Journal of
Marine Science and Engineering

MDPI

Article

Blockchain-Based Cold Chain Traceability with NR-PBFT and IoV-IMS for Marine Fishery Vessels

Zheng Zhang , Haonan Zhu and Hejun Liang *

College of Engineering Science and Technology, Shanghai Ocean University, Shanghai 201306, China;
z-zhang@shou.edu.cn (Z.Z.); 18021009135@163.com (H.Z.)
* Correspondence: hjliang@shou.edu.cn

Abstract: Due to limited communication, computing resources, and unstable environments, traditional cold chain traceability systems are difficult to apply directly to marine cold chain traceability scenarios. Motivated by these challenges, we construct an improved blockchain-based cold chain traceability system for marine fishery vessels. Firstly, an Internet of Vessels system based on the Iridium Satellites (IoV-IMS) is proposed for marine cold chain monitoring. Aiming at the problems of low throughput, long transaction latency, and high communication overhead in traditional cold chain traceability systems, based on the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm, a Node-grouped and Reputation-evaluated PBFT (NR-PBFT) is proposed to improve the reliability and robustness of blockchain system. In NR-PBFT, an improved node grouping scheme is designed, which introduces a consistent hashing algorithm to divide nodes into consensus and candidate sets, reducing the number of nodes participating in the consensus process, to lower communication overhead and transaction latency. Then, a reputation evaluation model is proposed to improve the node selection mechanism of NR-PBFT. It enhances the enthusiasm of nodes to participate in consensus, which considers the distance between fishery vessels, data size, and refrigeration temperature factors of nodes to increase throughput. Finally, we carried out experiments on marine fishery vessels, and the effectiveness of the cold chain traceability system and NR-PBFT were verified. Compared with PBFT, the transaction latency of NR-PBFT shortened by 81.92%, the throughput increased by 84.21%, and the communication overhead decreased by 89.4%.

Keywords: blockchain; marine fishery vessel; traceability; PBFT

check for updates

Citation: Zhang, Z.; Zhu, H.; Liang, H. Blockchain-Based Cold Chain Traceability with NR-PBFT and IoV-IMS for Marine Fishery Vessels. *J. Mar. Sci. Eng.* **2024**, *12*, 1371. https://doi.org/10.3390/jmse12081371

Received: 12 July 2024
Revised: 1 August 2024
Accepted: 9 August 2024
Published: 11 August 2024

1. Introduction

Traditional marine cold chain traceability systems often store data related to various stages in centralized databases. The storage method does not guarantee transparency between enterprises, connectivity of upstream and downstream information, or the security and reliability of data. Fraud in marine cold chain products is often reported, which could impact food safety [1]. Developing a trustworthy, transparent, and decentralized marine cold chain traceability system is a crucial research topic that urgently needs to be solved by the academic community and food regulatory agencies [2].

The marine cold chain traceability system is specifically designed to trace and monitor the entire process of cold chain products in the marine environment, from fishing and processing to transportation [3]. The system ensures that fishery products are always in optimal condition during transportation and storage by monitoring and recording parameters [4,5]. However, traditional marine cold chain traceability systems often face problems such as data opacity, information silos, and traceability difficulty, leading to food safety hazards. Blockchain technology is fundamentally a distributed ledger that combines multiple core technologies, including P2P networks, consensus mechanisms, cryptographic algorithms, and smart contracts [6]. It features decentralization, immutability, and traceability [7]. The concept of blockchain was first proposed by a scholar named Satoshi Nakamoto in

2008 [8]. With the development of related technologies, blockchain has incorporated smart contracts and cryptographic algorithms. Due to the high reliability and decentralization of blockchain, combining it with traditional marine cold chain traceability systems can solve many problems faced by traditional cold chain traceability systems [9]. It is also applied to fields such as cybersecurity [10], healthcare [11], cold chain management [12], and agricultural traceability [13], offering new solutions for traditional fishery product cold chain traceability problems [14]. Based on different application scenarios and participant permissions, blockchain is categorized into public, private, and consortium chains [15].

Public chains are fully decentralized, allowing any individual or organization to participate in or exit the network. Private chains are used within specific entities or organizations, with participation requiring authorized permission [16]. Consortium chains, which lie between public and private chains, consist of a group of known and trusted nodes, and any node or organization must obtain authorization to join. Consortium chains provide participants with a secure, efficient, and trustworthy environment, ensuring transparency and information sharing among organizations [17]. Compared to public chains, consortium chains have advantages such as high throughput, fast transaction speed, and privacy protection. The comparison of the three types of blockchain is shown in Table 1 below [18].

Table 1. Comparison of the characteristics of the three blockchains.

Blockchain Type	Participation Permission	Decentralization Level	Transaction Speed	Consensus Algorithm
Public Chain	Open to everyone	Fully decentralization	Slow	PoW/PoS/DpoS
Private Chain	Specified individuals or companies	Centralization	Fast	PBFT/RAFT
Consortium chain	Consortium members	Polycentralization	Fast	PBFT/RAFT

Each of the three blockchain types has its unique application scenarios and advantages. In the marine environment, limited communication, computing resources, and unstable environments on fishery vessels affect data transmission and processing and lead to system performance degradation and operational delays, impacting overall efficiency and reliability [19]. Current research shows that consortium chains reduce the complexity and bandwidth consumption of data transmission by limiting the number of participating nodes and selecting trusted nodes [20]. Therefore, consortium chains are promising for cold chain traceability scenarios. Leveraging the unique characteristics and advantages of consortium chains, many researchers have begun to apply them to traditional fishery product cold chain traceability systems, thereby facilitating their widespread application in the field. Zhang et al. developed a fishery product traceability system based on blockchain and the Internet of Things (BIOT-TS), which enhanced data management efficiency and ensured data security and reliability. However, the BIOT-TS system did not optimize the consensus algorithm based on actual scenarios. As the number of nodes increases, the system's response slows down when dealing with a large number of transactions, affecting traceability efficiency [21]. Facing challenges such as traceability difficulties and data tampering in the fishery supply chain, P.K. and colleagues improved the traceability efficiency and the quality safety of fishery products by integrating blockchain technology with traditional fishery product cold chain systems. Although it solves the problems of traceability difficulty and data tampering, it ignores the optimization of the consensus algorithm, resulting in high communication overhead [22]. Syam, M.M. and others used mini containers for the cold chain transportation of vegetables and fruits, reducing energy consumption and greenhouse gas emissions, and avoiding food and energy waste caused by cold chain failures. Although the safety issues of cold chain food have been resolved, further improvement is needed in terms of cold chain traceability efficiency [23]. M and others applied blockchain technology to the fishery supply chain, constructing a traceability system that reduced the possibility of data tampering, which enhanced food safety. But the consensus algorithm is not optimized, resulting in low efficiency [24]. Liu and Yu used the theory of stochastic Petri nets to construct a blockchain e-commerce cold chain traceability system model, solving the problem of difficult e-commerce cold chain traceability. However, the model not only has high complexity but also fails to consider consensus algorithm optimization, which may result in latency issues when handling transactions [25]. The above studies highlight the application of blockchain with traditional traceability systems. They seldom explore the security and efficiency problems of consensus algorithms in traditional cold chain traceability systems. In the practical environment of the marine fishery, the distance between fishery vessels, data size, and refrigeration temperature factors of nodes can affect communication quality and data transmission. Directly applying blockchain to marine cold chain traceability systems faces problems of low throughput, long transaction latency, and high communication overhead.

Consensus algorithms are the cornerstone of ensuring the security and reliability operation of blockchain networks [26]. Their primary function is to ensure that every node in the blockchain network records and stores data according to unified standards [27]. Current research shows that the PBFT algorithm has good fault tolerance in consortium chains. Therefore, the PBFT algorithm is one of the most widely applied consensus algorithms in consortium chains [28]. Compared to other consensus algorithms like Raft [29] and Kafka [30], PBFT demonstrates superior fault tolerance in the presence of Byzantine nodes. However, in the PBFT algorithm, the selection of the primary node is usually conducted through a round-robin mechanism, which could potentially allow malicious nodes to become primary nodes. If a malicious node becomes the primary node, it can pose a serious threat to the entire network's consensus algorithm [31]. Moreover, as the number of participating nodes in the marine cold chain traceability system increases, using the traditional PBFT algorithm will significantly increase the communication overhead of the system, making it unsuitable for large-scale environments [32].

To solve the problems of low throughput, long transaction latency, and high communication overhead in the marine cold chain traceability scenarios, we propose an improved consensus algorithm—NR-PBFT. Firstly, a node grouping scheme is designed based on a consistent hash algorithm to reduce the number of consensus nodes. Then, a reputation evaluation model is proposed, considering the distance between fishery vessels, data size, and refrigeration temperature factors in marine scenarios, to select highly reliable nodes. Finally, the node grouping scheme is adopted to optimize the consensus protocol processing of the PBFT algorithm in the preparation stage, submission stage, and response stage. NR-PBFT improves the throughput and reduces the transaction latency of the original PBFT algorithm. Some properties of the study which differ from the previous ones are summarized as follows:

(1) An improved PBFT consensus algorithm is proposed for a blockchain-based marine fishery cold chain traceability system.

(2) A node grouping scheme is designed based on a consistent hashing algorithm. It reduces the number of consensus nodes, improves the scale supported by the blockchain network, and optimizes the consensus protocol processing of the PBFT to reduce the communication overhead.

(3) To select highly reliable nodes, a reputation evaluation model is proposed. It updates the selection mechanism of consensus and leader nodes to reduce the probability of malicious nodes becoming leader nodes and the transaction latency.

The remainder of the paper is organized as follows: Section 2 describes the design of a blockchain-based cold chain traceability system for marine fishery vessels; Section 3 proposes an NR-PBFT algorithm; Section 4 analyzes the results of experiments; and Section 5 provides corresponding experimental conclusions and future work directions.

2. Design of a Blockchain-Based Cold Chain Traceability System for Marine Fishery Vessels

2.1. Communication Method

2.1.1. IoV-IMS Architecture

The IoV-IMS architecture is designed for marine cold chain monitoring. As illustrated in Figure 1, the IoV-IMS architecture is primarily composed of three major components: the shipboard data acquisition system, the shipboard data processing and transmission system, and the shore-based data receiving system. These components work together to achieve communication between the vessels and shore-based facilities. By using the S1-I Iridium Short Burst Data (SBD) module, communication between vessels and the shore is achieved. The module transmits data to the Iridium Ground Gateway. Iridium Ground Gateway not only improves signal stability but also decodes and preliminarily processes data. Finally, the data are transmitted to the shore-based storage server through the core switch.

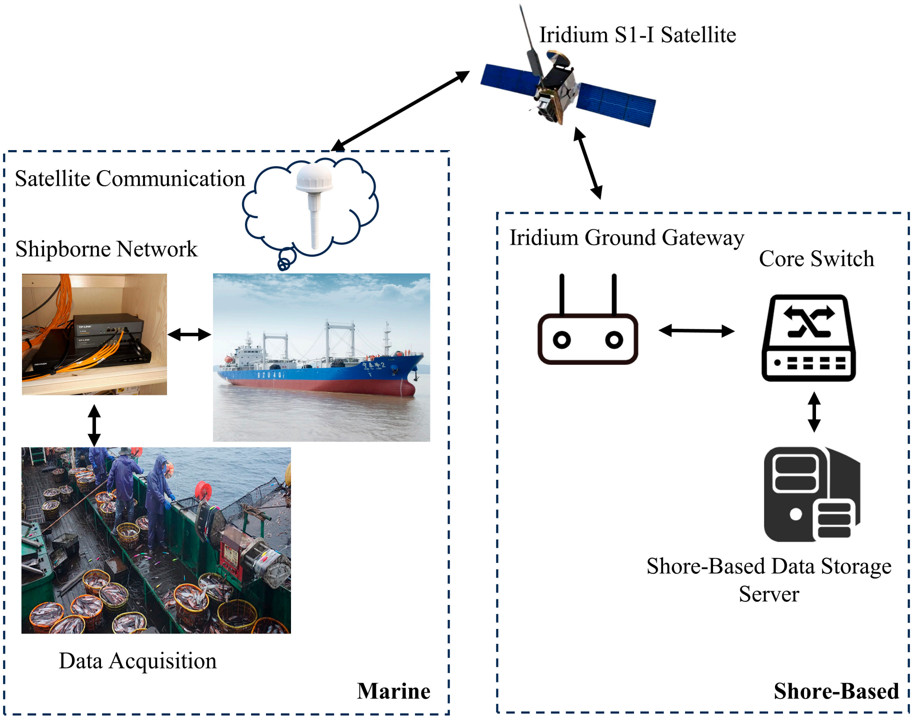


Figure 1. IoV-IMS architecture.

2.1.2. Data Acquisition System

Figure 2 shows the communication architecture of the data acquisition system, aimed at collecting and transmitting critical data. The system employs many devices including RFID reader–writer devices, GPS modules, weight sensors, time-recording modules, as well as temperature recorders and sensors within three refrigerated warehouses. These components are directly connected to the shipboard personal computer (SPC) by a 485 bus. The data include detailed information obtained through RFID devices, geographic locations by GPS modules, the weight of the catch measured by weight sensors, and temperature data of the refrigerated warehouses monitored by temperature sensors. Temperature recorders provide comprehensive records of refrigeration temperatures. All critical cold chain transportation data are transmitted to the shore-based storage server by the Iridium S1-I terminal connected to the SPC.

To monitor the temperature in the refrigerated warehouses, PT100 sensors are selected for the study. Operators can set upper and lower temperature thresholds on the SPC. Once the temperature inside the refrigerated warehouses exceeds or falls below the set threshold, the system will automatically trigger an alarm mechanism. The temperature data collected by the PT100 sensors are recorded by the temperature recorders. Finally, these data are transmitted to the SPC.

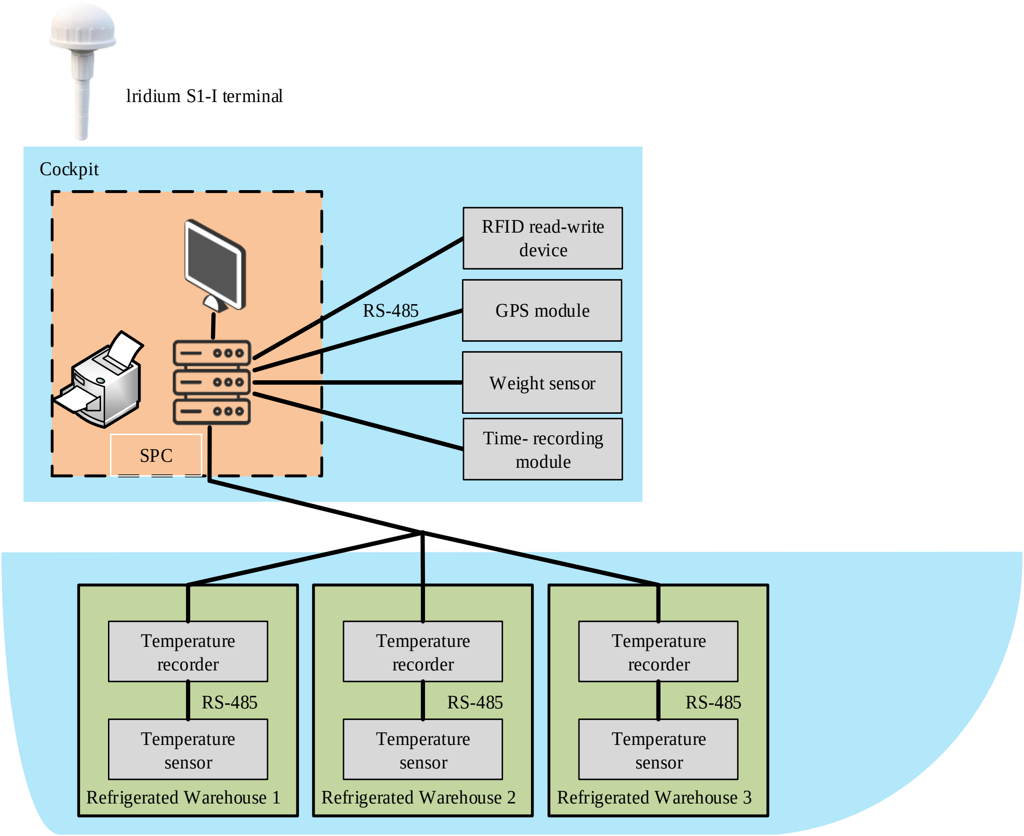


Figure 2. Architecture of data acquisition system.

2.1.3. Data Processing System

For a marine cold chain traceability system, key data such as refrigeration temperature, species and grade of catches, and quantity of catch are crucial. These data are transmitted to the Iridium Ground Gateway through the Iridium S1-I terminal connected to the SPC. The number of bytes of each data point is shown in Table 2.

Table 2. The number of bytes of key data.

Attribute	Bytes
Vessel number	1
Species and grade of catches	1.5
Catching position	8
Catching time	6
Quantity of catch	3
Processing time	6
Refrigeration temperature	2
Refrigeration time	6
Uploading position	8
Uploading time	6

Vessel number, occupying 1 byte; species and grade of catches, occupying 3.5 bytes; catching position: the position of a vessel in longitude and latitude, represented as 0.5 bytes (range), 1.5 bytes (degrees), 1 byte (minute), and 1 byte (second), for a total of 8 bytes; catching time, including year, month, day, hour, minute, and second, represented by one byte each, totaling 6 bytes; quantity of catch, expressed in kg, sharing 3 bytes; processing time, including year, month, day, hour, minute, and second, represented by one byte each, totaling 6 bytes; refrigeration temperature: the temperature is a signed number, accurate to one tenth of a degree, occupying 2 bytes; refrigeration time, including year, month, day, hour, minute, and second, represented by one byte each, totaling 6 bytes; uploading position: the position of a vessel in longitude and latitude, represented as 0.5 bytes (range), 1.5 bytes (degrees), 1 byte (minute), and 1 byte (second), for a total of 8 bytes; uploading time, including year, month, day, hour, minute, and second, represented by one byte each, totaling 6 bytes.

2.2. Design of the Blockchain-Based Cold Chain Traceability System

How to construct a transparent cold chain traceability system is challenging in marine fisheries. This study designs a blockchain-based cold chain traceability system for marine fishery vessels, including catching link, shipboard processing, shipboard refrigeration, marine transportation, and fishing port unloading. The system not only ensures the transparency of information but also solves the problems of the low throughput, long transaction latency, and high communication overhead of the cold chain for marine fishery vessels. The design of the cold chain for marine fishery vessels is shown in Figure 3.

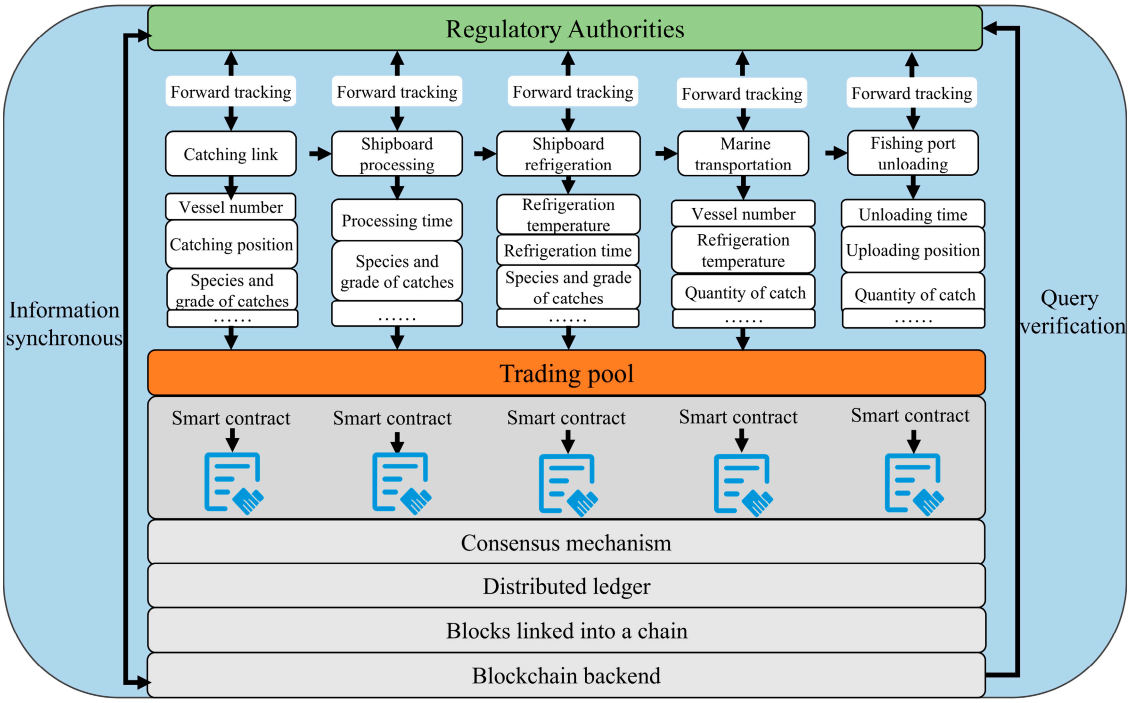


Figure 3. Cold chain traceability system model for marine fishery vessels.

The description of the procedures of the cold chain traceability system for marine fishery vessels is as follows:

(1) Catching Link: The locations of catches are recorded using GPS devices, with the data input into blockchain nodes. Through communication technology, the catch data are shared and broadcasted to the blockchain network for consensus. Once consensus is achieved, the messages are packaged into blocks.

(2) Shipboard Processing: During shipboard processing, sensors monitor environmental data such as temperature. These data are input into the blockchain. The cold chain information is synchronized to the blockchain network, where nodes authenticate blocks and update the ledger using consensus algorithms, ensuring that the data for each step are up-to-date and immutable.

(3) Shipboard Refrigeration: A temperature control system is used to monitor the temperature of the refrigerated warehouses. These data are transmitted to the blockchain, ensuring the stability and transparency of the cold chain traceability system.

(4) Marine Transportation: During transportation, IoT devices collect relevant data to ensure the quality of the catch.

(5) Fishing port unloading: Upon unloading at the fishing port, RFID technology is used to scan each tag, recording the unloading information into the blockchain.

3. Design of NR-PBFT Consensus Algorithm

Castro M. and Liskov B. proposed the PBFT algorithm in a paper titled "Practical Byzantine Fault Tolerance" [33]. The algorithm reduces the complexity of the Byzantine fault-tolerant algorithm from the exponential to polynomial level and is considered one of the best algorithms to solve Byzantine problems. It consists of a consensus protocol, view change protocol, and checkpoint protocol [34]. However, in the practical marine fishery environment, the PBFT algorithm still has some limitations, including low throughput, lack of an effective reputation evaluation model, and the arbitrariness of the primary node selection process. These drawbacks not only increase the communication cost of the algorithm but also reduce the consensus enthusiasm of nodes, as it cannot reward loyal nodes or punish malicious nodes. At the same time, malicious nodes may become the primary nodes, further reducing the consensus efficiency of the entire system [35].

Aiming at the above problems, we propose a Node-grouped and Reputation-evaluated PBFT (NR-PBFT). The NR-PBFT algorithm consists of a node grouping scheme, consensus process, reputation evaluation model, and Byzantine node detection mechanism.

3.1. Node Grouping Scheme

As shown in Figure 4, initially, the identifiers (vessel number) of the marine fishery vessel nodes are hashed to generate hash values. Subsequently, multiple virtual nodes are introduced for each actual node to enhance the uniformity of the hash ring, thereby avoiding data skew problems caused by the uneven distribution of actual nodes. Following this, both actual nodes and virtual nodes are arranged on the hash ring according to their hash values, forming an orderly hash ring [36]. Finally, nodes are grouped based on their positions on the hash ring. The blockchain network comprises N nodes in total, with the number of consensus nodes denoted as A and the number of candidate nodes as B, maintaining a ratio of A:B = 3:2. The nodes are divided into m groups, with m nodes randomly selected to serve as the initial leader for each group. Nodes within the candidate node set only update their local states upon reaching consensus and temporarily do not participate in the consensus process. Assuming that there are a total of 30 nodes in the blockchain network divided into five groups, the grouping process of nodes is presented in Figure 5.

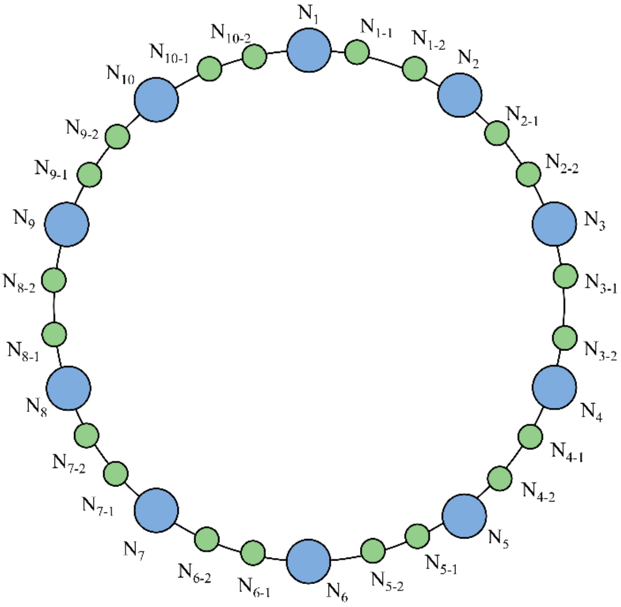


Figure 4. A hash ring with virtual nodes.

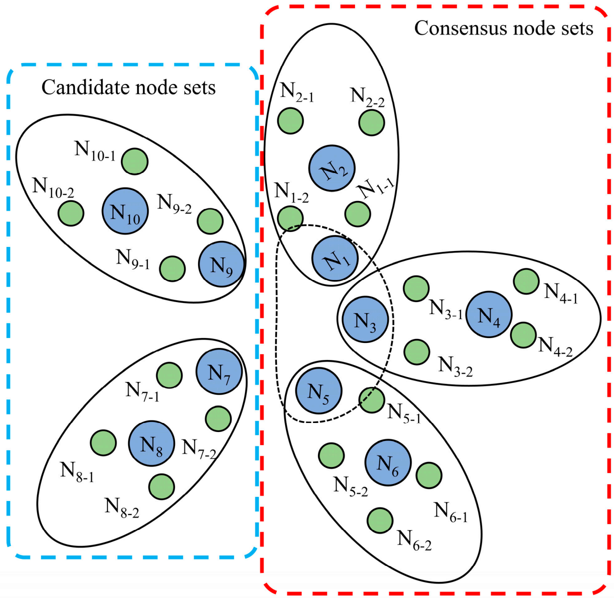


Figure 5. Grouping process.

3.2. NR-PBFT Consensus Process

The overall process of NR-PBFT is illustrated in Figure 6. Initially, all marine fishery vessel nodes are initialized and grouped into consensus and candidate sets. During the consensus process, groups validate and achieve consensus on request from clients. If a group timeout occurs, the process is reinitialized; if not, each group randomly selects a leader node. The group first reaches consensus within the consensus set, and then the leader node participates in consensus outside of the consensus set. It checks whether the consensus processing times out; if the transaction of any node times out, it is added to a danger list. If no timeout occurs, the consensus processing concludes. After the consensus concludes, each node's score and state are updated. Then, the system's leader node is optimally selected to reduce the possibility of Byzantine nodes becoming leader nodes.

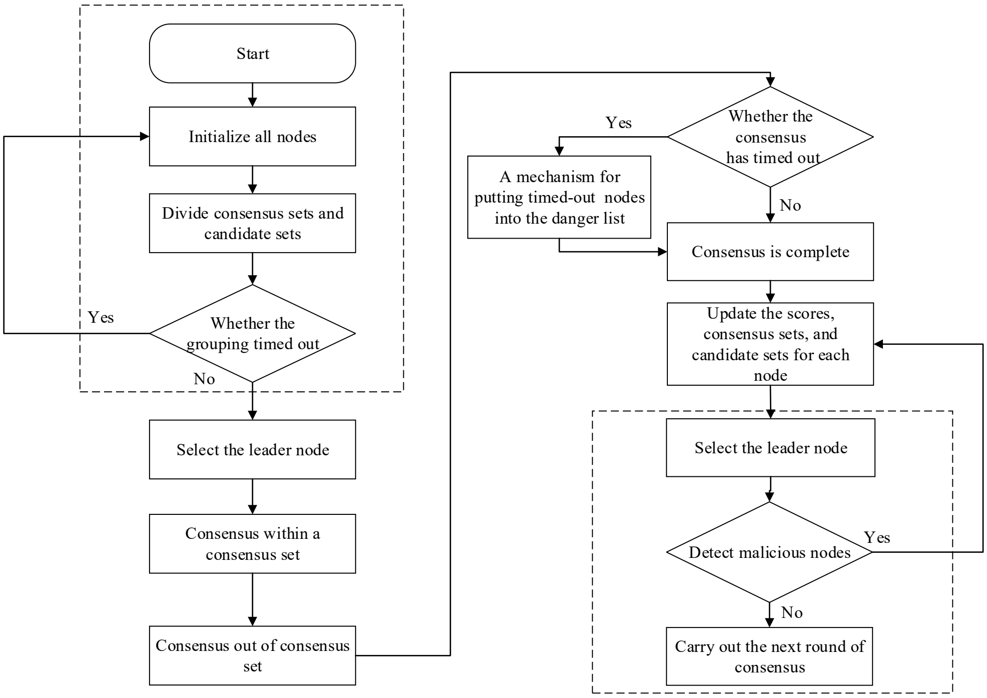

Start
Initialize all nodes
Divide consensus sets and candidate sets
Yes
Whether the grouping timed out
No
Select the leader node
Consensus within a consensus set
Consensus out of consensus set
Yes
Whether the consensus has timed out
A mechanism for putting timed-out nodes into the danger list
No
Consensus is complete
Update the scores, consensus sets, and candidate sets for each node
Select the leader node
Detect malicious nodes
Yes
No
Carry out the next round of consensus

Figure 6. Flowchart of NR-PBFT.

3.3. Reputation Eevaluation Model

In marine fishery satellite communication, the distance between fishery vessels, data size, and refrigeration temperature factors of nodes can affect the communication quality. Therefore, to analyze the impact of factors on communication quality, we consider factors for the reputation score calculation formula.

As for NR-PBFT, each node starts with an initial reputation score of 60. The higher the reputation score, the more trustworthy the node is considered. Nodes are categorized into five status levels based on their reputation scores: Excellent, Good, Normal, Abnormal, and Malicious. According to the different status of each node, corresponding weight coefficients are different, as shown in Table 3.

Table 3. Five types of node hierarchy criteria and corresponding weights.

Reputation Score	Node Status	Weight Coefficient
$G_p \geq 90$	Excellent	1.5
$80 \leq G_p < 90$	Good	1.2
$70 \leq G_p < 80$	Normal	1.0
$60 \leq G_p < 70$	Abnormal	0.7
$G_p < 60$	Malicious	0

Normal nodes have a reputation score between 70 and 80, which is the minimum standard to ensure participation in consensus. Nodes with scores below the range will be expelled from the blockchain system. Rewards and penalties for nodes are allocated based on their performance during the consensus process and their respective reputation levels. The specific formula for calculating the reputation score of a node is as follows:

(1) Punishment Rules

If the leader node or any node within the group fails to participate in the consensus outside the group, or if the nodes within the group do not successfully synchronize data, the reputation score calculation formula is expressed by (1):

$$G_p(k+1) = \alpha G_p(k),\ (0 < \alpha < 1) \tag{1}$$

When a node sends different messages to different nodes or incorrect messages, the reputation score calculation formula is expressed by (2):

$$G_p(k+1) = 0 \tag{2}$$

(2) Reward Rules

The parameters that affect satellite communication as standardized, such as the distance between fishery vessels, data size, and refrigeration temperature, to be between 0 and 1:

The standardized formula for the distance D between fishery vessels is expressed by (3):

$$D_{norm} = \frac{D}{D_{max}} \tag{3}$$

where D_{max} = 50, unit: nmi.

The standardized formula for the size S of data is expressed by (4):

$$S_{norm} = \frac{S}{S_{max}} \tag{4}$$

Here, S_{max} = 300, unit: Byte.

The standardized formula for refrigeration temperature T_r is expressed by (5):

$$T_{r,norm} = \frac{T_r - T_{r,min}}{T_{r,max} - T_{r,min}} \tag{5}$$

Here, $T_{r,min}$ = −30 °C and $T_{r,max}$ = 10 °C.

When a new block is generated, the reputation score of the node based on various factors is expressed by (6), and each factor is expressed by (7) and (8), respectively:

$$G_p(k+1) = G_p(k)(1 + f(D_{norm}, S_{norm})g(T_{r,norm})) \tag{6}$$

$$f(D_{norm}, S_{norm}) = \frac{1}{1 + e^{(D_{norm} - S_{norm})}} \tag{7}$$

$$g(T_{r,norm}) = \frac{1}{1 + e^{T_{r.norm}}} \tag{8}$$

In this context, G_p denotes the reputation score of node p, $k+1$ refers to the $k+1$ round of consensus, and α is the penalty index, which is set to 0.8 in this study.

To ensure that the reputation score $G_p(k+1)$ is between 0 and 100, the reputation score calculation formula is expressed by (9):

$$G_p(k+1) = min\big(100, max\big(0, G_p(k+1)\big)\big) \tag{9}$$

Although the individual performance of nodes is crucial when selecting a leader node, the level and weights of the nodes within the group help to balance the competitive relationships between nodes, ensuring that the chosen leader node has higher overall credibility and reliability. The final reputation score calculation formula for the leader node is as follows:

$$R_p = \beta * G_p(k) + (1-\beta) * \frac{1}{mN}\sum_{i=1}^{\frac{N}{m}} W_i G_i(k) \tag{10}$$

Within the framework, β serves as a proportionality constant, $\beta = 0.6$. A greater R_p score represents the possibility of a node being elected as the leader, which is instrumental in avoiding the participation of Byzantine nodes in the consensus process, improving reliability and robustness.

3.4. Optimized Consensus Protocol

The NR-PBFT consensus algorithm includes the original PBFT's prepare, commit, and reply phases and further divides the three stages into intra-group and out-group processes, as illustrated in Figure 7. The optimized consensus protocol of NR-PBFT comprises seven steps, described as follows:

The client C sends a transaction message $< REQUEST, t_x, t, c, C_{sig} >$ to each leader node of the consensus set, where t_x represents the transaction content, t is the timestamp, c is the client identifier, and C_{sig} is the client's signature.

Upon receiving the transaction message, the leader node verifies and orders the client message. Subsequently, it encapsulates this into a prepare message designated for the consensus set $< IN - PREPARE, n, v, t, D(m) > L_i$, and broadcasts it to intra-group members. Here, n is the message sequence number, v is the view number, $D(m)$ is the message digest, and L_i is the signature of the leader node i.

After receiving the message, intra-group members verify its correctness and reasonableness. If it passes verification, they will send a commit message, $< IN - COMMIT, n, v, t, D(m) > R_i$, back to the leader node, where R_i is the signature of the intra-group node i.

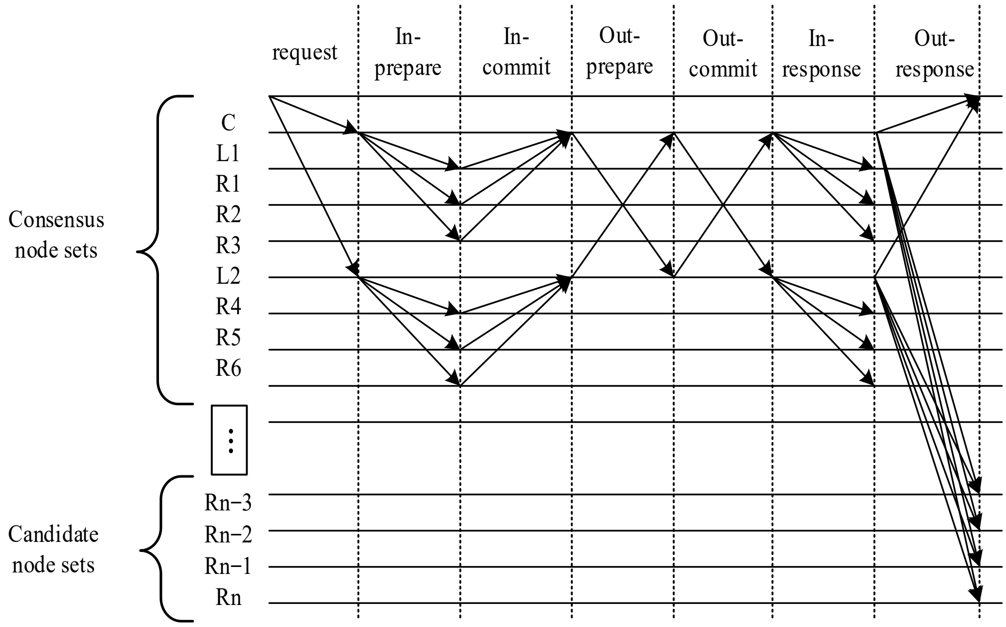


Figure 7. Seven-stage process of NR-PBFT algorithm.

Once the leader node receives a sufficient number of confirmations from the consensus set members and verification is successful, it signifies that the intra-group consensus is complete. The leader node then participates in the global consensus on behalf of each consensus set and broadcasts the prepared out-group message $< OUT - PREPARE, n, v, t, D(m) > L_i$ to all leader nodes.

Each leader node receives and verifies the incoming messages. If a message fails verification, it is cleared. If more than $2f$ validated messages are received, then an $< OUT - COMMIT, n, v, t, D(m) > L_i$ message is broadcast to other leader nodes.

Each leader node validates the received messages, and upon receiving more than $2f$ validated messages, it broadcasts the packaged $< IN - RESPONSE, n, v, t, D(m) > L_i$ to the intra-group nodes.

The leader node finally responds to the client with $< OUT - RESPONSE, n, v, t, D(m) > L_i$, marking the end of the consensus process.

3.5. Byzantine Node Detection Mechanism

In the blockchain network of the marine fishery, nodes are categorized into leader nodes, replica nodes, candidate nodes, monitor nodes, and Byzantine nodes. Leader nodes represent the consensus group in external consensus participation. Replica nodes first achieve consensus within the group before broadcasting the consensus results to the leader nodes. Candidate nodes are potential consensus participants. Monitor nodes primarily coordinate view changes within the network and collect reputation information sent by the leader nodes. Byzantine nodes represent those that are malfunctioning or exhibiting malicious performance due to system failures.

The mechanism's overall flow is shown in Figure 8 below. The Byzantine node detection mechanism is initiated before the start of the next consensus round. The leader node sends a probe message $< TEN - REQUEST, t, c, l, L_{sig} >$ to all nodes; t is the timestamp, c is the content of message, l represents the identifier of the leader node, and L_{sig} is the leader's signature.

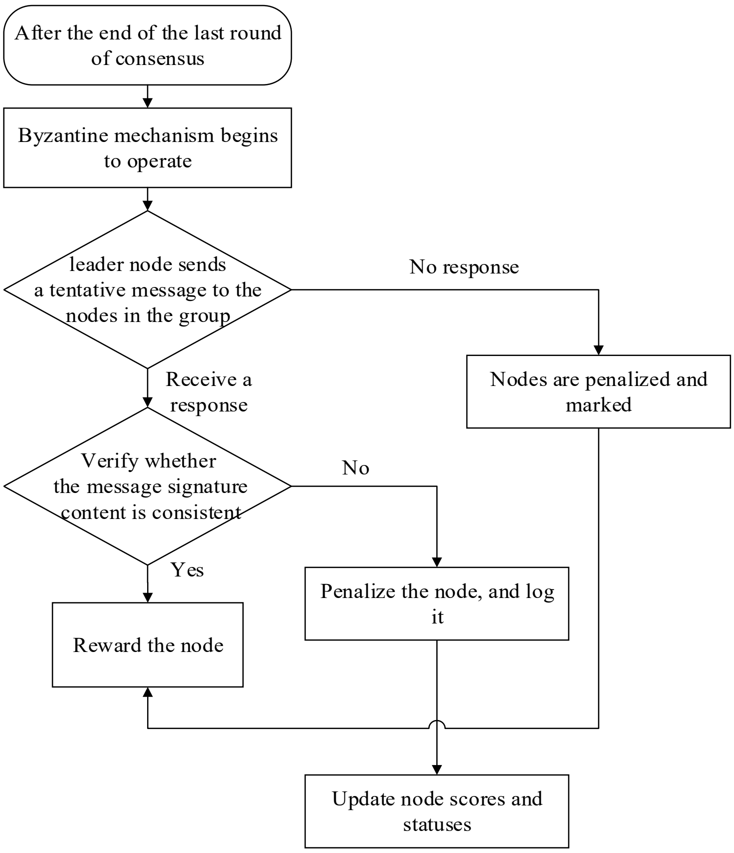

After the end of the last round of consensus
Byzantine mechanism begins to operate
leader node sends a tentative message to the nodes in the group
No response
Nodes are penalized and marked
Receive a response
Verify whether the message signature content is consistent
No
Yes
Penalize the node, and log it
Reward the node
Update node scores and statuses

Figure 8. Flow chart of the Byzantine node detection mechanism.

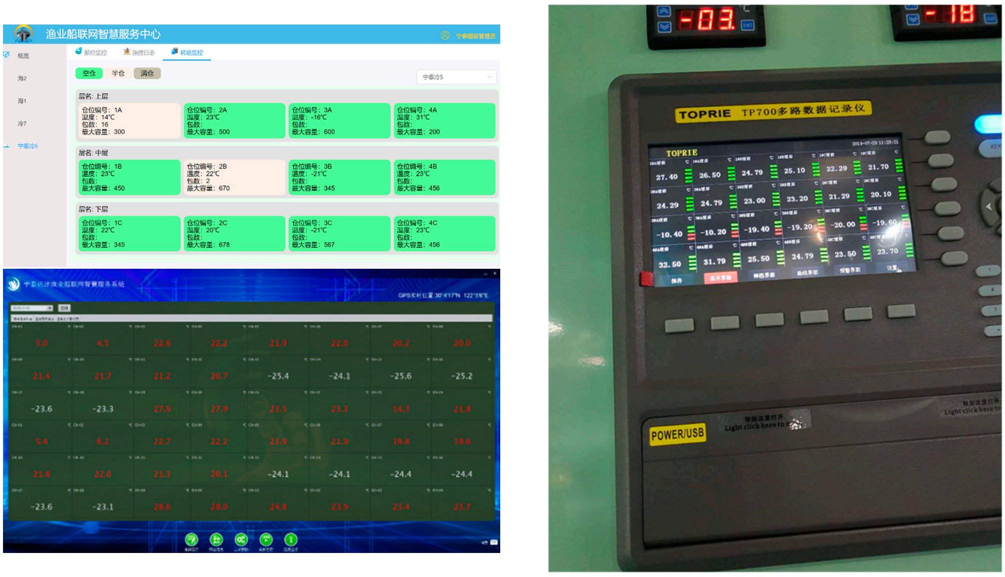
If the leader node receives a response from any node, it is necessary to verify the authenticity and consistency of the response. The process starts with the validation of the node's signature to ensure that the message is indeed from that node and has not been altered. Subsequently, the content of the messages from different nodes is compared to check for consistency. Nodes that provide consistent responses are rewarded accordingly; if the leader node does not receive a response or receives a malicious message, appropriate penalties are applied. Following this, the scores and statuses of the nodes are updated.

4. Experimental Results and Discussion

4.1. Experimental Setup and Parameters

4.1.1. Experimental Scenario

To verify the performance of the improved PBFT algorithm in the constructed marine cold chain traceability system, we carried out experiments on marine fishery vessels from Zhoushan Ningtai Marine Fisheries Co., Ltd. in Zhoushan, Zhejiang Province, China. Marine fishery vessel nodes communicate with the shore-based server by Iridium satellites to upload the related data. Marine fishery vessels operate in the North Pacific, Southeast Pacific, Southwest Atlantic, and Indian Ocean regions. These vessels are equipped with advanced temperature control systems to ensure the freshness and high quality of the catch, as illustrated in Figure 9. Figure 9a displays the temperature data, number of packages, and capacity of the warehouse. The red number indicates an alarm when the temperature exceeds the upper and lower limits, while the white number indicates a normal temperature.



渔业船联网智慧服务中心 宁泰超级管理员

概览 海2 海1 冷7 宁泰冷5

船位监控 渔捞日志 转运监控

空仓 半仓 满仓 宁泰冷5

层名: 上层

仓位编号：1A 温度：14°C 包数：16 最大容量：300	仓位编号：2A 温度：23°C 包数： 最大容量：500	仓位编号：3A 温度：-16°C 包数： 最大容量：600	仓位编号：4A 温度：31°C 包数： 最大容量：200

层名: 中层

仓位编号：1B 温度：23°C 包数： 最大容量：450	仓位编号：2B 温度：22°C 包数：2 最大容量：670	仓位编号：3B 温度：-21°C 包数： 最大容量：345	仓位编号：4B 温度：23°C 包数： 最大容量：456

层名: 下层

仓位编号：1C 温度：22°C 包数： 最大容量：345	仓位编号：2C 温度：20°C 包数： 最大容量：678	仓位编号：3C 温度：-21°C 包数： 最大容量：567	仓位编号：4C 温度：23°C 包数： 最大容量：456

5.0	4.5	22.6	22.2	21.9	22.0	20.2	20.0
21.4	21.7	21.2	20.7	-25.4	-24.1	-25.6	-25.2
-23.6	-23.3	27.9	27.9	23.5	23.3	14.3	21.8
5.4	6.2	22.7	22.2	21.9	21.9	19.8	19.6
21.8	22.0	21.3	20.1	-24.1	-24.1	-24.4	-24.4
-23.6	-23.1	28.6	28.0	24.8	23.9	23.4	23.7

(**a**) (**b**)

Figure 9. Temperature monitoring system: (**a**) onboard monitoring software and (**b**) temperature monitoring host.

4.1.2. Experimental Parameters

PBFT, KBFT, GPBFT, and the proposed NR-PBFT are applied to the marine cold chain traceability system for comparative analysis. The comparison focuses on four key metrics: transaction latency, throughput, communication overhead, and security. The initial reputation score for all nodes is set to 60. During the experiments, clients concurrently sent 500 transactions, with every 50 transactions being packed into a single block. The configuration details for the experiments are shown in Table 4.

Table 4. Experiment setting.

Experiment Setting	Configuration
CPU	Intel Core i5-12450H 2.0 GHz
Memory	16GB DDR4
Operating System	Windows 11
Total number of nodes	20–60
Number of groups	4–12
Initialize reputation score	60

4.2. Transaction Latency

In a blockchain system, transaction latency refers to the time it takes for a transaction request from a client node to reach consensus among all nodes in the blockchain network. In the experiments, the number of nodes increases from 20 to 60, with a step size of 5. To ensure generality, 20 transactions are repeated under different numbers of nodes, and the final transaction latency value for different numbers of nodes is the average of 20 transactions. A lower transaction latency implies a faster consensus process. The latency formula is expressed as follows:

$$Delay_t = T_{end} - T_{start} \tag{11}$$

In Equation (11), $Delay_t$ represents the transaction latency of transaction t, T_{end} denotes the time taken for the block containing the transaction to be confirmed, and T_{start} indicates the time at which the client sends the transaction.

Figure 10 illustrates the variation in transaction latency for PBFT, KBFT, GPBFT, and the proposed NR-PBFT as the number of nodes in the network increases. The abscissa represents the total number of nodes in the network, while the ordinate represents the transaction latency.

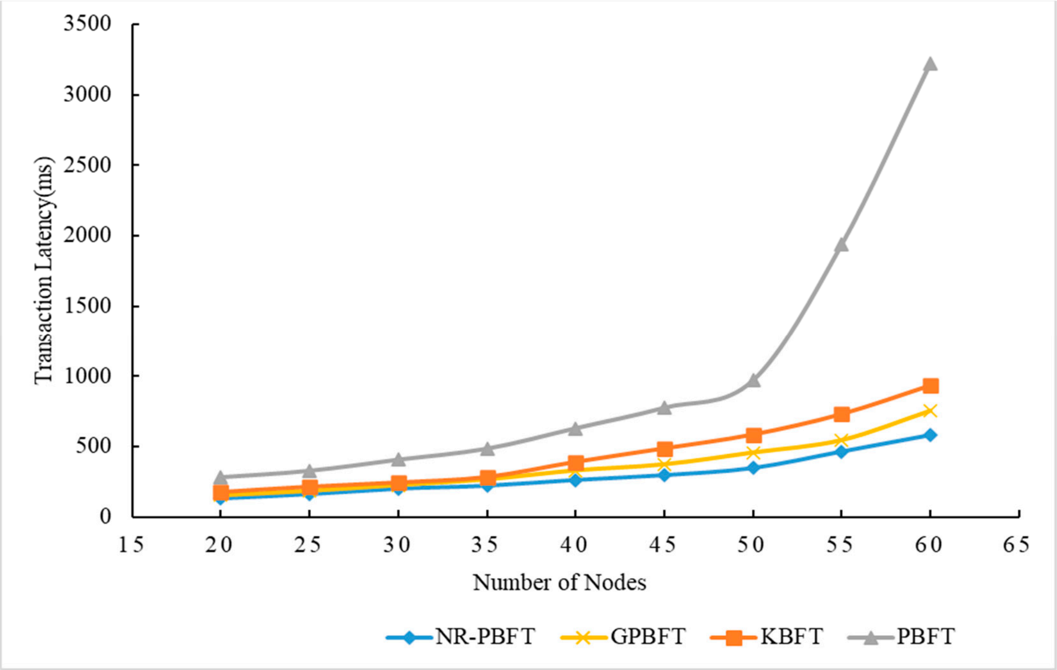


Figure 10. Comparison of transaction latency of NR-PBFT, GPBFT, KBFT, and PBFT.

It is observed that at the same node count, PBFT, KBFT, and GPBFT exhibit a higher transaction latency compared to NR-PBFT. As the number of nodes varies while processing the same volume of transactions, the transaction latency for all algorithms increases with the number of nodes. The transaction latency for the improved PBFT consistently remains lower than that of PBFT, KBFT and GPBFT. When the number of nodes is below 35, the transaction latency for the four consensus algorithms ranges between 100 ms and 500 ms. As the number of nodes in the network continues to grow, the transaction latency of PBFT, KBFT, and GPBFT rapidly increases. When the number of nodes reaches 60, the transaction latency of PBFT increases to 3226 ms, the transaction latency of KBFT increases to 934 ms, and the transaction latency of GPBFT increases to 754 ms. In contrast, NR-PBFT maintains a transaction latency of 583 ms, which is 81.92%, 37.58%, and 22.67% lower than PBFT, KBFT and GPBFT, respectively.

Due to the lack of an effective node grouping scheme and the optimization of consensus protocol, the transaction latency of PBFT, KBFT, and GPBFT increases rapidly with the increase in the number of nodes. In contrast, the NR-PBFT algorithm, with its improved node grouping scheme and optimized consensus protocol, limits the selection of leader nodes to those with high credibility. It not only reduces the possibility of Byzantine nodes becoming leader nodes but also decreases the frequency of view changes, thus maintaining a lower transaction latency. Therefore, under the same network conditions, the transaction latency of PBFT, KBFT, and GPBFT is higher than that of NR-PBFT.

4.3. Throughput

Throughput refers to the number of transactions that a system completes within a unit of time. It is a key indicator for evaluating the transaction processing speed of a blockchain and is typically denoted by Transactions Per Second (TPS). In the experiment, the number of nodes is set to increase from 20 to 60, with a step size of five, and for generality, 20 transactions are repeatedly conducted under different numbers of nodes.

The final transaction latency value for different numbers of nodes is the average of these 20 transactions. The calculation formula is as follows:

$$TPS = \frac{TX_{total}}{T_{total}} \tag{12}$$

In Equation (12), TX_{total} represents the total number of transactions and T_{total} denotes the total time spent on the exchange. The unit of throughput is T_x/s.

To evaluate the performance of NR-PBFT in terms of throughput, the study compares PBFT, KBFT, GPBFT, and NR-PBFT across different numbers of nodes. The higher throughput indicates that the network can process more transactions, demonstrating greater processing efficiency. Figure 11 shows the trends in throughput changes for PBFT, KBFT, GPBFT, and NR-PBFT as the number of nodes increases. The abscissa represents the total number of nodes in the network, while the ordinate represents the throughput.

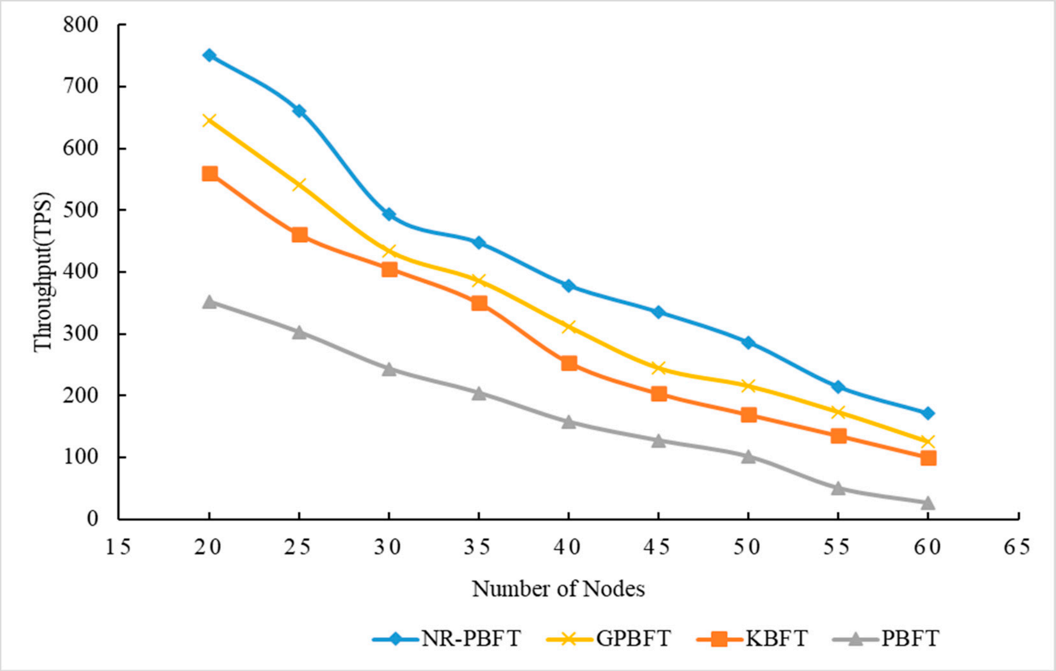


Figure 11. Comparison of throughput of NR-PBFT, GPBFT, KBFT, and PBFT.

It can be seen that, under the same experimental conditions, NR-PBFT consistently exhibits higher throughput than the other three algorithms. When the number of nodes is 20, the difference in throughput among the four algorithms is the most significant. The throughput of NR-PBFT is 106TPS higher than GPBFT, 191TPS higher than KBFT, and 399TPS higher than PBFT, respectively. As the number of network nodes increases, the throughput for all algorithms shows a declining trend. When the number of nodes reaches 60, PBFT's throughput is 27TPS, KBFT's is 101TPS, GPBFT's is 126TPS, and NR-PBFT's is 171TPS, which is 84.21%, 40.93%, and 26.31% higher than PBFT, KBFT, and GPBFT respectively.

Due to the lack of a specific reputation evaluation model, PBFT, KBFT, and GPBFT are unable to effectively reward or penalize nodes. This deficiency prevents the system from prioritizing consensus nodes and leader nodes with good reputations, thereby failing to achieve improvements in transaction processing speed and efficiency. The reputation evaluation model of NR-PBFT is designed specifically for traceability scenarios in marine cold chains. Considering the distance between fishery vessels, refrigeration temperature, and data size in the traceability scenario of the marine cold chain, the reliability and robustness of the system are improved.

4.4. Communication Overhead

Communication overhead refers to the amount of communication generated by nodes during the consensus process. The NR-PBFT consensus algorithm reduces communication overhead by decreasing the number of consensus nodes and optimizing the consensus protocol within the PBFT consensus algorithm.

4.4.1. Analysis of PBFT Communication Overhead

The communication overhead of PBFT mainly occurs during the pre-prepare, prepare, commit, and reply phases. Assuming there are N nodes in the system, during the pre-prepare phase, the primary node communicates $(N-1)$ times; during the prepare phase, each node sends a message to all other nodes except itself, resulting in $(N-1)^2$ communications; during the commit phase, each node broadcasts a message to all other nodes, amounting to $N\ (N-1)$ communications.

Let the total number of communications in PBFT be denoted as C_1; the calculation is as follows in Equation (13):

$$C_1 = N - 1 + (N-1)^2 + (N)(N-1) = 2N^2 - 2N \tag{13}$$

4.4.2. Analysis of NR-PBFT Communication Overhead

The improved PBFT adds a grouping phase, and the node consensus process includes stages such as intra-group prepare, intra-group commit, out-group prepare, out-group commit, intra-group response, and out-group response. Assuming there are m consensus sets in the system, during the intra-group prepare phase, the number of communications is $\left[\left(\frac{3N}{5}-1\right)/m-1\right]*m$; in the intra-group commit phase, each member of the consensus set sends a message to the lead node for commit, and the number of communications is $\left[\left(\frac{3N}{5}-1\right)/m-1\right]*m$; in the out-group prepare phase, each lead node broadcasts a prepare message to other lead nodes, and the number of communications is $m\ (m-1)$; and in the intra-group commit phase, each lead node verifies the received messages and broadcasts them to other lead nodes, and the number of communications is $m\ (m-1)$.

Let the total number of communications in NR-PBFT be denoted as C_2; the number of communications in NR-PBFT is as follows:

$$C_2 = m + 2 * \left[\frac{3N-5}{5m} - 1\right] * m + 2m(m-1) \tag{14}$$

Assuming $m = \frac{3N}{5q}$, where m is any positive integer greater than 3, and q denotes the number of members in the consensus set $(q = 5)$ when $N > 20$, $C_2 < C_1$.

Figure 12 shows the change in consensus communication overhead of four consensus algorithms when there are more and more system nodes.

The abscissa represents the total number of nodes in the network, while the ordinate represents the communication overhead. When the number of nodes is 20, the difference in communication overhead among the four algorithms is the smallest. The communication overhead of NR-PBFT is 116 times lower than GPBFT, 257 times lower than KBFT, and 536 times lower than PBFT. As the number of nodes increases, the communication overhead of the four algorithms tends to increase. The communication overhead of PBFT increases the fastest, while the growth rate of NR-PBFT is the slowest. When the number of nodes reaches 60, PBFT's communication overhead is 7080, KBFT's is 1350, GPBFT's is 1047, and NR-PBFT's is 748, which is 89.4%, 44.5%, and 28.5% lower than PBFT, KBFT, and GPBFT, respectively. The reduction in communication overhead in the marine cold chain traceability system not only improves the traceability efficiency of the system but also reduces the operating costs of the system.

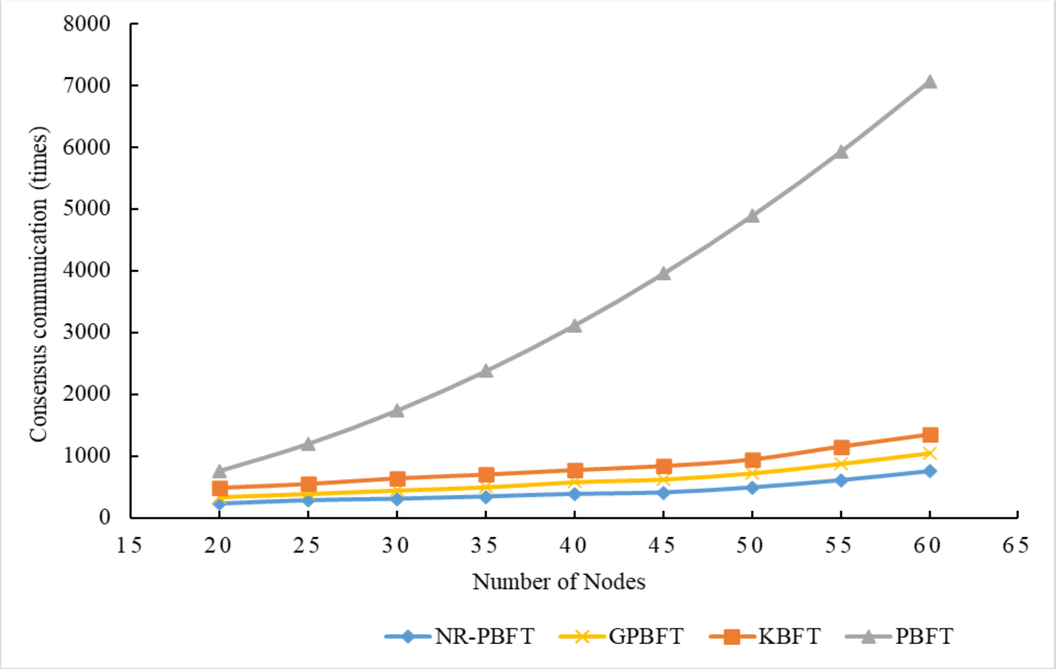


Figure 12. The communication overload of four consensus algorithms.

4.5. Security

Due to the lack of a reputation evaluation model, the PBFT consensus algorithm fails to effectively penalize Byzantine nodes, allowing them to persist in the blockchain network and thus weakening the overall system security. To solve the problem, the NR-PBFT algorithm introduces a Byzantine node detection mechanism. Through this mechanism, once the system detects a malicious node, it immediately reduces the node's reputation value to zero and removes it from the blockchain network. It reduces the possibility of Byzantine nodes becoming primary nodes, thereby enhancing the security of the blockchain network. The comparison of the number of Byzantine nodes in the PBFT and NR-PBFT consensus algorithms is shown in the following Figure 13.

To evaluate the performance of NR-PBFT in terms of security, Byzantine nodes are deliberately introduced into the system, and the trend of the number of Byzantine nodes changes with the increase in consensus rounds observed. The total number of nodes is set to 45, and the NR-PBFT consensus algorithm randomly divides the nodes into groups using the consistent hashing algorithm, with the ratio of consensus node set to candidate node set being 3:2, resulting in 27 consensus nodes. Since the PBFT and NR-PBFT consensus algorithms all have a certain fault tolerance to Byzantine nodes, the number of Byzantine nodes is set to six. It is assumed that the six Byzantine nodes are initially consensus nodes; the number of consensus rounds increases from 0 to 30, with a step size of five.

The experimental results show that as the number of consensus rounds increases, PBFT, due to the lack of a reputation evaluation model and Byzantine node detection mechanism, maintains a constant number of Byzantine nodes. NR-PBFT not only limits the selection of nodes to those with high reliability but also takes advantage of a Byzantine detection mechanism to detect malicious nodes, thereby reducing the possibility of malicious nodes becoming leading nodes. The improvement not only reduces the risk of Byzantine attack systems but also enhances the overall stability and reliability of the system.

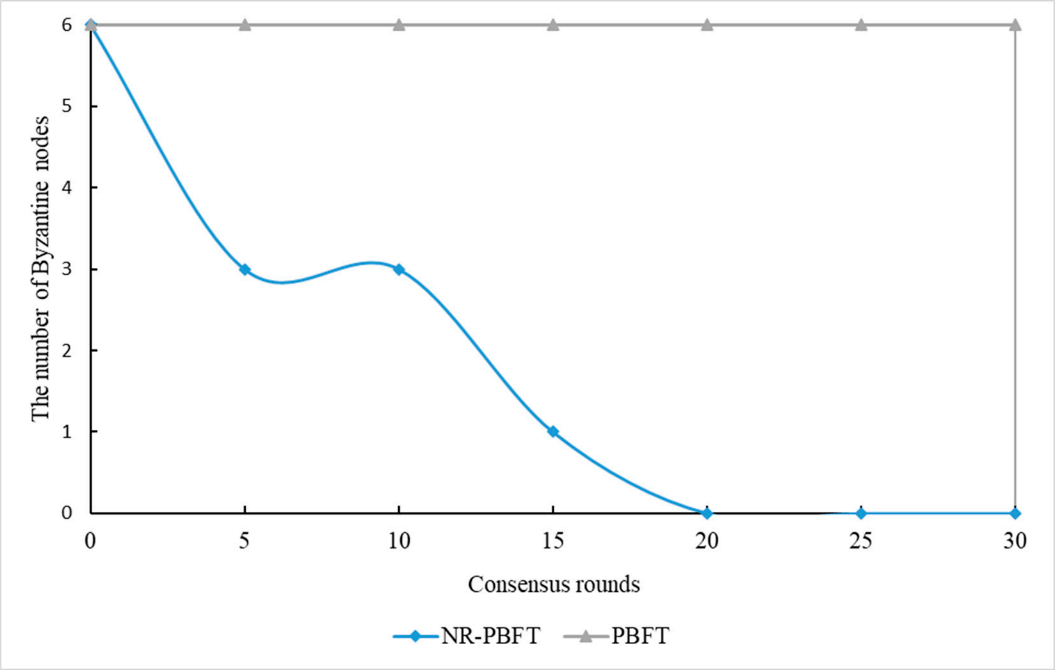


Figure 13. The comparison results of the number of Byzantine nodes.

5. Conclusions

This study focuses on the problems of low throughput, long transaction latency, and high communication overhead in the blockchain-based cold chain traceability system for marine fishery vessels. To solve the above problems, a NR-PBFT consensus algorithm is proposed. NR-PBFT includes a node grouping scheme, which is designed based on the consistent hashing algorithm to reduce the number of consensus nodes participating in the consensus process. Then, it presents a specific reputation evaluation model that considers the distance between fishery vessels, data size, and refrigeration temperature factors of nodes in marine scenarios, enhancing the reliability and robustness of the blockchain-based cold chain traceability system. Clear experimental results were found demonstrating that, compared with PBFT, NR-PBFT presents an 81.92% reduction in the transaction latency, an 84.21% increase in the throughput, and an 89.4% reduction in the communication overhead. Thus, the study makes improvements in terms of the blockchain system for marine cold chain traceability. In future work, we will further optimize the proposed algorithms for large-scale marine cold chain traceability scenarios. Moreover, the security of smart contracts will be enhanced.

Author Contributions: Conceptualization, Z.Z. and H.Z.; methodology, H.Z.; software, Z.Z.; validation, Z.Z. and H.Z.; formal analysis, H.L.; investigation, H.L.; resources, Z.Z.; data curation, H.Z.; writing—original draft preparation, H.Z.; writing—review and editing, H.L.; visualization, Z.Z.; supervision, H.L.; project administration, Z.Z.; funding acquisition; Z.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Key R&D Program of China (2023YFD2401304).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: There are no conflicts to declare.

Abbreviations

Character	Description
IoV-IMS	The Internet of Vessels system based on the Iridium Satellites
PBFT	Practical Byzantine Fault Tolerance
NR-PBFT	The Node-grouped and Reputation-evaluated PBFT
SBD	Short Burst Data
SPC	Shipboard personal computer
G_p	The reputation score of node p
k	The round of consensus
α	The penalty index
D	The distance between fishery vessels
D_{norm}	The standardized value of distance between fishery vessels
D_{max}	The maximum distance between fishery vessels
S	The size of data
S_{norm}	The standardized value of data size
S_{max}	The maximum value of data size
T_r	The refrigeration temperature
$T_{r,norm}$	The standardized value of refrigeration temperature
$T_{r,min}$	The minimum value of refrigeration temperature
$T_{r,max}$	The maximum value of refrigeration temperature
R_p	The possibility of a node being elected as the leader
β	The proportionality constant
m	Number of node groups
N	Total number of nodes
W_i	The weight of the node i
$Delay_t$	The transaction latency of transaction t
T_{end}	The time taken for the block containing the transaction to be confirmed
T_{start}	The time at which the client sends the transaction
TPS	Transactions Per Second
TX_{total}	The total number of transactions
T_{total}	The total time spent on the exchange
C_1	The total number of communications in PBFT
C_2	The total number of communications in NR-PBFT
q	The number of members in the consensus set

References

1. Ismail, S.; Reza, H.; Salameh, K.; Kashani Zadeh, H.; Vasefi, F. Toward an Intelligent Blockchain IoT-Enabled Fish Supply Chain: A Review and Conceptual Framework. *Sensors* **2023**, *23*, 5136. [CrossRef]
2. Sheikha, A.F.E.; Xu, J. Traceability as a Key of Seafood Safety: Reassessment and Possible Applications. *Rev. Fish. Sci. Aquac.* **2017**, *25*, 158–170. [CrossRef]
3. Humphries, F.; Rabone, M.; Jaspars, M. Traceability Approaches for Marine Genetic Resources Under the Proposed Ocean (BBNJ) Treaty. *Front. Mar. Sci.* **2021**, *8*, 661313. [CrossRef]
4. Akram, H.W.; Akhtar, S.; Ahmad, A.; Anwar, I.; Sulaiman, M.A.B.A. Developing a Conceptual Framework Model for Effective Perishable Food Cold-Supply-Chain Management Based on Structured Literature Review. *Sustainability* **2023**, *15*, 4907. [CrossRef]
5. Yu, F.; Li, Y.; Xie, B. Research on Food Safety Assurance for Ocean-going Vessels. *Food Ind.* **2023**, *44*, 337–341.
6. Tolentino-Zondervan, F.; Ngoc, P.T.A.; Roskam, J.L. Use Cases and Future Prospects of Blockchain Applications in Global Fishery and Aquaculture Value Chains. *Aquaculture* **2023**, *565*, 739158. [CrossRef]
7. Xu, J.; Zhao, Y.; Chen, H.; Deng, W. ABC-GSPBFT: PBFT with Grouping Score Mechanism and Optimized Consensus Process for Flight Operation Data-Sharing. *Inf. Sci.* **2023**, *624*, 110–127. [CrossRef]
8. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. *Decentralized Bus. Rev.* **2008**, 21260. Available online: https://www.debr.io/article/21260.pdf (accessed on 7 November 2021).
9. Yu, Q.; Zhang, M.; Mujumdar, A.S. Blockchain-Based Fresh Food Quality Traceability and Dynamic Monitoring: Research Progress and Application Perspectives. *Comput. Electron. Agric.* **2024**, *224*, 109191. [CrossRef]
10. Manimurgan, S.; Anitha, T.; Divya, G.; Latha, G.C.P.; Mathupriya, S. A Survey on Blockchain Technology for Network Security Applications. In Proceedings of the 2022 2nd International Conference on Computing and Information Technology (ICCIT), Tabuk, Saudi Arabia, 25–27 January 2022; pp. 440–445. [CrossRef]

11. Qahtan, S.; Yatim, K.; Zulzalil, H.; Osman, M.H.; Zaidan, A.A.; Alsattar, H.A. Review of Healthcare Industry 4.0 Application-Based Blockchain in Terms of Security and Privacy Development Attributes: Comprehensive Taxonomy, Open Issues and Challenges and Recommended Solution. *J. Netw. Comput. Appl.* **2023**, *209*, 103529. [CrossRef]
12. Xu, S.; Govindan, K.; Wang, W.; Yang, W. Supply Chain Management under Cap-and-Trade Regulation: A Literature Review and Research Opportunities. *Int. J. Prod. Econ.* **2024**, *271*, 109199. [CrossRef]
13. Lei, M.; Liu, S.; Luo, N.; Yang, X.; Sun, C. Trusted-Auditing Chain: A Security Blockchain Prototype Used in Agriculture Traceability. *Heliyon* **2022**, *8*, e11477. [CrossRef] [PubMed]
14. Hasan, A.S.; Sabah, S.; Haque, R.U.; Daria, A.; Rasool, A.; Jiang, Q. Towards Convergence of IoT and Blockchain for Secure Supply Chain Transaction. *Symmetry* **2022**, *14*, 64. [CrossRef]
15. Xiao, J.; Luo, T.; Li, C.; Zhou, J.; Li, Z. CE-PBFT: A High Availability Consensus Algorithm for Large-Scale Consortium Blockchain. *J. King Saud Univ.—Comput. Inf. Sci.* **2024**, *36*, 101957. [CrossRef]
16. Wu, Y.; Jin, X.; Yang, H.; Tu, L.; Ye, Y.; Li, S. Blockchain-Based Internet of Things: Machine Learning Tea Sensing Trusted Traceability System. *J. Sens.* **2022**, *2022*, e8618230. [CrossRef]
17. Wang, T.; Liu, X.; Guo, S.; Han, B.; Yang, W. Blockchain and IoT Based Traceability System for Agricultural Products. In Proceedings of the 2022 3rd International Conference on Computer Vision, Image and Deep Learning & International Conference on Computer Engineering and Applications (CVIDL & ICCEA), Changchun, China, 20–22 May 2022; pp. 316–321. [CrossRef]
18. Liu, S.; Zhang, R.; Liu, C.; Shi, D. P-PBFT: An Improved Blockchain Algorithm to Support Large-Scale Pharmaceutical Traceability. *Comput. Biol. Med.* **2023**, *154*, 106590. [CrossRef] [PubMed]
19. Gao, X.; Tong, G. Research on the Characteristics and Restrictions of the Pelagic Fishery Industry and Its Corresponding Institutional Arrangements. *Mar. Econ.* **2023**, *13*, 69–80. [CrossRef]
20. Liu, S.; Zhu, L.; Huang, F.; Hassan, A.; Wang, D.; He, Y. A Survey on Air-to-Sea Integrated Maritime Internet of Things: Enabling Technologies, Applications, and Future Challenges. *J. Mar. Sci. Eng.* **2024**, *12*, 11. [CrossRef]
21. Zhang, Y.; Liu, Y.; Jiong, Z.; Zhang, X.; Li, B.; Chen, E. Development and Assessment of Blockchain-IoT-Based Traceability System for Frozen Aquatic Product. *J. Food Process Eng.* **2021**, *44*, e13669. [CrossRef]
22. Patro, P.K.; Jayaraman, R.; Salah, K.; Yaqoob, I. Blockchain-Based Traceability for the Fishery Supply Chain. *IEEE Access* **2022**, *10*, 81134–81154. [CrossRef]
23. Syam, M.M.; Cabrera-Calderon, S.; Vijayan, K.A.; Balaji, V.; Phelan, P.E.; Villalobos, J.R. Mini Containers to Improve the Cold Chain Energy Efficiency and Carbon Footprint. *Climate* **2022**, *10*, 76. [CrossRef]
24. Jadhav, M.; Iyer, S. Traceability Study on Fishery Supply Chain Using Blockchain. *ECS Trans.* **2022**, *107*, 15595–15601. [CrossRef]
25. Liu, S.; Yu, Z. Modeling and Efficiency Analysis of Blockchain Agriculture Products E-Commerce Cold Chain Traceability System Based on Petri Net. *Heliyon* **2023**, *9*, e21302. [CrossRef] [PubMed]
26. Jiang, W.; Wu, X.; Song, M.; Qin, J.; Jia, Z. Improved PBFT Algorithm Based on Comprehensive Evaluation Model. *Appl. Sci.* **2023**, *13*, 1117. [CrossRef]
27. Xu, G.; Liu, Y.; Khan, P.W. Improvement of the DPoS Consensus Mechanism in Blockchain Based on Vague Sets. *IEEE Trans. Ind. Inform.* **2020**, *16*, 4252–4259. [CrossRef]
28. Onireti, O.; Zhang, L.; Imran, M.A. On the Viable Area of Wireless Practical Byzantine Fault Tolerance (PBFT) Blockchain Networks. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019; pp. 1–6. [CrossRef]
29. Wang, T.; Huang, D.; Zhang, S. Consensus Algorithm Analysis in Blockchain: PoW and Raft. In *Wireless Blockchain*; John Wiley & Sons, Ltd.: Hoboken, NJ, USA, 2021; pp. 27–72. [CrossRef]
30. Kreps, J.; Narkhede, N.; Rao, J. Kafka: A distributed messaging system for log processing. In Proceedings of the 6th International Workshop on Networking Meets Databases (NetDB), Athens, Greece, 12–16 June 2011; Volume 11, pp. 1–7.
31. Luo, H. ULS-PBFT: An Ultra-Low Storage Overhead PBFT Consensus for Blockchain. *Blockchain Res. Appl.* **2023**, *4*, 100155. [CrossRef]
32. Jain, A.K.; Gupta, N.; Gupta, B.B. A Survey on Scalable Consensus Algorithms for Blockchain Technology. *Cyber Secur. Appl.* **2025**, *3*, 100065. [CrossRef]
33. Castro, M.; Liskov, B. Practical Byzantine Fault Tolerance. In Proceedings of the 3rd Symposium on Operating Systems Design and Implementation (OSDI 1999), New Orleans, LA, USA, 22–25 February 1999; pp. 173–186.
34. Huang, B.; Peng, L.; Zhao, W.; Chen, N. Workload-Based Randomization Byzantine Fault Tolerance Consensus Protocol. *High-Confid. Comput.* **2022**, *2*, 100070. [CrossRef]
35. Liu, S.; Zhang, R.; Liu, C.; Xu, C.; Wang, J. An Improved PBFT Consensus Algorithm Based on Grouping and Credit Grading. *Sci. Rep.* **2023**, *13*, 13030. [CrossRef]
36. Zhong, W.; Zheng, X.; Feng, W.; Huang, M.; Feng, S. Improve PBFT Based on Hash Ring. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, e7327372. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.