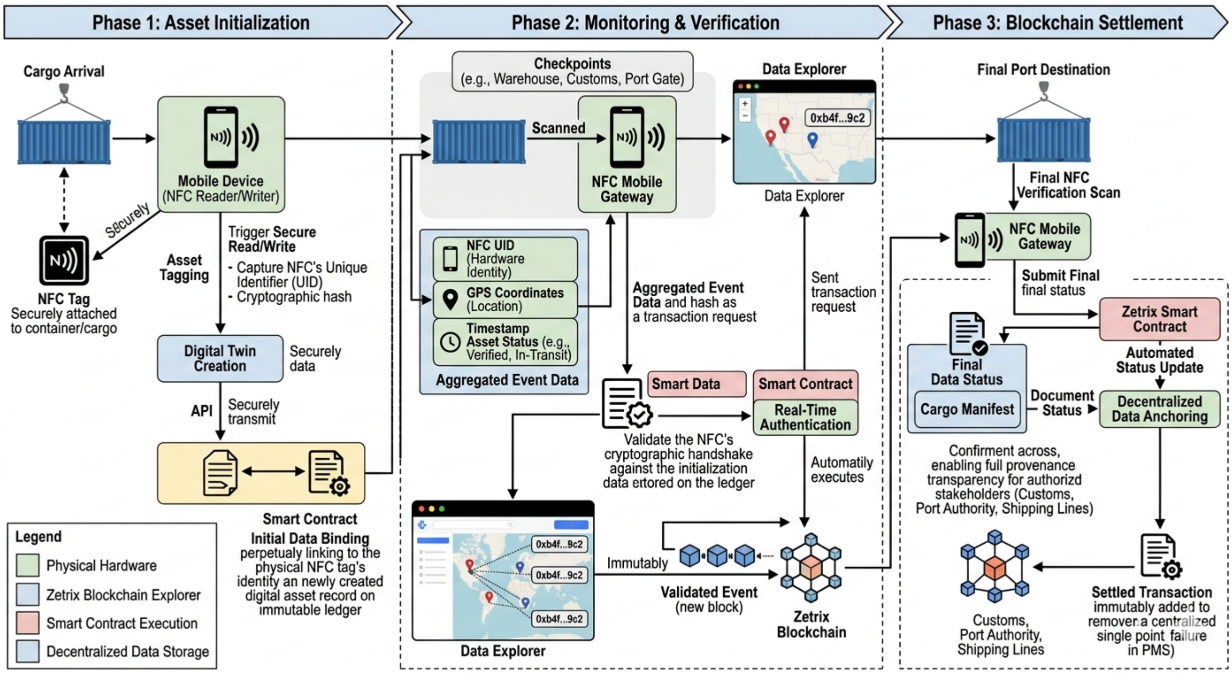

Fig. 4: Prototype Development and Workflow

3.3 Technical Novelty

Unlike existing maritime blockchain solutions that rely on manual data entry, which is prone to human error and "garbage-in, garbage-out" risks, this architecture enforces Automated Data Integrity [43]. By requiring a proximity-based NFC scan to trigger a blockchain transaction, the system ensures that the person scanning the cargo was physically present at the container, thereby mitigating remote document forgery and unauthorized manifest changes.

4.0 RESULTS

This section presents the empirical findings derived from the mixed-methods analysis, providing a comprehensive examination of the security landscape and technological readiness within the maritime sector. The results are synthesized from 423 quantitative survey responses collected from three major port operators in East Malaysia, supplemented by qualitative insights from five in-depth interviews with industry experts and a review of relevant case studies. The following subsections evaluate participant demographics, perceived fraud prevalence, and awareness levels regarding blockchain and NFC technologies. Furthermore, this section details stakeholder perspectives on the effectiveness of these tools, the anticipated benefits of their integration, and the primary barriers currently impeding their adoption in port operations, followed by a prototype recommendation.

4.1 Survey Findings and Technology Perceptions

The survey data reveals a significant incidence of security concerns, with 40% of respondents reporting high levels of fraud within their operational environments. As detailed in Table 2, which consolidates the key frequencies for fraud types and technology perceptions, cargo theft and document falsification emerge as the most pervasive threats, each affecting 65% of the sampled operations. These findings underscore a critical need for the enhanced authentication and transparency measures offered by emerging digital solutions.

Despite the high awareness of blockchain technology (70%), familiarity with NFC remains comparatively low at 35%. Nevertheless, a combined 75% of participants expressed confidence in the effectiveness of these technologies for fraud mitigation, either agreeing or strongly agreeing with their potential utility. This positive perception suggests that while technical knowledge of specific tools such as NFC may be limited, there is a strong industry-wide appetite for the security improvements they facilitate.

Table 2: Consolidated Survey Results for Fraud Prevalence and Technology Perceptions (n = 423)

Category	Item	Percentage (%)
Fraud Level	High	40
	Moderate	30
	Low	30
Primary Fraud Types	Cargo theft	65
	Document falsification	65
	Smuggling	45
	Unauthorized access	30
	Bribery / corruption	25
Technology Awareness	Blockchain awareness	70
	NFC awareness	35
Perceived Effectiveness	Strongly agree	40
	Agree	35
	Neutral	10
	Disagree / Strongly disagree	15

4.2 Adoption Barriers and Perceived Benefits

The results in this section are derived from a triangulation of the 423 questionnaire responses, thematic analysis of the five expert interviews, and the examination of existing maritime case studies. This multifaceted analysis identifies the specific organizational and technical hurdles that must be overcome for successful implementation. As shown in Table 3, the primary obstacles identified by the survey are multifaceted, ranging from financial constraints to technical and regulatory concerns.

Table 3: Perceived Benefits and Barriers to Adoption

Category	Item	Percentage (%)
Perceived Benefits	Enhanced security	70
	Improved transparency	65
	Enhanced traceability	50
	Prevention of unauthorized access	45
	Reduction of fraud	40
Adoption Barriers	High implementation cost	55
	Data privacy and security concerns	55
	Lack of technical expertise	55
	Resistance to change	50
	Regulatory constraints	50
	Insufficient technical infrastructure	30

4.2.1 Synthesis of Qualitative Findings and Case Evidence

Beyond the quantitative survey figures, the in-depth interviews with five industry experts provided critical context regarding the "lack of technical expertise" and "resistance to change". Experts noted that while the industry is aware of blockchain, the "siloed" nature of port data remains a significant hurdle to adoption. They emphasized that document falsification often occurs because manual verification processes cannot keep pace with high-volume throughput.

The case study analysis further corroborated these findings by showcasing real-world implementations where blockchain-enabled transparency successfully reduced document processing times and improved audit trails. These cases demonstrated that the integration of NFC with blockchain can create a "digital twin" of physical assets, making unauthorized cargo movement significantly easier to detect. However, the case studies also highlighted that "insufficient technical infrastructure" (noted by 30% of survey respondents) remains a bottleneck for full-scale deployment in certain regions.

By synthesizing these results, it becomes clear that while the industry recognizes the value of blockchain and NFC, strategic support in infrastructure and specialized training is essential to bridge the gap between perceived value and actual operational adoption.

4.2.2 The Analysis

The identification of high implementation costs, data privacy concerns, and a lack of technical expertise (all at 55%) as the leading barriers highlights the complexity of the digital transition. However, these concerns are balanced by the significant benefits recognized by stakeholders, most notably enhanced security (70%) and improved transparency (65%). These results indicate that while the industry recognizes the value of blockchain and NFC, strategic support in infrastructure and training is essential to bridge the gap between perceived value and actual adoption.

	A	B	C	D	E	F
A	1.00	0.70	0.29	0.46	0.49	0.46
B	0.70	1.00	0.16	0.44	0.49	0.54
C	0.29	0.16	1.00	0.37	0.35	0.31
D	0.46	0.44	0.37	1.00	0.83	0.73
E	0.49	0.49	0.35	0.83	1.00	0.79
F	0.46	0.54	0.31	0.73	0.79	1.00

Legend	
A	Understanding of blockchain benefits in port operations.
B	Belief in the improvement of efficiency and productivity via Blockchain.
C	Frequency of participation in Blockchain and NFC related training.
D	Readiness of the port to adopt blockchain technologies.
E	Alignment of the port's strategy with digital transformation goals.
F	Confidence in achieving digitalization objectives.

Fig. 5: Correlation matrix for the factors related to the adoption of blockchain and NFC technologies

The correlation matrix for the factors related to the adoption of blockchain and NFC technologies among Malaysian port operators is depicted in Fig.5. This matrix reveals how various perceptions and experiences are interrelated, including understanding and confidence in the technologies, the frequency of training, openness to adoption, alignment with strategic goals, and overall confidence in achieving digital transformation objectives. From the matrix, we can see how strongly these factors are correlated with each other, indicating that improvements or deficiencies in one area might influence others.

The histogram shown in Fig. 6 is the distribution of the composite maturity scores for blockchain and NFC adoption, which can give an insight into the overall readiness and acceptance levels among the respondents. Scores are spread evenly, suggesting a range of maturity levels among port operators.

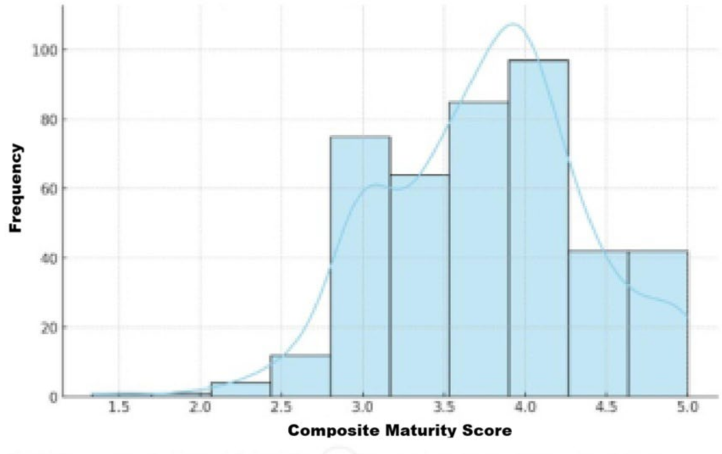

Fig. 6: Distribution of Composite Maturity Score

The scatter plot in Fig. 7 shows the visualization of the relationship between understanding the benefits of blockchain and openness to adoption, that visualizes the relationship between respondents' understanding of the benefits of blockchain technologies and their openness to adopting these technologies in port operations. The plot is color-coded and sized according to the composite maturity score, helping illustrate how these factors correlate with overall readiness. This visualization provides insights into the alignment between knowledge of blockchain benefits and the willingness to adopt such technologies, which are essential for strategic planning and targeted training initiatives.

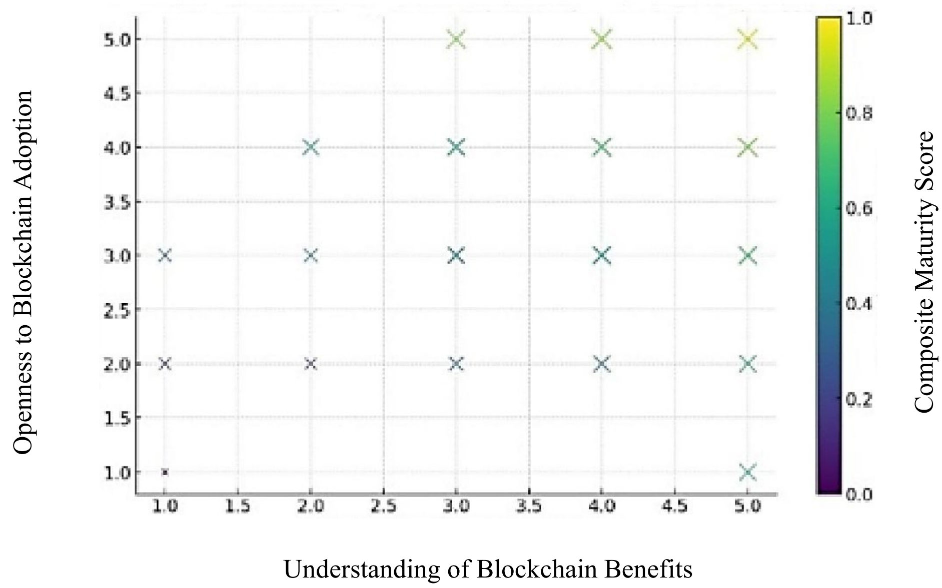

Fig. 7: Relationship between understanding the benefits of blockchain and openness to adoption

4.3 Prototype Implementation and System Architecture

While the empirical data in Sections 4.1 and 4.2 highlight a significant demand for enhanced security, it also reveals a critical readiness gap regarding the technical execution of these solutions. To address this, a functional prototype was developed based on a three-tier layered architecture designed to bridge the physical-digital disconnect identified as a primary security vulnerability.

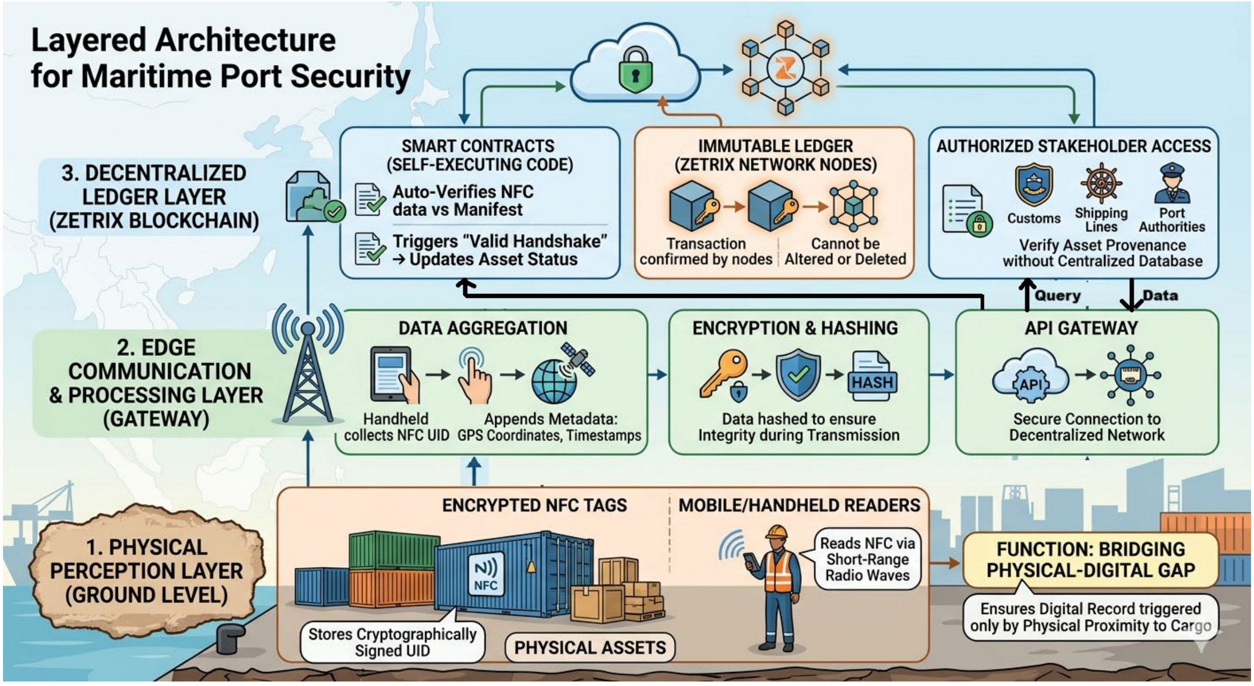

Fig. 8: Layered Architecture for Maritime Port Security

As illustrated in Fig. 8, the implementation begins at the Physical Perception Layer, which utilizes hardware-encrypted NFC tags attached to cargo. By requiring a proximity scan via handheld readers, the system ensures that a digital record can only be initiated or updated if the physical asset is present, thereby mitigating the document falsification risks reported by 65% of survey respondents. This data then flows into the Edge Communication & Processing Layer, where the NFC's Unique Identifier (UID) is aggregated with real-time metadata, including GPS coordinates and timestamps. This information is hashed and encrypted before being transmitted through a secure API gateway, ensuring that the data remains tamper-proof and eliminating the centralized information silos that traditional port management systems rely upon. Finally, the Decentralized Ledger Layer, built on the Zetrix blockchain, acts as the single source of truth. Within this layer, self-executing smart contracts verify the cryptographic "handshake" between the physical hardware and the digital manifest. Once validated, transactions are recorded immutably on the ledger, providing the real-time authentication and stakeholder transparency that 70% of survey participants recognized as a fundamental necessity for modernizing port operations.

5.0 DISCUSSION

The findings of this study, supported by both empirical data from 423 respondents and the technical prototype, demonstrate that while blockchain provides the necessary data integrity, it requires a physical anchoring mechanism like NFC to be truly effective in a port environment.

5.1 Current State of Fraud in Port Operations

The survey results indicated a high prevalence of fraud in port operations, with 423 respondents identifying the theft of cargo and falsification of documents as the most common types of fraudulent activity. The widespread occurrence of these fraudulent activities underscores the need for effective prevention and detection mechanisms. Expert interviews revealed that the lack of effective fraud detection mechanisms and regulatory oversight exacerbates the vulnerability of port operations to fraudulent schemes. This qualitative insight mirrors the survey data and supports earlier research by Zhao et al [44], which highlighted the inadequacy of existing control measures. Furthermore, Nisar et al [45] pointed out regulatory gaps and inconsistencies in port management practices, which create opportunities for fraudulent behaviour to go undetected. Consequently, the high prevalence of fraud, particularly cargo theft and document falsification, underscores an urgent need for improved measures. Addressing these challenges requires a multi-faceted approach, including technological innovations such as blockchain and NFC technology, alongside enhanced regulatory oversight.

5.2 Awareness and Adoption Trends

The survey results revealed that awareness of blockchain technology among port operators is relatively high, whereas NFC technology remains less familiar to the general workforce. However, despite this awareness gap, there is a shared recognition across all three data collection methods (survey, interviews, and case studies) of the potential of both technologies in mitigating fraud. Studies have underscored the importance of increasing awareness and educating stakeholders on the advantages of blockchain for transparency and NFC for security [46]. Nevertheless, the case study analysis indicated that actual adoption remains limited. Although blockchain's benefits are acknowledged in theory, expert interviews highlighted that integration challenges within existing port systems persist, compounded by regulatory and interoperability issues [47], [48]. Similarly, NFC technology faces adoption hurdles due to inadequate infrastructure and a lack of technical expertise among operators. Overcoming these challenges will require coordinated efforts in training, policy reform, and infrastructure investment.

5.3 Barriers to Technological Adoption

The triangulation of the 423 survey responses and expert interviews identified several critical barriers that impede the adoption of blockchain and NFC technologies. High implementation costs represent a foremost challenge, as the financial burden of upgrading infrastructure and acquiring necessary hardware constitutes a significant obstacle for port authorities operating under limited budgets [49], [50]. Beyond financial constraints, the expert interviews highlighted major interoperability issues; the absence of standardized protocols complicates integration with existing systems and hinders seamless data exchange among stakeholders, thereby reducing operational efficiency. These technical hurdles are further complicated by regulatory uncertainties. The evolving nature of frameworks related to data privacy and digital signatures contributes to compliance challenges, which may discourage operators from adoption due to potential legal risks [51].

Organizational and human factors also play a critical role in the slow pace of adoption. The survey data pointed toward significant resistance to change from stakeholders, including employees and management. This organizational inertia, characterized by deeply embedded traditional practices and a cultural reluctance to adopt new digital tools, requires strategic change management and active engagement. Furthermore, concerns regarding data privacy and security are prominent, given the sensitive nature of cargo details and financial transactions. Robust security frameworks and compliance with data protection standards are therefore essential to mitigate these perceived risks. Finally, a lack of technical expertise remains a pervasive barrier across the sector. The shortage of professionals with specialized skills in blockchain and NFC integration makes it difficult for authorities to recruit and retain the personnel required for successful implementation [52], [53]. Addressing these barriers necessitates a coordinated effort to mitigate costs, resolve regulatory issues, and build technical capacity within the maritime industry.

5.4 Comparative Analysis: Bridging the Physical-Digital Gap

A primary critique of existing maritime blockchain studies, such as those focusing on TradeLens or generic Hyperledger implementations, is their reliance on manual data entry or standard RFID. Manual entry introduces the "garbage-in, garbage-out" risk, where fraudulent data is immutably recorded in a ledger. Our proposed architecture differs significantly by enforcing a hardware-level "handshake." As demonstrated in the Phase I initialization (Fig. 9 in Appendix B), the use of hardware-encrypted NFC UIDs ensures that the digital twin is cryptographically bound to the physical asset at the source. Unlike standard RFID, which is susceptible to cloning, the NFC-Zetrix integration utilizes asymmetric encryption to ensure that only authorized devices can trigger a state change on the ledger.

5.5 Addressing Technical Barriers and Readiness

Our survey data revealed a significant "readiness gap," with 70% awareness of blockchain but only 35% familiarity with NFC. This disparity explains why many port authorities struggle to move past the pilot phase of digitalization. The prototype developed in this study addresses the "Implementation Complexity" barrier (cited by 55% of respondents) by utilizing commodity mobile hardware for scanning. This proves that high-security maritime tracking does not require expensive, proprietary infrastructure, but can be achieved through Layer 1 blockchain platforms like Zetrix, which offer the scalability needed for high-volume port throughput.

5.6 Novelty and Actionable Recommendations

Previous studies have often proposed blockchain as a universal solution for maritime fraud without defining the specific technical protocols required for physical-to-digital synchronization [54]. This research moves beyond these generic claims by proposing a concrete, validated protocol where:

a) Automated Execution via Hardware Oracles: Smart contracts function as automated escrow agents, releasing cargo status updates only upon a verified cryptographic handshake from an NFC hardware oracle. This ensures that digital state changes are physically anchored, a necessity highlighted in recent studies on IoT-Blockchain interoperability [55], [56].
b) Resilience against Single Points of Failure (SPOF): The decentralized verification model (as illustrated in Fig. 11 in Appendix B) eliminates the systemic vulnerabilities of traditional Port Management Systems (PMS). By distributing the verification across the Zetrix network, the framework achieves Byzantine Fault Tolerance (BFT) [57], preventing unauthorized manifest alterations that are common in centralized database architectures.

Based on these results, we recommend that port authorities prioritize investment in decentralized "Digital Twin" frameworks over incremental centralized database upgrades. This transition enables a strategic shift from reactive fraud detection to proactive, cryptographic prevention, ensuring that maritime security is enforced at the hardware level rather than through manual, error-prone administrative cycles [58], [59].

6.0 RECOMMENDATIONS

To mitigate maritime fraud and bridge the current "readiness gap," the industry must move beyond pilot phases toward standardized technical integration. Collaborative efforts between port authorities, technology providers, and regulators are essential to overcome implementation costs and establish a culture of innovation. Strategic partnerships and demonstration trials, such as the Zetrix-NFC prototype developed in this study, are instrumental in validating these technologies within live operational environments. By prioritizing the transition from paper-based systems to blockchain-enabled electronic Bills of Lading, stakeholders can ensure immutable transaction records and drastically reduce administrative forgery.

Furthermore, the maritime sector should adopt a dual-layered security approach by linking NFC-enabled hardware tags to blockchain-based "digital twins." This ensures real-time verification of physical cargo authenticity and allows for the implementation of self-executing smart contracts that automate compliance and payments. For these advancements to be effective, stakeholders must collaborate with organizations like the Digital Container Shipping Association (DCSA) to develop interoperable protocols and enforce robust cybersecurity measures, including regular encryption audits. Ultimately, successful adoption hinges on building technical capacity through comprehensive training programs, ensuring that the workforce is equipped to manage a secure, transparent, and resilient decentralized maritime ecosystem.

7.0 CONCLUSION

This research addresses the critical need for advanced security architectures in maritime port operations by proposing and validating an integrated NFC-Blockchain framework. While the maritime industry has long recognized the potential of blockchain, this study identifies and solves a primary technical bottleneck: the lack of a secure, automated link between physical cargo and digital ledgers. Through the development of a functional prototype on the Zetrix blockchain, we have demonstrated that binding hardware-encrypted NFC identifiers to smart contracts effectively mitigates common fraud vectors such as document forgery and cargo tampering. Our technical validation, supported by asset initialization and real-time measurement tracking proves that a "digital twin" approach can eliminate the "dark windows" of visibility that currently exist in manual or centralized port management systems. Empirical evidence from 423 port operators confirms that while the industry is ready for blockchain-enabled transparency, technical barriers such as implementation complexity and low NFC familiarity must be addressed. By providing a concrete system architecture and protocol design, this study moves beyond previous descriptive research to offer a scalable, technically rigorous framework for securing global trade. Future research will focus on extending the NFC-Blockchain integration framework by addressing cross-chain interoperability across heterogeneous Layer 1 networks and incorporating AI-driven anomaly detection models to automatically flag irregular scanning behaviours and physical tampering in real time.

ACKNOWLEDGEMENT

The authors acknowledge the use of large language models (LLMs) during the editing and proofreading phase to enhance clarity and readability. The conceptualization, analysis, and writing remain the sole responsibility of the authors.

FUNDING

This study is financed by MYEG through a private grant (PV081-2023).

REFERENCES

[1] Y. B. P. Sitompul, "Governance, risk management, compliance on preventing potential fraud in Indonesian state-owned port service industry," *Indones. J. Multidiscip. Sci.*, vol. 3, no. 6, pp. 818–829, 2024, doi: 10.55324/ijoms.v3i6.846.

[2] R. Subramaniam, S. R. Azzuhri, and T. Y. Wah, "Enhanced security approach powered by blockchain technology with NFC to prevent fraudulence in bank letter of credits," in *ACM International Conference Proceeding Series*, 2020, pp. 90–95. doi: 10.1145/3409934.3409945.

[3] Halima Oluwabunmi Bello, Courage Idemudia, and Toluwalase Vanessa Iyelolu, "Integrating machine learning and blockchain: Conceptual frameworks for real-time fraud detection and prevention," *World J. Adv. Res. Rev.*, vol. 23, no. 1, pp. 056–068, 2024, doi: 10.30574/wjarr.2024.23.1.1985.

[4] R. Song, L. Huang, W. Cui, M. Óskarsdóttir, and J. Vanthienen, "Fraud detection of bulk cargo theft in port using bayesian network models," *Appl. Sci.*, vol. 10, no. 3, 2020, doi: 10.3390/app10031056.

[5] S. Baechler, "Document Fraud: Will Your Identity Be Secure in the Twenty-first Century?," *Eur. J. Crim. Policy Res.*, vol. 26, no. 3, pp. 379–398, 2020, doi: 10.1007/s10610-020-09441-8.

[6] Waqar Azeem, Aftab Ahmad Malik, and Mujtaba Asad, "Information Systems and Mechanism for Prevention of Cyber Frauds," *Int. J. Electron. Crime Investig.*, vol. 8, no. 3, pp. 207–215, 2024, doi: 10.54692/ijeci.2024.0803207.

[7] E. Bellotti, J. Spencer, N. Lord, and K. Benson, "Counterfeit alcohol distribution: A criminological script network analysis," *Eur. J. Criminol.*, vol. 17, no. 4, pp. 373–398, Jul. 2020, doi: 10.1177/1477370818794870.

[8] J. Li, D. Han, T. H. Weng, H. Wu, K. C. Li, and A. Castiglione, "A secure data storage and sharing scheme for port supply chain based on blockchain and dynamic searchable encryption," *Comput. Stand. Interfaces*, vol. 91, pp. 103887, 2025, doi: 10.1016/j.csi.2024.103887.

[9] N. Kshetri, "Will blockchain emerge as a tool to break the poverty chain in the Global South?," *Third World Q.*, vol. 38, no. 8, pp. 1710–1732, 2017, doi: 10.1080/01436597.2017.1298438.

[10] A. Nasser, F. Ouzayd, and H. Ech-cheikh, "Blockchain technology in maritime single window and port community systems: A bibliometric analysis and systematic literature review," *Telemat. Informatics Reports*, vol. 18, pp. 100206, 2025, doi: 10.1016/j.teler.2025.100206.

[11] P. Guan, L. C. Wood, J. X. Wang, and L. N. K. Duong, "Blockchain adoption in the port industry: a systematic literature review," *Cogent Bus. Manag.*, vol. 11, no. 1, pp. 2431650, 2024, doi: 10.1080/23311975.2024.2431650.

[12] X. Liang, S. Fan, J. Lucy, and Z. Yang, "Risk analysis of cargo theft from freight supply chains using a data-driven Bayesian network," *Reliab. Eng. Syst. Saf.*, vol. 226, pp. 108702, 2022, doi: 10.1016/j.ress.2022.108702.

[13] M. Ben Farah *et al.*, "A survey on blockchain technology in the maritime industry: Challenges and future perspectives," *Futur. Gener. Comput. Syst.*, vol. 157, pp. 618–637, 2024, doi: 10.1016/j.future.2024.03.046.

[14] P. Onumadu and H. Abroshan, "Near-Field Communication (NFC) Cyber Threats and Mitigation Solutions in Payment Transactions: A Review," *Sensors*, vol. 24, no. 23, pp. 7423, 2024, doi: 10.3390/s24237423.

[15] J. A. B. Velez, E. R. V. Ramirez, and F. A. B. Caceres, "Real-time tracking and monitoring system for container terminals using RFID and IoT," *IEEE Access*, vol. 9, pp. 124850–124862, 2021, doi: 10.1109/ACCESS.2021.3110982.

[16] T. C. Y. Ng, D. Y. W. Liu, and A. C. Y. Leung, "Leveraging Blockchain and RFID/NFC Technology for Secure and Traceable Logistics for Documents with Digital Twin," in *Proceedings - 2024 IEEE International Conference on Blockchain, Blockchain 2024*, 2024, pp. 428–433. doi: 10.1109/Blockchain62396.2024.00063.

[17] S.-H. Chin, C. Lu, P.-T. Ho, Y.-F. Shiao, and T.-J. Wu, "Commodity anti-counterfeiting decision in e-commerce trade based on machine learning and Internet of Things," *Comput. Stand. Interfaces*, vol. 76, pp. 103504, 2021, doi: 10.1016/j.csi.2020.103504.

[18] Y. yip Lau, Q. Chen, M. C. P. Poo, A. K. Y. Ng, and C. C. Ying, "Maritime transport resilience: A systematic

literature review on the current state of the art, research agenda and future research directions," *Ocean Coast. Manag.*, vol. 251, pp. 107086, 2024, doi: 10.1016/j.ocecoaman.2024.107086.
[19] L. Zhang, Q. Zeng, and L. Wang, "How to Achieve Comprehensive Carbon Emission Reduction in Ports? A Systematic Review," *J. Mar. Sci. Eng.*, vol. 12, no. 5, pp. 715, 2024, doi: 10.3390/jmse12050715.
[20] A. Sergi, "Policing the port, watching the city. Manifestations of organised crime in the port of Genoa," *Polic. Soc.*, vol. 31, no. 6, pp. 639–655, 2021, doi: 10.1080/10439463.2020.1758103.
[21] E. Romsom, *Countering global oil theft: responses and solutions*. Helsinki, Finland: UNU-WIDER, 2022.
[22] R. Chen, J. Zhang, and H. Wang, "Autonomous fleet management system in smart ports: Practical design and analytical considerations," *Multimodal Transp.*, 2025, doi: 10.1016/j.multra.2025.100211.
[23] J. Basulo-Ribeiro, C. Pimentel, and L. Teixeira, "Digital Transformation in Maritime Ports: Defining Smart Gates through Process Improvement in a Portuguese Container Terminal," *Futur. Internet*, vol. 16, no. 10, 2024, doi: 10.3390/fi16100350.
[24] A. Boothroyd, V. Adams, K. Alexander, and N. Hill, "Priority areas for marine protection in the Amundsen and Bellingshausen Seas, Antarctica," *Mar. Policy*, vol. 167, pp. 106232, 2024, doi: 10.1016/j.marpol.2024.106232.
[25] M. Perkovič, L. Gucma, and S. Feuerstack, "Maritime Security and Risk Assessments," *J. Mar. Sci. Eng.*, vol. 12, no. 6, pp. 988, 2024, doi: 10.3390/jmse12060988.
[26] R. Subramaniam, S. R. Azzuhri, T. Y. Wah, A. Mahmood, and V. Balakrishnan, "A Holistic Anti-Counterfeiting Platform Using NFC and Blockchain Technologies," *Comput. Mater. Contin.*, vol. 83, no. 3, pp. 4257–4280, 2025, doi: 10.32604/cmc.2025.061560.
[27] Amitoj Singh, "Partnership to Operate Malaysia's National Blockchain Infrastructure Sealed," *https://www.coindesk.com/policy/2022/10/07/partnership-to-operate-malaysias-national-blockchain-infrastructure-sealed/*, 2022.
[28] H. T. Liao, T. M. Lo, and C. L. Pan, "Knowledge Mapping Analysis of Intelligent Ports: Research Facing Global Value Chain Challenges," *Systems*, vol. 11, no. 2, pp. 88, 2023, doi: 10.3390/systems11020088.
[29] X. Li, M. Tan, and W. Tian, "A secure and efficient sharing framework for student electronic academic records: Integrating zero-knowledge proof and proxy re-encryption," *Future Internet*, vol. 18, no. 1, art. no. 47, 2026, doi: 10.3390/fi18010047.
[30] K. Isobe, J.-P. Eisenbarth, D. Kondo, T. Cholez, and H. Tode, "A Deeper Grasp of Handshake: A Thorough Analysis of Blockchain-based DNS Records," in *2024 6th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, Berlin, Germany, 2024, pp. 1–10, doi: 10.1109/BRAINS63024.2024.10732335.
[31] P. Thilakavathy, S. Jayachitra, A. Aeron, N. Kumar, S. S. Ali, and M. Malathy, "Investigating Blockchain Security Mechanisms for Tamper-Proof Data Storage," in *2023 International Conference on Communication, Security and Artificial Intelligence, ICCSAI 2023*, 2023, pp. 926–930. doi: 10.1109/ICCSAI59793.2023.10421006.
[32] O. Nwabuko, "An Overview of Research Study Designs in Quantitative Research Methodology," *Am. J. Med. Clin. Res. Rev.*, vol. 3, no. 1, pp. 1–8, 2024, doi: 10.58372/2835-6276.1169.
[33] P. Anyin, D. Wittenberg, and J. Pannek, "Quantitative Methodology for Comparing Microscopic Traffic Simulators," *Futur. Transp.*, vol. 6, no. 3, pp. 101–115, 2025, doi: 10.3390/futuretransp5040201.
[34] D. S. Makateng and N. T. Mokala, "Understanding Qualitative Research Methodology: A Systematic Review," *E-Journal Humanit. Arts Soc. Sci.*, 2025, doi: 10.38159/ehass.2025637.
[35] K. Rana, P. Poudel, and R. Chimoriya, "Qualitative methodology in translational health research: Current practices and future directions," *Healthcare*, vol. 11, no. 19, art. no. 2665, 2023, doi: 10.3390/healthcare11192665.
[36] D. M. Zucker, P. Bruckenthal, and M. Patterson, "Case study methodology," in *Case Study Methodology for Nursing: Exploring the Lived Experience of those with Chronic Health Problems*, London, UK: Routledge, 2024. doi: 10.4324/9781003435358-3.
[37] A. Aravind, "The use of Case Study Methodology in Research," *International Journal For Multidisciplinary Research*. vol. 7, no. 1, pp. 45–52, 2025.
[38] O. N. Oyefusi, W. I. Enegbuma, and A. Brown, "A multi-level hierarchy decision-making framework for the implementation of novel regenerative supply chain management practices in construction," *Environ. Impact Assess. Rev.*, vol. 104, pp. 108128, 2026, doi: 10.1016/j.eiar.2025.108128.
[39] Z. Du, H. Cheng, Y. Fu, M. Huang, L. Liu, and Y. Ma, "A Four-Tier Smart Contract Model with On-Chain Upgrade," *Secur. Commun. Networks*, vol. 2023, Art. no. 8455894,2023, doi: 10.1155/2023/8455894.
[40] L. Alevizos, "Automated cybersecurity compliance and threat response using AI, blockchain and smart contracts," *Int. J. Inf. Technol.*, vol. 17, no. 2, pp. 767–781, 2025, doi: 10.1007/s41870-024-02324-9.
[41] K. G. Arachchige, P. Branch, and J. But, "An Analysis of Blockchain-Based IoT Sensor Network Distributed Denial of Service Attacks," *Sensors*, vol. 24, no. 10, pp. 3083, 2024, doi: 10.3390/s24103083.

[42] X. Yang *et al.*, “VeDB: A Software and Hardware Enabled Trusted Relational Database,” *Proc. ACM Manag. Data*, vol. 1, no. 1, pp. 1–26, 2023, doi: 10.1145/3589774.
[43] B. Gu, J. Liu, X. Ye, Y. Gong, and J. Chen, “Data-driven approach for port resilience evaluation,” *Transp. Res. Part E Logist. Transp. Rev.*, vol. 186, pp. 103570, 2024, doi: 10.1016/j.tre.2024.103570.
[44] R. Zhao, Z. Zhu, Y. Li, J. Zhang, and X. Zhang, “Use a UAV System to Enhance Port Security in Unconstrained Environment,” in *Advances in Intelligent Systems and Computing*, vol. 1210 AISC, Cham: Springer, 2021, pp. 78–84. doi: 10.1007/978-3-030-51758-8_11.
[45] U. Nisar *et al.*, “Unlocking the potential of blockchain technology in enhancing the fisheries supply chain: an exploration of critical adoption barriers in China,” *Sci. Rep.*, vol. 14, no. 1, pp. 10167, 2024, doi: 10.1038/s41598-024-59167-4.
[46] A. Andreadakis, T. F. Sloane, and D. Dalaklis, “An automated lifeboat manifesting embarkation system (Almes): Optimizing evacuation and passenger manifestation via rfid/nfc,” *TransNav*, vol. 15, no. 1, pp. 215–221, 2021, doi: 10.12716/1001.15.01.23.
[47] H. Kim, Z. Xiao, X. Zhang, X. Fu, and Z. Qin, “Rethinking Blockchain Technologies for the Maritime Industry: An Overview of the Current Landscape,” *Future Internet*. vol. 16, no. 12, pp. 454, 2024. doi: 10.3390/fi16120454.
[48] S. Shin, Y. Wang, S. Pettit, and W. Abouarghoub, “Blockchain application in maritime supply chain: a systematic literature review and conceptual framework,” *Marit. Policy Manag.*, vol. 51, no. 3, pp. 410–432, 2024, doi: 10.1080/03088839.2023.2234896.
[49] B. Jankowska, E. Mińska-Struzik, M. Bartosik-Purgat, M. Götz, and I. Olejnik, “Industry 4.0 technologies adoption: barriers and their impact on Polish companies’ innovation performance,” *Eur. Plan. Stud.*, vol. 31, no. 4, pp. 780–802, 2023, doi: 10.1080/09654313.2022.2068347.
[50] G. K. Akella, S. Wibowo, S. Grandhi, and S. Mubarak, “A Systematic Review of Blockchain Technology Adoption Barriers and Enablers for Smart and Sustainable Agriculture,” *Big Data and Cognitive Computing*. vol. 7, no. 2, pp. 86, 2023. doi: 10.3390/bdcc7020086.
[51] G. Zhao, X. Xie, Y. Wang, S. Liu, P. Jones, and C. Lopez, “Barrier analysis to improve big data analytics capability of the maritime industry: A mixed-method approach,” *Technol. Forecast. Soc. Change*, vol. 203, pp. 123345, 2024, doi: 10.1016/j.techfore.2024.123345.
[52] U. H. Govindarajan, G. Narang, D. K. Singh, and V. S. Yadav, “Blockchain technologies adoption in healthcare: Overcoming barriers amid the hype cycle to enhance patient care,” *Technol. Forecast. Soc. Change*, vol. 205, pp. 124031, 2025, doi: 10.1016/j.techfore.2025.124031.
[53] A. R. Nayeem *et al.*, “Unraveling the blockchain technology adoption barriers in the fast-moving consumer goods supply chain: An integrated fuzzy-set qualitative comparative analysis approach,” *Asia Pacific Manag. Rev.*, vol. 30, no. 1, pp. 100374, 2025, doi: 10.1016/j.apmrv.2025.100374.
[54] F. K. Elmay, K. Salah, I. Yaqoob, R. Jayaraman, A. Battah, and Y. Maleh, “Blockchain-Based Traceability for Shipping Containers in Unimodal and Multimodal Logistics,” *IEEE Access*, vol. 10, pp. 133539–133556, 2022, doi: 10.1109/ACCESS.2022.3231689.
[55] P. Das, S. Ray, and M. C. Govil, "A novel and secure blockchain-assisted NFC-based e-wallet architecture," in *Proc. 4th Int. Conf. Recent Adv. Inf. Technol. (RAIT)*, 2025, pp. 1–6, doi: 10.1109/RAIT65068.2025.11088914.
[56] R. Nayaka, “Enhancing Trust and Security in E-Voting: A Comprehensive Review of Blockchain and NFC Integration,” *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 12, no. 4, pp. 1205–1212,2024, doi: 10.22214/ijraset.2024.61170.
[57] N. H. A. Wahab, Z. Dayong, J. N. Fadila, and K. Y. Wong, “Advances in Consortium Chain Scalability: A Review of the Practical Byzantine Fault Tolerance Consensus Algorithm,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 7, pp. 880–892, 2024, doi: 10.14569/IJACSA.2024.0150796.
[58] F. Zhou, K. Yu, W. Xie, J. Lyu, Z. Zheng, and S. Zhou, “Digital Twin-Enabled Smart Maritime Logistics Management in the Context of Industry 5.0,” *IEEE Access*, vol. 12, pp. 15200–15215, 2024, doi: 10.1109/ACCESS.2024.3354838.
[59] A. Golovan *et al.*, “Enhancing Information Exchange in Ship Maintenance through Digital Twins and IoT: A Comprehensive Framework,” *Computers*, vol. 13, no. 10, pp. 261, 2024, doi: 10.3390/computers13100261.

APPENDIX A: RESEARCH INSTRUMENT (QUESTIONNAIRE)

The quantitative phase of this study utilized a 25-item questionnaire designed to assess the technological readiness and perceptions of port operators. All items were measured using a 5-point Likert scale (1 = Lowest Rating/Strongly Disagree; 5 = Highest Rating/Strongly Agree). To ensure anonymity, references to specific port names have been generalized.

Section I: Technology Understanding and Personal Capability

1. How well do you understand the benefits of adopting blockchain technologies in port operations?
2. To what extent do you believe that blockchain technology can improve your efficiency and productivity?
3. How frequently do you participate in training sessions or workshops related to blockchain technology and new technologies?
4. How confident are you in using blockchain tools and software for your daily tasks?
5. How important do you think it is for the port to embrace blockchain technology to stay competitive in the industry?

Section II: Operational Integration and Infrastructure

6. How seamlessly do different software systems utilizing blockchain technology in the port communicate and share data with each other?
7. To what extent is blockchain technology integrated into your day-to-day operations?
8. How effectively is blockchain technology utilized to track and manage cargo movement within the port?
9. How often are new technologies evaluated and implemented to enhance port operations?
10. How satisfied are you with the current level of blockchain technology support provided for your job role?

Section III: Data Integrity and Security

11. How organized and accessible do you find the data collected from various operations within the port?
12. How effectively is data used to make informed decisions at different levels of management?
13. How secure do you believe data systems are from cyber threats and unauthorized access?
14. How frequently are data analytics used to identify trends and opportunities for improvement within the port?
15. How well do you think the port utilizes data from blockchain for predictive maintenance and resource optimization?

Section IV: User Experience and Support

16. How user-friendly do you find the interfaces of digital tools and software for blockchain used in your daily tasks?
17. To what extent does blockchain technology enhance your efficiency and effectiveness in performing your job?
18. How satisfied are you with the support and assistance provided for troubleshooting blockchain tools and software?
19. How well does blockchain technology cater to the specific needs and requirements of different departments within the port?
20. How often do you provide feedback or suggestions for improving blockchain tools and systems used in the port?

Section V: Future Readiness and Strategic Alignment

21. How prepared do you feel the port is to adapt to future advancements in blockchain technology?
22. To what extent do you believe the port is investing in research and development of new blockchain technology?
23. How open do you think the port is to adopting emerging technologies to stay ahead in the industry?
24. How well do you perceive the port's strategy aligns with the broader goals of digital transformation, especially in Blockchain?
25. How confident are you in the port's ability to achieve its blockchain technology objectives in the coming years?

APPENDIX B: PROTOTYPE DEVELOPMENT AND WORKFLOW

The prototype was implemented using the Zetrix Layer 1 blockchain platform, chosen for its high throughput and cross-border interoperability in maritime trade. The technical workflow consists of three critical phases:

Phase I: Asset Initialization As shown in Fig. 9 , the process begins with the "Binding" of a physical asset to the blockchain. The mobile interface triggers an NFC scan; once the hardware UID is captured, a transaction is broadcast to the Zetrix network to register the asset's "Digital Twin." This ensures that the physical container cannot be replaced by a fraudulent one without breaking the cryptographic link.


```
Using source address: ZTX3Wtak2v9ogqbtZ2wNVgY78Z3jPK7qrKwrN
Using contract address: ZTX3eCaTtYZ6JEibqyB8jQUWU89rWNCQrMVVC
JSONbig [Object: null prototype] {
  error_code: 0,
  result: [Object: null prototype] {
    address: 'ZTX3Wtak2v9ogqbtZ2wNVgY78Z3jPK7qrKwrN',
    assets: null,
    assets_hash: 'ad67d57ae19de8068dbcd47282146bd553fe9f684c57c8c114453863ee41abc3',
    balance: 5629640,
    metadatas: null,
    metadatas_hash: 'ad67d57ae19de8068dbcd47282146bd553fe9f684c57c8c114453863ee41abc3',
    nonce: 379,
    priv: [Object: null prototype] {
      master_weight: 1,
      thresholds: [Object: null prototype]
    }
  }
}
```


Fig. 9: Asset Initialization

Phase II: Real-Time Measurement and Validation Once initialized, the system enters the monitoring phase. As illustrated in Fig. 10, the prototype captures real-time operational data. This interface displays the current status of the asset, including verification timestamps. This stage prevents "dark windows" in the supply chain by ensuring that every time the cargo is scanned at a checkpoint, its integrity is verified against the hash stored on the ledger.


```
Write #1: TxHash=bc2d90cadac1512b2e36d40047daa6f3cafab019c63c2de42452a233192061ba, Time=152.52ms

Write Operations:
- Successful writes: 1/1
- Failed writes: 0
- Total write time (ms): 154.29
- Average write latency (ms): 152.52
- Write throughput (TPS): 6.48

Write Latency Percentiles:
- 50th percentile: 152.52ms
- 90th percentile: 152.52ms
- 95th percentile: 152.52ms
- 99th percentile: 152.52ms
JSONbig [Object: null prototype] {
  error_code: 0,
  result: [Object: null prototype] {
    address: 'ZTX3Wtak2v9ogqbtZ2wNVgY78Z3jPK7qrKwrN',
    assets: null,
    assets_hash: 'ad67d57ae19de8068dbcd47282146bd553fe9f684c57c8c114453863ee41abc3',
    balance: 5629640,
    metadatas: null,
    metadatas_hash: 'ad67d57ae19de8068dbcd47282146bd553fe9f684c57c8c114453863ee41abc3',
    nonce: 379,
    priv: [Object: null prototype] {
      master_weight: 1,
      thresholds: [Object: null prototype]
```


Fig. 10: Real-Time Measurement and Validation

Phase III: Blockchain Settlement and Integrity Check. The final verification is handled through the Zetrix interface, as depicted in Fig. 11. The blockchain serves as the "Single Source of Truth." Any attempt to alter cargo manifests or document status in the Port Management System (PMS) would fail, as the decentralized ledger would show a mismatch with the original encrypted NFC handshake recorded during Phase I.

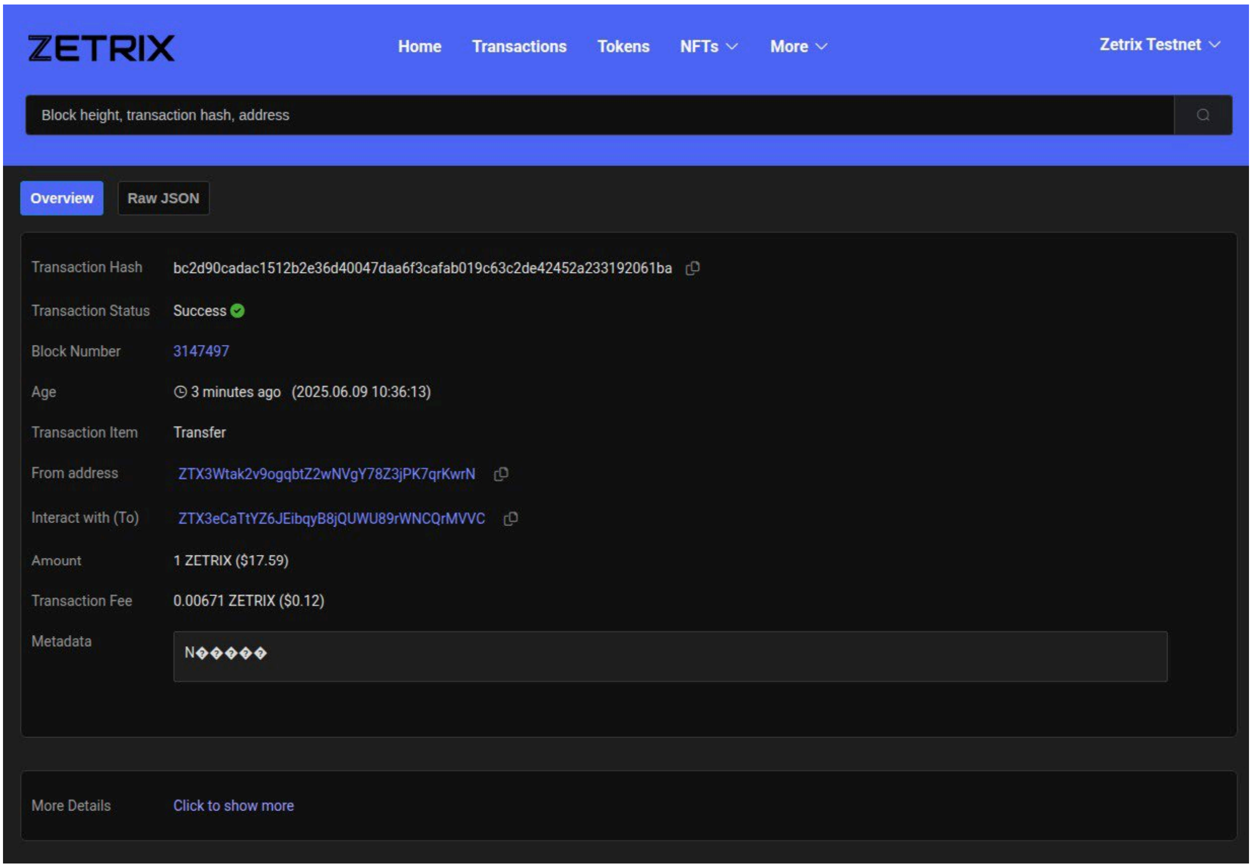

Fig. 11: Blockchain Settlement and Integrity Check