Scientific and Social Research, 2025, Volume 7, Issue 2
https://ojs.bbwpublisher.com/index.php/SSR
Online ISSN: 2981-9946
Print ISSN: 2661-4332

Research on Blockchain-Enabled Resilience Building and Risk Prevention and Control in Shipping Supply Chains Under Multiple Crises

Wanqi Su*

College of Foreign Languages, Shanghai Maritime University, Shanghai 201306, China

***Corresponding author:** Wanqi Su, 2135658683@yeah.net

Copyright: © 2025 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

Abstract: Under the wave of economic globalization, the development of a global shipping network urgently requires the enhancement of supply chain resilience and risk prevention mechanisms. In recent years, the world has experienced multiple crises, including the public health crisis and the geopolitical crisis represented by the Red Sea shipping crisis. These crises have severely impacted international logistics and supply chains. The public health crisis has led to disconnections between production and demand, increased trade barriers, and higher shipping costs. The suspension and rerouting of the Red Sea shipping route via the Cape of Good Hope have resulted in extended shipping times, delayed deliveries, and soaring freight rates. The widespread application of blockchain technology can alleviate these issues. This paper investigates the positive effects of blockchain technology's high transparency, automated risk control, and promotion of multi-party collaboration in addressing current crises, enhancing shipping supply chain resilience, and strengthening risk management. The paper aims to contribute to cost reduction, quality improvement, and high-quality development of international logistics.

Keywords: Blockchain; Shipping supply chain; Risk management; Decentralization

Online publication: March 10, 2025

1. Introduction

1.1. Current pain points in shipping development

The global shipping industry is facing a digital transformation wave. However, the current progress of shipping digitalization is hindered by several pain points, such as information asymmetry and data silos, contract disputes, legal adaptation delays, lagging risk response and rigid emergency mechanisms, and the contradiction between technology and cost. Under public health and geopolitical crises, these pain points in shipping digitalization have impeded the process of economic globalization and increased the difficulty of international trade.

1.2. Supply-demand imbalance under public health crisis impact

Geopolitical conflicts have forced shipping companies to reroute their vessels to avoid high-risk areas (e.g., bypassing the Red Sea region), increasing transportation costs and time. It is estimated that the cost of rerouting via the Cape of Good Hope is 15%–20% higher than that of the Suez Canal route, with additional risks of piracy. Moreover, trade sanctions have directly cut off some supply chain nodes, leading to the fragmentation of the global energy transportation network.

1.3. Logistics route restructuring triggered by regional disputes

Geopolitical conflicts have forced shipping companies to reroute their vessels to avoid high-risk areas (e.g., bypassing the Red Sea region), increasing transportation costs and time. It is estimated that the cost of rerouting via the Cape of Good Hope is 15%–20% higher than that of the Suez Canal route, with additional risks of piracy. Moreover, trade sanctions have directly cut off some supply chain nodes, leading to the fragmentation of the global energy transportation network.

1.4. Increased coordination difficulty of multimodal transport

The lockdown of ports (e.g., the temporary suspension of some operations at the Port of Shanghai) and insufficient railway capacity (e.g., the strained capacity of the China-Europe Railway Express) during 2019 have exposed the fragility of coordination across different transportation modes. For example, the blockage of the Suez Canal in 2021 triggered a "domino effect" in the global supply chain, affecting ports, highways, and warehousing systems [1].

Furthermore, low efficiency in multi-party collaboration is also hindering global shipping trade. In the event of sudden risks, coordination across enterprises and governments is required, but traditional communication methods (e.g., emails and phone calls) are inefficient. During the 2021 Suez Canal blockage, the lack of a collaborative scheduling platform led to a 48-hour delay in dredging decisions, resulting in global trade losses exceeding USD 10 billion [2].

2. Theoretical and practical significance

The core characteristics of blockchain technology are highly compatible with the needs of the shipping supply chain.

2.1. Decentralization and multi-party collaboration

The shipping industry involves multiple stakeholders such as shipowners, ports, and freight forwarders. Blockchain technology breaks down information silos through a distributed ledger, ensuring real-time data sharing (e.g., the TradeLens platform connects global shipping nodes) and avoiding the single-point failure risk of traditional centralized systems [3].

2.2. Data immutability and trust mechanism

Key information such as cargo status and contract terms, once recorded on the blockchain, cannot be tampered with and is highly traceable. This reduces the risks of bill of lading forgery and cargo damage liability disputes. For example, electronic bills of lading with blockchain notarization can shorten dispute resolution time by 60% [4].

2.3. Smart contracts and process automation

Smart contracts automatically execute rules such as freight payment and insurance claims, reducing manual intervention and operational delays. Maersk's use of smart contracts has improved cross-border settlement efficiency by 80% while

lowering the risk of breach of contract [5].

2.4. Transparency and risk control optimization

Full-chain data transparency helps in the real-time identification of anomalies (e.g., deviation from the shipping route, temperature control failure). Combined with AI prediction models, it enables early warning and enhances supply chain resilience.

The blockchain technology studied in this paper, which reconstructs trust through technology, is becoming a core tool for the shipping industry to cope with the fragmentation of globalization and improve collaborative efficiency.

3. Theoretical basis and technical architecture

3.1. Blockchain technology principles

3.1.1. Distributed ledger

The core mechanism of a distributed ledger is that data is stored in a shared ledger across multiple participating nodes, with each node independently maintaining a complete copy of the data. Consistency is ensured through synchronization mechanisms. For example, the status of goods in shipping (e.g., location, temperature, and humidity) is jointly recorded by shipping companies, ports, and freight forwarders. The failure of any single node does not affect the overall system operation. Distributed ledgers break down the single-point failure risk of traditional centralized databases, enhancing supply chain transparency and resistance to attacks.

3.1.2. Consensus mechanism

The consensus mechanism ensures that all nodes reach an agreement on ledger updates to prevent malicious tampering. Typical consensus algorithms include as following.

PBFT (Practical Byzantine Fault Tolerance): Suitable for consortium chains, it allows consensus to be reached even if up to 1/3 of the nodes are malicious. It is fast (in milliseconds) and suitable for high-real-time scenarios (e.g., synchronization of vessel arrival information at ports). It can support thousands of transactions per second (TPS), meeting the high-frequency needs of shipping operations such as bill of lading circulation and customs clearance.

PoW (Proof of Work): High energy consumption and slow speed, mainly used in public chains (e.g., Bitcoin), and not suitable for shipping.

Comparing the two algorithms, PBFT is more efficient in a scenario with known trusted nodes (e.g., members of a shipping consortium) and can support thousands of transactions per second (TPS), meeting the trading needs of shipping.

3.1.3. Smart contracts

Smart contracts are automated agreements based on code that execute operations automatically when predefined conditions are triggered (e.g., payment, cargo release). These smart contracts can be applied to freight payment and document verification: after cargo receipt, the smart contract calls the bank's API to complete freight payment, eliminating payment delays (e.g., Maersk and IBM's automated insurance claims); automatically verifying the bill of lading and letter of credit information reduces the error rate of manual review (case: Rotterdam Port's blockchain customs clearance system shortened clearance time by 70%). This enhances the efficiency of shipping transaction processes.

3.1.4. Cryptography

Cryptography typically includes the following.

Asymmetric Encryption: Using a public-private key system to ensure controllable data access permissions. For example, after the shipper signs the bill of lading with a private key, customs can verify its authenticity with the public key to prevent forgery.

Hash Algorithm: Converts data (e.g., contract text) into a fixed-length hash value, where any modification results in a change in the hash value, ensuring data integrity. In shipping, it is used to verify whether cargo status records have been tampered with (e.g., temperature data in cold chain logistics).

3.2. Blockchain type selection: The suitability of consortium chains for shipping

3.2.1. Comparison of public, private, and consortium chains

Public Chain (e.g., Ethereum): Fully open with anonymous nodes, but low performance (e.g., Ethereum's TPS is about 15), and public data, which does not meet the privacy needs of shipping.

Private Chain: Centrally controlled (e.g., owned by a single enterprise), which contradicts the multi-party collaboration scenario in shipping.

Consortium Chain: The optimal choice, maintained by pre-selected organizations (e.g., shipping companies, ports, banks), balancing efficiency and privacy. Typical frameworks include Hyperledger Fabric and R3 Corda.

3.2.2. Core advantages of consortium chains in shipping

Permission Control: Node access requires voting by consortium members to prevent malicious participation (e.g., restricting unauthenticated freight forwarders from joining).

Performance Optimization: Through efficient consensus mechanisms such as PBFT, high throughput can be achieved (Hyperledger Fabric's TPS can reach over 2000), meeting the high-frequency trading needs of shipping.

Data Privacy Grading: Supports channel technology to isolate different business data. For example, the bill of lading data is shared between the shipper and customs, while fuel purchase information is only accessible to shipping companies and suppliers.

Compliance: Meets regulatory requirements such as GDPR and supports data localization storage (e.g., data from European port nodes is stored only on EU-based servers).

4. Risk management

Shipping supply chain risk management requires a systematic approach to potential threats in each link. The framework consists of four stages.

4.1. Risk identification

The goal of risk management is to identify potential threats to the supply chain. This can be achieved through the following methods.

PESTEL Analysis: Identifies macro risks such as political (e.g., sanctions), economic (e.g., exchange rate fluctuations), and technological (e.g., hacker attacks).

Process Mapping: Locates vulnerable nodes through supply chain process diagrams (e.g., dependency on a single port).

Typical risks in shipping trade include:

Operational Risks: Such as pirate attacks (a 50% increase in pirate attacks in the Red Sea in 2023) and crew shortages (a global deficit of over 100,000 crew members).

Market Risks: Such as freight rate volatility (the Shanghai Containerized Freight Index (SCFI) has an annual fluctuation rate of over 200%).

Compliance Risks: Such as fines for exceeding carbon emission limits (the IMO's Carbon Intensity Indicator (CII) took effect in 2023).

4.2. Risk Assessment

The following models illustrate the application of blockchain technology in risk assessment.

Quantitative Analysis: Calculating the probability and impact of risks

Monte Carlo Simulation: Predicting the probability and cost losses of extreme weather causing port closures.

Value-at-Risk (VaR) Model: Estimating the potential impact of freight rate volatility on corporate cash flow.

4.3. Risk response

Based on risk identification and assessment, blockchain technology can provide different strategies for navigation to achieve relatively low-cost, low-risk, and high-efficiency route design. These strategies include:

Avoidance Strategy: Rerouting to avoid high-risk routes.

Mitigation Strategy: Diversifying supply sources and strengthening technology.

Transfer Strategy: Purchasing war risk insurance and supply chain interruption insurance (global shipping insurance premiums increased by 18% in 2022).

Acceptance Strategy: Reserving emergency budgets for low probability/low impact risks (e.g., minor customs delays).

4.4. Risk monitoring

Through real-time data tracking, KPI alerting, and periodic auditing, closely monitor shipping-related data, integrate diverse resources, and ensure real-time follow-up of shipping information. Real-time data tracking involves integrating data sources such as AIS (vessel positioning), weather, and political dynamics on the blockchain platform. KPI alerting can be achieved by setting thresholds (e.g., triggering an alarm if port stay time exceeds 72 hours) and linking smart contracts to initiate emergency procedures. Periodic auditing involves reviewing supply chain resilience quarterly (e.g., the effectiveness of alternative supplier plans).

5. Specific applications of blockchain in shipping supply chains

5.1. Automated risk identification

Blockchain technology can integrate historical data on-chain, for example:

Vessel Accident Data: Shipping companies and insurance firms upload accident records (e.g., collisions, mechanical failures) to the blockchain. Each record includes fields such as time, location, cause, and loss amount, with digital signatures to ensure authenticity.

Supplier Credit Ratings: Third-party rating agencies (e.g., Lloyd's Register) write suppliers' compliance and on-time delivery rates into the chain, with data updates verified through consensus mechanisms.

Real-Time Operational Data: IoT devices collect data such as vessel position (AIS), engine status, and cargo temperature and humidity, synchronizing it in real-time to blockchain nodes.

5.2. Collaborative assessment and response

Blockchain smart contracts can execute cross-organizational data in a joint manner, achieving multi-layer data linkage, for example:

Pirate Alert Triggering: Through off-chain oracles (Oracle) connected to the International Maritime Bureau's (IMB) real-time pirate activity database, if a particular sea area reports ≥2 pirate attacks within 24 hours, it is marked as a high-risk zone.

Vessel Dynamic Monitoring: Blockchain synchronizes AIS data of vessels. If a vessel enters a high-risk zone without requesting an escort, the smart contract is triggered.

In addition to data warning and monitoring, blockchain can also complete further responses:

Notify Shipowners: The smart contract calls the shipowner's reserved API interface (e.g., enterprise WeChat, Slack) to push warning information and suggestions (e.g., request escort, change route). Coordinate with Insurers: The contract automatically generates a warning record and sends it to the insurance company's system to initiate a quick claim preparation process (e.g., pre-review policies, and prepare rescue funds).

Blockchain technology upgrades traditional passive risk management, which relies on manual labor, to a data-driven active defense system through automated risk identification and collaborative response. This enhances risk response efficiency, precise decision-making, and supply chain resilience.

6. Retrospect and prospect

6.1. Research conclusions

Blockchain technology demonstrates significant value in shipping supply chains and risk management. The complexity and globalization of shipping supply chains make them susceptible to multidimensional risks, necessitating a systematic management framework. Blockchain technology enhances supply chain resilience by improving data transparency, automating processes, and facilitating multi-party collaboration.

6.2. Challenges and risks

However, the widespread application of blockchain still faces real challenges.

Technical Limitations: Mainstream consortium chains (e.g., Hyperledger Fabric) have a throughput of about 2000 TPS, which is insufficient to support large-scale global shipping networks (with daily data points in the hundreds of millions).

Legal Conflicts: The EU's eIDAS (Electronic Identification and Trust Services) Regulation has not yet recognized the legal validity of blockchain bills of lading, leading to the detention of 12 batches of blockchain-based goods by Italian customs in 2023.

Ecosystem Fragmentation: There are currently 27 shipping blockchain platforms worldwide that are incompatible with each other. The annual data interoperability cost between COSCO's GSBN and Maersk's TradeLens is as high as USD 3 million.

Blockchain is driving the transformation of shipping supply chains from "experience-driven" to "data-intelligent," but continuous breakthroughs are needed in technical performance, legal adaptation, and ecosystem integration.

Disclosure statement

The author declares no conflict of interest.

References

[1] Liu X, 2025, Digitalization of Bills of Lading Accelerates the Green Transition of Trade. International Commerce News, Trade and Investment, February 14, 2025, 3.

[2] Shi CL, Li FY, 2024, Suggestions for China to Enhance International Logistics Supply Chain Security under the Red Sea Shipping Crisis. Journal of the Ministry of Transport Management Cadre College, 34(4): 12–18.

[3] Kjaergaard-Winther C, 2022, A.P. Moller-Maersk and IBM to Discontinue TradeLens, A Blockchain-enabled Global Trade Platform. https://www.maersk.com/news/articles/2022/11/29/maersk-and-ibm-to-discontinue-tradelens

[4] Zhou B, 2024, Research on Shipping Supply Chain Security under the Red Sea Crisis. China Maritime, 2024(8): 63–65. https://doi.org/10.16831/j.cnki.issn1673-2278.2024.08.020

[5] Zheng JY, 2018, IBM and Maersk Aim to Use Blockchain Platforms to Break Down Shipping Barriers. Tianjin Navigation, 2018(3): 77.

Publisher's note

Bio-Byword Scientific Publishing remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.