https://doi.org/10.5755/j02.eie.38758

Enhancing Maritime Communication Security with Blockchain Technology

Georgi Dimitrov[*], Ivaylo Mitishev
Department of Navigation, Nikola Vaptsarov Naval Academy
73, Vasil Drumev St., 9000 Varna, Bulgaria
[*]g.dimitrov@naval-acad.bg; i.mitishev@naval-acad.bg

***Abstract*—Blockchain technology, fundamentally characterised by decentralisation, immutability, and consensus mechanisms, revolutionises data management and communication security. Unlike traditional centralised databases controlled by a single authority, blockchain distributes data across a network of nodes in a peer-to-peer framework, enhancing security by eliminating single points of failure. Immutability ensures that once data are recorded, they cannot be altered due to cryptographic hashing, where the hash of each block depends on its content, making tampering evident. Real-world applications include secure cargo tracking, identity management, and smart contracts. Blockchain enables real-time tracking of cargo, verified digital identities, and self-executing contracts that automate processes such as ownership verification and payment settlements. This article explores the potential of blockchain to fortify maritime communication security. Suggestion for a secure communication structure in shipping is presented, as well as a blockchain algorithm in Python for secure application onboard. For practical implementation, a blockchain-based document workflow management system can be developed to manage critical maritime documents.**

***Index Terms*—Blockchain; Bill of lading; Secure communications; Document workflow.**

I. INTRODUCTION

The maritime industry, a vital artery of global trade and commerce, relies heavily on efficient communication networks. However, this critical lifeline faces persistent challenges, including data tampering vulnerabilities, unauthorised access, and operational inefficiencies. In recent years, blockchain technology has emerged as a beacon of promise, offering innovative solutions to fortify communication security within this dynamic ecosystem. Maritime communication involves a complex web of interactions among shipping companies, port authorities, regulatory bodies, and other stakeholders. These interactions span diverse processes, from cargo tracking and vessel management to compliance checks and financial settlements. Traditional communication systems face inherent limitations: trust deficits, data integrity, and operational delays. Centralised communication channels lack transparency, leaving room for doubt and mistrust among participants. Tampering with communication logs, cargo manifests, or identity records jeopardises the entire supply chain. Ensuring data integrity is paramount for secure operations. Cumbersome paperwork, manual verifications, and legacy systems contribute to delays, which affects efficiency and timely decision-making.

One of the defining characteristics of blockchain is its immutability. Once data are recorded on the blockchain, they cannot be altered or deleted. This feature is crucial for maritime communication, where the integrity of the data is paramount. For example, communication logs detailing ship routes, cargo manifests listing shipped goods, and identity records of crew members become permanently fixed on the blockchain. This immutability ensures that all recorded information is tamper-proof, fostering a higher level of trust among stakeholders. Blockchain technology also introduces a high degree of transparency. Every authorised participant in the blockchain network can view and verify communication records. This openness increases confidence among shipping companies, port authorities, and customs officials, as they can independently confirm the authenticity and accuracy of the data. Transparency streamlines processes by reducing the need for intermediaries and simplifying document verification, leading to faster and more efficient operations. Traditional centralised systems are prone to single points of failure, which can disrupt operations and compromise security. The blockchain, however, operates on a decentralised network of nodes. Each node holds a copy of the entire blockchain and work collectively to validate and record new transactions. This decentralisation ensures that even if one node fails or is compromised, the system remains operational and secure [1]–[17]. According to Chang, Chen, Lu, and Luo [1], for the maritime industry, this means a more resilient communication infrastructure that can withstand cyber attacks and technical failures.

Blockchain technology is not obsolete. It continues to evolve and find applications beyond cryptocurrencies. Enterprises are exploring user cases in areas like identity management, data integrity, and certifications. Although not yet fully mainstream, blockchain is maturing and shaping the future of business and asset management.

II. LITERATURE OVERVIEW

Researchers aiming to enhance maritime communication security have identified key features of blockchain technology that are particularly relevant. The maritime

Manuscript received 9 September, 2024; accepted 21 December, 2024.

industry communication networks involve numerous stakeholders, including shipping companies, port authorities, customs officials, and regulatory bodies, all of whom interact through various processes such as cargo tracking, vessel management, compliance checks, and financial settlements. The intricacy and critical nature of these interactions underscore the need for robust, secure, and efficient communication systems to ensure smooth operations within the industry.

Current systems within the maritime industry face significant challenges that obstruct their efficiency and security. Traditional centralised databases are susceptible to security breaches and lack robust mechanisms to prevent data tampering. Operational inefficiencies arise from manual verifications, cumbersome paperwork, and outdated legacy systems, resulting in delays and overall inefficiency. Blockchain eliminates single points of failure, enhancing the resilience of communication systems against cyber-attacks and technical failures. Only authorised participants can view and verify blockchain records, reducing the need for intermediaries and streamlining verification processes. Moreover, smart contracts automate processes, reducing administrative overhead and speeding up transactions according to Blockchain Basics [2].

Implementing blockchain in the maritime industry involves addressing several key considerations. Scalability can be managed using off-chain solutions and optimised consensus algorithms to handle increased transaction volumes. Interoperability requires the development of industry-wide standards and middleware to integrate blockchain with existing maritime systems. Ensuring regulatory compliance is crucial, necessitating that blockchain solutions adhere to various legal frameworks and data protection regulations. Data privacy and security can be maintained through the use of private or consortium blockchains, robust encryption, and stringent identity management protocols. Overcoming resistance to change involves educational campaigns and pilot projects to demonstrate the practical benefits and feasibility of blockchain, as discussed by Li, Lee, and Gharehgozli [16].

Several related works contribute to the foundation of this research. Tian [6] presents a blockchain-based system to improve transparency and traceability in the agri-food supply chain using radio frequency identification (RFID) technology, highlighting the potential of the blockchain to ensure data integrity and trace product origins efficiently, but limited to the agri-food sector and not addressing maritime complexities. Tam and Jones [13] focus on the assessment of cyber risks for autonomous ships, highlighting the importance of robust cybersecurity measures for maritime operations but do not propose a specific blockchain-based solution. Dobrovnik, Herold, Fürst, and Kummer [4] explore potential blockchain applications in logistics, including maritime logistics, to improve transparency and efficiency in supply chain operations, but lack detailed implementation frameworks specifically for maritime communication security [10]. Christidis and Devetsikiotis [3] examine integrating blockchains and smart contracts with IoT devices to streamline supply chain management, emphasising automation and security, but primarily focussing on IoT integration and not maritime-specific applications. Taghavifard *et al.* [17] discuss the role of blockchain in ensuring data integrity and sustainability in supply chain management with a case study from the airport industry that has parallels to maritime logistics but does not focus primarily on maritime communication security challenges. These works often focus on specific sectors, provide broad overviews without detailed implementation strategies, or lack maritime-specific solutions [7]. Moreover, issues like interoperability with existing maritime systems and scalability of blockchain networks under high transaction volumes are often not thoroughly addressed. By incorporating blockchain nature, the proposed solution in this paper aims to mitigate identified problems and improve overall security and efficiency in maritime communications.

The methodologies in blockchain-related studies emphasise the integration of blockchain technology to improve security, efficiency, and performance in various IoT and transportation systems. One approach, Kebande, Karie, Takako, and Muthoni [9] involves the development of a blockchain-based multifactor authentication (MFA) model, which integrates single sign-on (SSO) and Security Assertion Markup Language (SAML) protocols. Such a model is further enhanced with an embedded probabilistic polynomial-time algorithm (ePPTA) and an additional hash function, specifically designed to strengthen authentication schemes in IoT and Internet of Vehicles (IoV) environments, ensuring robust security in cloud-based systems. In maritime IoT applications [18], a blockchain-based authentication mechanism is proposed, using a private blockchain network governed by a Proof-of-Authority (PoA) consensus algorithm. Therefore, the Port Authority Command and Operation (CO) centre acts as the blockchain administrator, overseeing the mining and maintenance of the ledger. According to Rahimi, Khan, Chrysostomou, Vassiliou, and Nazir [11], each vehicle or vessel, buoy, and Fusion Center (FC) is assigned a unique blockchain SHA-256 hash address for identification, and the FC is responsible for validating these IDs before data storage. This method underscores the importance of secure, decentralised data management in maritime communication systems. Further expanding the application of blockchain, the studies propose its use in autonomous vessel control and transportation management systems. Techniques such as "database sharding" are used to secure vessel control data, with certification authorities managing digital cryptographic certificates. Additionally, blockchain-based simulations investigate captain or driver behaviour in transportation systems, leading to the development of the parallel transportation management and control system (PTMS) and the quick road system (QRS). These systems leverage blockchain to improve traffic management, optimise energy efficiency, and incentivise data sharing among drivers, thus encouraging more efficient and secure transportation networks.

III. DISCUSSION

Traditional centralised communication systems are liable to data tampering and unauthorised access, leading to compromised cargo information, falsified identity records, and altered communication logs, thereby jeopardising the integrity and trustworthiness of the entire maritime supply chain. Additionally, the reliance on manual paperwork, legacy systems, and slow verification processes creates significant operational delays, resulting in increased costs and a lack of timely decision-making. To address these issues, the paper proposes blockchain technology as a robust solution. The application and experiments with real software will be a matter of future development. The paper also addresses implementation challenges with existing systems, regulatory compliance, data privacy and security, and resistance to change, proposing mitigation strategies such as off-chain solutions, industry-wide standards, legal compliance features, private blockchains, and educational campaigns to encourage greater adoption. According to Tsiulin, Reinau, Hilmola, Goryaev, and Karam [14], by overcoming these challenges, the maritime industry can leverage blockchain to create a more secure, transparent, and efficient global trade environment.

Blockchain technology holds great promise in revolutionising maritime communications. However, its implementation in the maritime industry presents both opportunities and challenges [12]. Blockchain technology is increasingly recognised as a transformative force in maritime communications, offering unprecedented security and reliability, particularly in applications involving unmanned aerial vehicles (UAVs) and autonomous maritime surface ships (MASS). In the realm of maritime IoT systems [17], blockchain-based authentication mechanisms are increasingly essential to secure data transmissions between UAVs and other connected systems. By leveraging the decentralised blockchain structure, these mechanisms ensure that communication channels remain secure against potential cyber threats. This is particularly critical for UAVs, which play a vital role in maritime surveillance, cargo delivery, and environmental monitoring. Similarly, for MASS, which relies heavily on real-time data and communication to operate autonomously, blockchain provides a robust solution to the vulnerabilities posed by traditional, centralised communication systems. The result is a more secure and resilient framework that underpins the autonomous operations of these advanced vessels. Beyond enhancing security, blockchain is also being integrated into new IoT-enabled maritime transport systems, which are designed to address the dual challenges of security and energy efficiency. By incorporating distributed network architecture and edge computing, these systems ensure that data integrity is maintained even in a vast and often harsh maritime environment. The decentralised blockchain ledger provides a secure platform for data exchange, while edge computing processes data closer to the source, reducing latency and improving response times. Furthermore, the novel application of dynamic voltage frequency scaling in this context optimises energy consumption. This technique adjusts the power usage of computing resources in real time, balancing the high demands of secure communication with the limited energy resources typically available in maritime operations. This innovative approach not only enhances the performance of maritime communication networks but also extends the operational lifespan of energy-constrained systems, such as those onboard ships or in remote maritime installations. In addition to securing communications and optimising energy use, blockchain technology is also driving innovation in maritime navigation and operational efficiency. The concept of a “quick road system” (QRS) from land transport, which uses blockchain to manage real-time lane sharing, offers a glimpse into how similar decentralised approaches could be adapted to maritime settings [5]. In a maritime context, such a system could facilitate peer-to-peer real-time coordination among vessels, optimising navigation routes, reducing congestion in busy shipping lanes, and improving overall traffic management. By using blockchain to enable secure and transparent communication between vessels, a maritime QRS could provide a decentralised solution for route optimisation, reducing reliance on centralised authorities, and allowing for more flexible, dynamic responses to real-time conditions at sea. The use of blockchain in such systems introduces new possibilities to “incentivise” collaboration between maritime operators. Through blockchain-based tokens, vessels could be rewarded for participating in coordinated lane sharing or for sharing real-time navigational data, creating a more dynamic and responsive maritime transport ecosystem. This tokenization could drive a more efficient use of maritime routes, encourage better resource management, and ultimately lead to reduced operational costs for shipping companies. The integration of blockchain in various aspects of maritime communication and operation highlights its potential not only to secure and optimise existing systems but also to innovate new processes and collaborative frameworks that will define the future of maritime transport.

Blockchain networks may encounter scalability issues as transaction volumes increase. This risk can result in slower processing times and increased resource requirements. As a mitigation strategy, implementation of off-chain solutions such as payment channels or side chains to alleviate the load on the main blockchain network could be utilised. If the blockchain is partitioned into smaller shards, this could enable parallel transaction processing, thus improving throughput. Further to the option for optimised consensus algorithms, it is necessary to explore energy-efficient mechanisms such as Proof-of-Stake (PoS) to expedite transaction validation while reducing resource consumption. Integrating blockchain with existing maritime systems, comprising legacy databases, IoT devices, and diverse blockchain platforms, poses significant challenges in interoperability. A mitigation strategy is to develop industry-wide standards for data formats, APIs, and communication protocols to facilitate seamless interoperability. Other ways are to utilise middleware and interoperability modules (e.g., Hyperledger Fabric module) to effectively bridge disparate blockchain networks and establish well-defined APIs and gateways to facilitate smooth interaction between blockchain and legacy systems, ensuring compatibility and ease of integration. Maritime regulations vary globally, necessitating blockchain solutions that align with diverse legal frameworks regarding data privacy, ownership, and cross-border transactions. Engaging maritime law-proficient legal experts to navigate complex regulatory landscapes and ensure compliance is one mitigation strategy. Blockchain solutions should be designed with built-in privacy features to comply with stringent data protection regulations such as the general data protection regulation (GDPR). Contracts should be developed smartly to comply with relevant regulations that govern trade finance, customs declarations, and other maritime operations. Storing sensitive maritime data on public blockchains poses risks of unauthorised access and compromise. This will lead to the need to utilise private or consortium-permitted blockchains with restricted access controls to safeguard sensitive information. Therefore, robust encryption mechanisms for data should be applied before they are stored on the blockchain, ensuring confidentiality and integrity.

Stakeholders in the maritime industry may resist blockchain adoption due to concerns about change management, lack of awareness, or conflicting interests. Targeted educational campaigns could elucidate the benefits of blockchain technology and dispel misconceptions among stakeholders. If small-scale pilot projects are initiated, this will demonstrate the practical benefits and feasibility of blockchain solutions in real-world maritime scenarios. In conclusion, while the implementation of blockchain technology in maritime communication presents multifaceted challenges, proactive mitigation strategies can significantly improve the likelihood of success. By systematically addressing scalability, interoperability, regulatory compliance, data privacy, security concerns, and change resistance, the maritime industry can harness the transformative potential of blockchain.

On the diagram of Fig. 1:

– A smart contract monitors cargo delivery and compliance;

– Upon successful delivery and compliance verification, the smart contract automatically triggers payment release.

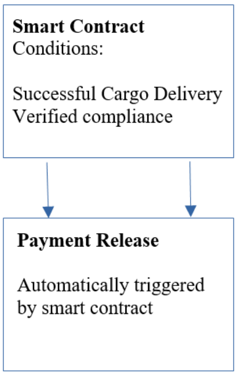

Smart Contract
Conditions:
Successful Cargo Delivery
Verified compliance
Payment Release
Automatically triggered by smart contract

Fig. 1. The process with the smart contract.

This approach ensures secure, efficient, and transparent payment settlements in maritime operations. The smart contract-based approach ensures secure, efficient, and transparent payment settlements in maritime operations, benefiting all involved parties.

The diagram provided illustrates how a smart contract monitors cargo delivery and compliance in maritime operations.

1. *Smart Contract Creation*

– A smart contract is a self-executing programme deployed on a blockchain network (such as Ethereum).

– In our case, the smart contract is designed specifically to manage payment settlements related to cargo delivery.

2. *Trigger Events*

The smart contract monitors two critical trigger events:

– Cargo Delivery: When cargo reaches its destination or designated port, the smart contract receives a signal indicating successful delivery.

– Compliance Verification: The smart contract verifies compliance with predefined conditions (e.g., delivery time, cargo condition).

These trigger events are essential to determine when payment should be made.

3. *Automated Payment Release*

Upon successful cargo delivery and compliance verification, the following occurs: the smart contract automatically executes the payment release process. Funds are transferred from the payer’s account (e.g., shipping company) to the payee’s account (e.g., cargo owner or supplier). This automation eliminates manual intervention and reduces administrative overhead.

4. *Security and Transparency*

– Immutable Records: All payment-related events are recorded on the blockchain ledger. Once recorded, this information cannot be altered or tampered with.

– Fraud Prevention: Immutable records prevent unauthorised changes, ensuring trust between stakeholders.

– All parties involved (shipping companies, cargo owners, financial institutions) can verify the payment process.

– Transparency encourages confidence and reduces disputes.

5. *Efficiency Gains*

By automating payment settlements, the process becomes more efficient:

– Faster Transactions: Real-time execution eliminates the delays associated with manual approvals.

– Reduced Administrative Burden: Smart contracts handle repetitive tasks without human intervention.

6. *Stakeholder Roles*

The Payer (Shipping Company) initiates the smart contract by specifying the payment terms and conditions. Then monitors the execution of the contract. The Payee (Cargo Owner or Supplier) receives payments automatically after meeting the contract conditions. Then verifies payment details on the blockchain. Regulators and auditors can independently verify compliance and payment execution. The smart contract is then audited for transparency and accuracy.

7. *Legal Considerations*

One should ensure that the smart contract aligns with legal requirements such as jurisdiction-specific regulations and digital signatures and enforceability. Legal experts should review and validate the contract.

8. Scalability and Adoption

– Scalability: Optimise the smart contract for high transaction volumes.

– Industry-Wide Adoption: Encourage other stakeholders to adopt similar smart contract solutions for consistent and streamlined payment processes.

Implementing blockchain technology in maritime communications and shipping can offer significant advantages, such as increased transparency, security, and efficiency according to Blockchain for business [8]. Here is a suggestion on how blockchain can be used in maritime communications through the management of cargo-related documents, verification of data authenticity, and tracking of goods through the supply chain.

IV. BLOCKCHAIN ALGORITHM FOR MARITIME COMMUNICATIONS

Implementing a blockchain algorithm for maritime communications involves several structured stages to ensure efficient handling of transactions and cargo movements throughout the supply chain. Every generated block is verified by the blockchain network. Verification is achieved through a consensus mechanism - Proof-of-Stake (PoS), where network participants validate the accuracy and legitimacy of the transaction. Once consensus is reached and the block is verified, it is appended to the existing blockchain. One of the key benefits of this technology in maritime communication is the real-time tracking of goods. Each participant in the network can trace the movement of a specific cargo by accessing the history of blocks associated with that cargo. This transparency not only enhances visibility, but also serves as a deterrent to fraudulent activities, ensuring accountability throughout the supply chain. As the status of goods changes - whether due to transfer to another vessel, customs clearance, or arrival at a port - new information is recorded in the subsequent blocks. These updates are synchronised between all participants in the network, maintaining a consistent and updated record of the journey of the cargo. Upon successful delivery of goods to their final destination, a final block is created that confirms completion of the transaction. All participants involved validate and confirm the delivery, effectively closing the chain for that particular transaction. This final step ensures that all stakeholders are informed about the successful journey of the cargo and the completion of the relevant transactions.

In Fig. 2, the flow chart is given for the blockchain algorithm.

1. *Start*. The process begins with the creation of a blockchain network that includes all relevant stakeholders in maritime operations. This typically includes shipping companies, port authorities, customs officials, suppliers, and other pertinent entities. Each participant is assigned a unique cryptographic key, ensuring secure access and authentication within the network.
2. *Initialise Blockchain*. As transactions occur within the maritime ecosystem, such as loading or transferring cargo, a new block is generated for each transaction. This involves creating a Blockchain class instance that automatically generates the Genesis Block. The Genesis Block is the first block on the blockchain, typically containing default values or a simple transaction. This block is crucial as it serves as the foundation for the entire blockchain.
3. *Create Genesis Block*. This block contains basic information like an index, timestamp, and initial data. Importantly, it also includes a hash that is computed using the SHA-256 algorithm. This block is manually added to the blockchain to kick-start the chain.
4. *Add New Transaction*. After the blockchain is initialised and the Genesis Block is created, new transactions can be added. Each transaction represents an event or piece of data that needs to be securely stored on the blockchain. For example, in the maritime supply chain, a transaction could represent a cargo transfer, a ship’s departure, or the reception of goods.
5. *Add New Block to Blockchain*. For every transaction added, a new block is created. It contains the transaction data, an index, a timestamp, the hash of the previous block, and its own hash. The inclusion of the hash of the previous block ensures the immutability of the blockchain - modifying any block would require recalculating the hashes of all subsequent blocks, making tampering detectable.
6. *Repeat for Each Transaction*. This step is iterative. For every new transaction, steps 4 and 5 are repeated: the transaction is added, a new block is created, and it is appended to the blockchain. This process continues for each event or transaction in the maritime supply chain.
7. *Display Blockchain (End)*. Once all transactions have been added and the blockchain has been constructed, the entire blockchain can be displayed. This display will show the complete history of all transactions, with each block containing its respective transaction data, index, timestamp, previous hash, and current hash. This step allows for the tracking of cargo or any other tracked entity within the blockchain, providing a transparent record of all events.

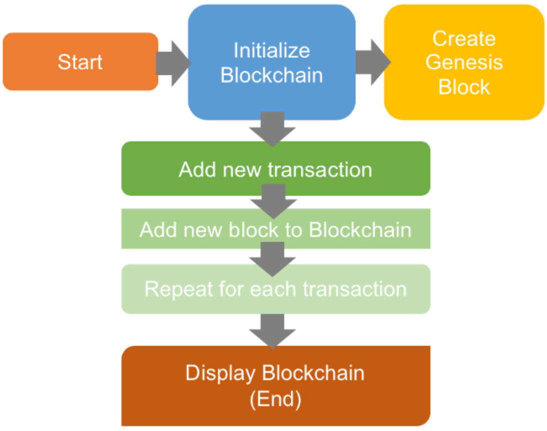


Fig. 2. Flow chart of the algorithm with suggested coding using Python.

Each stage - from initialisation and transaction recording to verification, tracking, synchronisation, and transaction completion - plays a crucial role in ensuring the reliability and efficiency of maritime operations in a globally interconnected supply chain. The code can be found in Appendix A.

V. BLOCKCHAIN TECHNOLOGY FOR HANDLING BILL OF LADING IN SHIPPING COMMUNICATIONS

The diagram in Fig. 3 illustrates the key stages of the process, the entities involved, and the flow of information through the blockchain system.

Stages in the Process:

1. Bill of Lading Issued: Initiation of the Bill of Lading by the shipping company;

2. Cargo Loaded: Cargo is loaded onto the ship;
3. Cargo in Transit: Cargo is in transit over the sea;
4. Cargo Unloaded: Cargo is unloaded at the destination port;
5. Customs Clearance: Customs clearance processes the cargo;
6. Bill of Lading Verified: Verification of the Bill of Lading by relevant authorities;
7. Delivery Confirmed: Final confirmation of cargo delivery to the recipient.

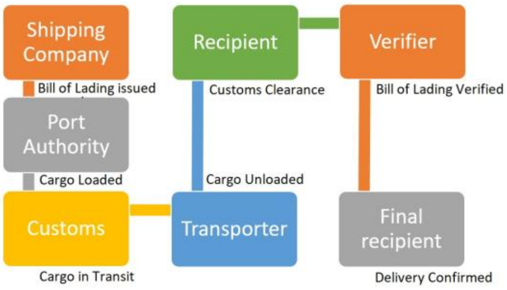


Fig. 3. The visual presentation of the entities involved and information flow.

Entities Involved:

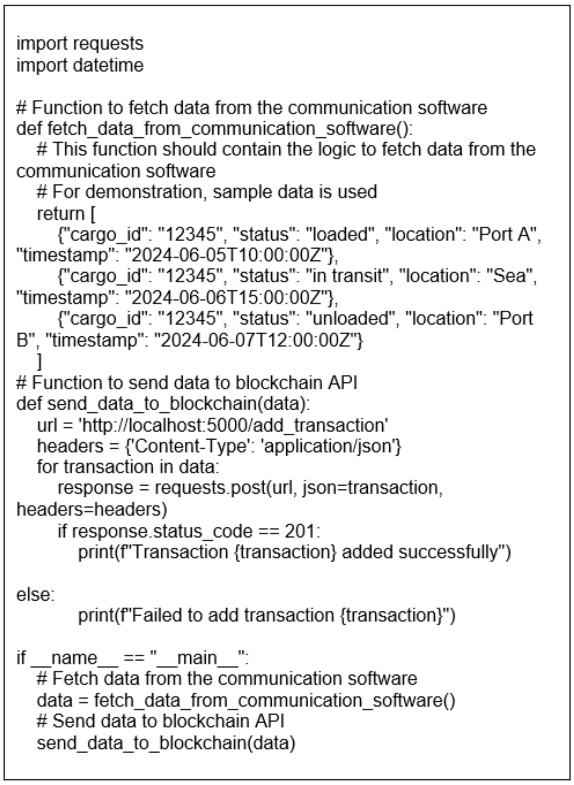
1. Shipping Company: Issues the Bill of Lading and manages the cargo;
2. Port Authority: Manages port operations and cargo loading/unloading;
3. Customs: Processes and clears cargo through customs;
4. Transporter: Handles the transportation of the cargo;
5. Recipient: Receives the cargo at the destination;
6. Verifier: Verifies the authenticity and correctness of the Bill of Lading;
7. Recipient: Final confirmation by the recipient upon delivery.

Each block in the blockchain represents a stage in the process, ensuring transparency and security throughout the shipping process.

VI. Experimental Verification and Software Implementation

The main code suggested and given in the Appendix A has been tested using the Python's built-in unittest framework. The unittest module in Python enables developers to validate the functionality of specific sections of code, such as individual functions, methods, or classes, by running them through a series of controlled cases. If the test code is saved to a Python file, it is possible to execute tests and report problems found, ensuring that the blockchain implementation works as expected. To integrate the blockchain code into a communication software application, the following steps should be completed: creation of API layer, transaction handling, and user interface. The API layer will allow communication software to interact with the blockchain. Functionality should be implemented to handle the addition and retrieval of transactions. Additionally, an interface will be needed to allow users to view and manage blockchain transactions. Further research by the authors will follow and will concern the integration of API with a communication software. For example, AmosConnect. It is used for email and data communications onboard ships. To integrate the blockchain API, a script or a service could be created that communicates with the blockchain API and interacts with the software. Below, in Fig. 4, an example how to create script that runs on the same network, which is a cron job that fetches data and sends them to the blockchain API is given.

As different shipborne software uses specific data formats and protocols, the data fetched and sent must be correctly structured and should comply with the data handling mechanisms. Additional parsing and data conversion functions could be implemented. The deployment of the blockchain API and the integration script on the ship's server or communication systems might take place as follows. Hosting the Flask API on a server will be accessible by the ship network. The integration.py script would be deployed on the same network and scheduled to run periodically (e.g., using cron jobs).



```
import requests
import datetime

# Function to fetch data from the communication software
def fetch_data_from_communication_software():
    # This function should contain the logic to fetch data from the
communication software
    # For demonstration, sample data is used
    return [
        {"cargo_id": "12345", "status": "loaded", "location": "Port A",
"timestamp": "2024-06-05T10:00:00Z"},
        {"cargo_id": "12345", "status": "in transit", "location": "Sea",
"timestamp": "2024-06-06T15:00:00Z"},
        {"cargo_id": "12345", "status": "unloaded", "location": "Port
B", "timestamp": "2024-06-07T12:00:00Z"}
    ]
# Function to send data to blockchain API
def send_data_to_blockchain(data):
    url = 'http://localhost:5000/add_transaction'
    headers = {'Content-Type': 'application/json'}
    for transaction in data:
        response = requests.post(url, json=transaction,
headers=headers)
        if response.status_code == 201:
            print(f"Transaction {transaction} added successfully")

else:
            print(f"Failed to add transaction {transaction}")

if __name__ == "__main__":
    # Fetch data from the communication software
    data = fetch_data_from_communication_software()
    # Send data to blockchain API
    send_data_to_blockchain(data)
```

Fig. 4. The script that runs on the same vessel network example.

It should be ensured that *fetch_data_from_communication_software* runs correctly retrieving data. Testing Data Submission would check if the *send_data_to_blockchain* function successfully adds transactions to the blockchain.

VII. Secure Communication Structure in Shipping

Establishing a secure communication structure in shipping involves implementing several essential stages to safeguard sensitive data, transactions, and communications throughout the maritime industry. Here is a detailed overview of each stage:

1. *Blockchain Layer*. At the core of the secure communication structure lies the blockchain layer. This utilises a distributed ledger technology where all transactions and communications pertinent to shipping

activities are recorded in a decentralised manner. Blockchain ensures transparency, immutability, and tamper-proof records. Smart contracts, integral to this layer, automate and enforce the terms of shipping agreements, reducing the need for intermediaries and enhancing operational efficiency.

2. *Encryption and Authentication*. To protect communications between parties, robust encryption and authentication mechanisms are employed: End-to-End Encryption: Ensures that all communications, including messages, documents, and transactional data, are encrypted from sender to recipient, preventing unauthorised access. Public key infrastructure (PKI) uses digital certificates and cryptographic keys to authenticate the identities of entities participating in shipping transactions, thereby ensuring secure communication channels.

3. *Access Control*. Access control mechanisms restrict data access to authorised personnel only. Role-based access control (RBAC) ensures that individuals within the shipping network have access only to the specific data and functions necessary for their roles, minimising the risk of data breaches. Multifactor authentication (MFA) adds an additional layer of security by requiring multiple forms of verification (e.g., password and biometric verification) before granting access.

4. *Network Security*. Securing the network infrastructure is critical to prevent unauthorised access and data breaches. The virtual private network (VPN) encrypts communication channels over public networks, such as the Internet, ensuring secure data transmission between different locations and entities. Firewalls and intrusion detection systems (IDS) act as barriers to unauthorised access attempts and monitor network traffic for suspicious activities, promptly alerting security personnel to potential threats.

5. *Data Integrity and Backup*. Ensuring the integrity and availability of data is essential to maintain operational continuity. Hashing algorithms generate unique cryptographic hashes for each data block recorded on the blockchain, facilitating data integrity verification and preventing unauthorised alterations.

Regular Backups maintain redundant copies of all data, stored securely and off-site, to mitigate the risk of data loss due to system failures, cyberattacks, or natural disasters.

6. *Audit and Compliance*. Regular audits and compliance management are crucial to ensuring adherence to industry regulations and standards. Regular Audits: Conduct periodic security audits to assess the effectiveness of security measures, identify vulnerabilities, and implement necessary improvements. Compliance management establishes and maintains compliance with maritime regulations, data protection laws (e.g., GDPR), and industry-specific standards to mitigate legal and regulatory risks.

7. *Incident Response and Recovery*: Preparedness for security incidents and data breaches is the key to minimising their impact. It is recommended to develop an incident response structured plan that outlines procedures for detecting, responding to, and mitigating security incidents promptly. Ensure that there is a comprehensive strategy in place for recovering data and restoring operations in the event of a data breach, cyber attack, or other emergency.

Each stage of this structured approach contributes specific security measures tailored to protect the integrity, confidentiality, and availability of data and communications within the shipping industry. By integrating these layers effectively, shipping companies can establish a comprehensive and resilient security framework that addresses current and emerging threats in maritime communications. Below on Fig. 5 is a suggestion how a blockchain enabled communication structure could be utilised in the shipping industry.

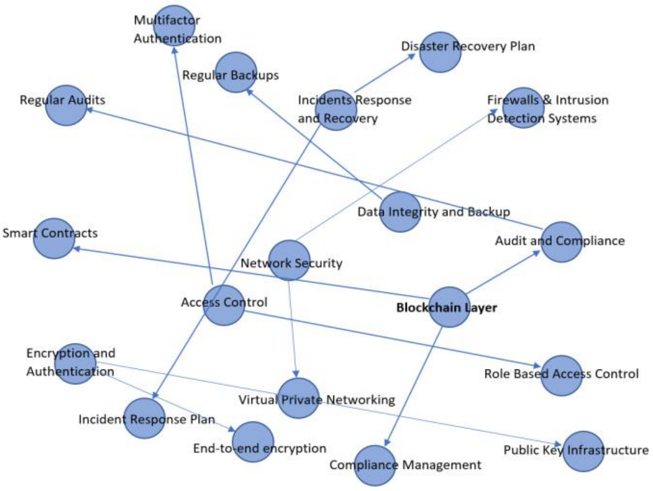

Multifactor Authentication
Regular Backups
Disaster Recovery Plan
Regular Audits
Incidents Response and Recovery
Firewalls & Intrusion Detection Systems
Data Integrity and Backup
Smart Contracts
Audit and Compliance
Network Security
Access Control
Blockchain Layer
Encryption and Authentication
Role Based Access Control
Virtual Private Networking
Incident Response Plan
End-to-end encryption
Public Key Infrastructure
Compliance Management

Fig. 5. Proposed secure communication structure for the shipping industry.

VIII. CONCLUSIONS

The integration of blockchain technology into maritime communication systems represents a significant advancement in enhancing security and efficiency. However, to fully realise the potential of blockchain in this sector, future experimental work is necessary. One promising area of research involves the development and testing of blockchain-based smart contracts tailored to automate complex maritime transactions, such as real-time cargo tracking and autonomous vessel operations. Additionally, experimental implementations of blockchain in conjunction with emerging technologies, such as the Internet of Things (IoT) and artificial intelligence (AI), could further strengthen the resilience and adaptability of maritime communication networks [15]. Informed decision-making, collaboration, and industry-wide adoption are crucial to realise the promise of blockchain in maritime communication. The transparency and immutability of the blockchain technology ensure tamper-proof records, enhancing trust and accountability, and offer a transformative path for the maritime industry. By streamlining processes and reducing paperwork, blockchain improves efficiency. Moreover, its security features prevent fraud and unauthorised access, making it a robust solution for secure communication. The following lines contain some recommendations for adoption to fully harness the potential of blockchain. First, *educate stakeholders*: Raise awareness of blockchain benefits and dispel misconceptions. Then *collaborate*: Involve shipping companies, port authorities, and regulators in shaping policies, as providing pilot projects can demonstrate value and build confidence. As a legal requirement, it is necessary to ensure compliance with maritime regulations and explore smart contract legal frameworks. These types of network should be scalable, so the blockchain should be optimised for high transaction volumes.

In conclusion, by harnessing the power of blockchain, the maritime sector can forge efficient, resilient, and reliable communication systems. Stakeholders in the intricate supply chain stand to benefit, ushering in a new era of maritime connectivity.

APPENDIX A

TABLE A-I. THE SUGGESTED CODE.

```
import hashlib
import datetime
class Block:
    def __init__(self, index, timestamp, data, previous_hash):
        self.index = index
        self.timestamp = timestamp
        self.data = data
        self.previous_hash = previous_hash
        self.hash = self.calculate_hash()
    def calculate_hash(self):
        return
hashlib.sha256(f"{self.index}{self.timestamp}{self.data}{self.previous
_hash}".encode()).hexdigest()

class Blockchain:
    def __init__(self):
        self.chain = [self.create_genesis_block()]

    def create_genesis_block(self):
        return Block(0, datetime.datetime.now(), "Genesis Block", "0")

    def get_latest_block(self):
        return self.chain[-1]

    def add_block(self, new_block):
        new_block.previous_hash = self.get_latest_block().hash
        new_block.hash = new_block.calculate_hash()
        self.chain.append(new_block)

# Initializing the blockchain network
shipping_blockchain = Blockchain()

# Function to add a new transaction
def add_transaction(data):
    latest_block = shipping_blockchain.get_latest_block()
    new_block = Block(latest_block.index + 1,
datetime.datetime.now(), data, latest_block.hash)
    shipping_blockchain.add_block(new_block)

# Example transactions
add_transaction({"cargo_id": "12345", "status": "loaded", "location":
"Port A", "timestamp": "2024-06-05T10:00:00Z"})
add_transaction({"cargo_id": "12345", "status": "in transit", "location":
"Sea", "timestamp": "2024-06-06T15:00:00Z"})
add_transaction({"cargo_id": "12345", "status": "unloaded",
"location": "Port B", "timestamp": "2024-06-07T12:00:00Z"})

# Tracking cargo
for block in shipping_blockchain.chain:
    print(vars(block))
```

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] S. E. Chang, Y. Chen, M. Lu, and H. L. Luo, “Development and evaluation of a smart contract–Enabled blockchain system for home care service innovation: Mixed methods study”, *JMIR Medical Informatics*, vol. 8, no. 7, p. e15472, 2020. DOI: 10.2196/15472.

[2] Blockchain Basics, Coursera, 2020. [Online]. Available: https://www.coursera.org/learn/blockchain-basics

[3] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the Internet of Things”, *IEEE Access*, vol. 4, pp. 2292–2303, 2016. DOI: 10.1109/ACCESS.2016.2566339.

[4] M. Dobrovnik, D. M. Herold, E. Fürst, and S. Kummer, “Blockchain for and in logistics: What to adopt and where to start”, *Logistics*, vol. 2, no. 3, p. 18, 2018. DOI: 10.3390/logistics2030018.

[5] L. Eremina, A. Mamoiko, and L. Bingzhang, “Use of blockchain technology in planning and management of transport systems*”, E3S Web of Conferences*, vol. 157, p. 04014, 2020. DOI: 10.1051/e3sconf/202015704014.

[6] F. Tian, “An agri-food supply chain traceability system for China based on RFID & blockchain technology”, in *Proc. of 2016 13th International Conference on Service Systems and Service Management (ICSSSM)*, 2016, pp. 1–6. DOI: 10.1109/ICSSSM.2016.7538424.

[7] K. S. Hald and A. Kinra, “The key challenges of blockchain implementation in the maritime sector”, Aalborg University Research Portal, 2020. [Online]. Available: https://vbn.aau.dk/en/publications/the-key-challenges-of-blockchain-implementation-in-maritime-sector

[8] Blockchain for Business, Topics, IBM. [Online]. Available: https://www.ibm.com/topics/blockchain

[9] V. R. Kebande, F. M. Awaysheh, R. A. Ikuesan, S. A. Alawadi, and M. D. Alshehri, “A blockchain-based multi-factor authentication model for a cloud-enabled Internet of Vehicles”, *Sensors*, vol. 21, no. 18, p. 6018, 2021. DOI: 10.3390/s21186018.

[10] M. Petković, V. Mihanović, and I. Vujović, “Blockchain security of autonomous maritime transport”, *Journal of Applied Engineering Science*, vol. 17, no. 3, pp. 333–337, 2019. DOI: 10.5937/jaes17-22740.

[11] P. Rahimi, N. D. Khan, C. Chrysostomou, V. Vassiliou, and B. Nazir, “A secure communication for maritime IoT applications using blockchain technology”, in *Proc. of 2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, 2020, pp. 244–251. DOI: 10.1109/DCOSS49796.2020.00047.

[12] J. Smith and C. Lee, “Challenges of implementing blockchain in maritime communication”, *IOSR Journal of Humanities and Social Science*, vol. 28, no. 10, pp. 50–55, 2023.

[13] K. Tam and K. Jones, “Cyber-risk assessment for autonomous ships”, in *Proc. of 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 2018, pp. 1–8. DOI: 10.1109/CyberSecPODS.2018.8560690.

[14] S. Tsiulin, K. H. Reinau, O.-P. Hilmola, N. Goryaev, and A. Karam, “Blockchain-based applications in shipping and port management: A literature review towards defining key conceptual frameworks”, *Review of International Business and Strategy*, vol. 30, no. 2, pp. 201–224, 2020. DOI: 10.1108/RIBS-04-2019-0051.

[15] U.S. Department of Transportation Maritime Administration, Blockchain Use Cases Final Report, 2020.

[16] K. Li, J.-Y. Lee, and A. Gharehgozli, “Blockchain implementation in the maritime industry: A literature review and synthesis analysis of benefits and challenges”, *Maritime Economics & Logistics*, vol. 26, pp. 630–657, 2024. DOI: 10.1057/s41278-023-00280-y.

[17] M. T. Taghavifard, R. Khezrian, and S. R. Sefidi, “Identification of stakeholders in personal health records using blockchain technology,” *J. Inf. Technol. Manag.*, vol. 13, no. 3, pp. 110–121, 2021. DOI: 10.22059/jitm.2024.366017.3498.

[18] T. Yang, Z. Cui, A. H. Alshehri, M. Wang, K. Gao, and K. Yu, “Distributed maritime transport communication system with reliability and safety based on blockchain and edge computing”, *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 2, pp. 2296–2306, 2023. DOI: 10.1109/TITS.2022.3157858.