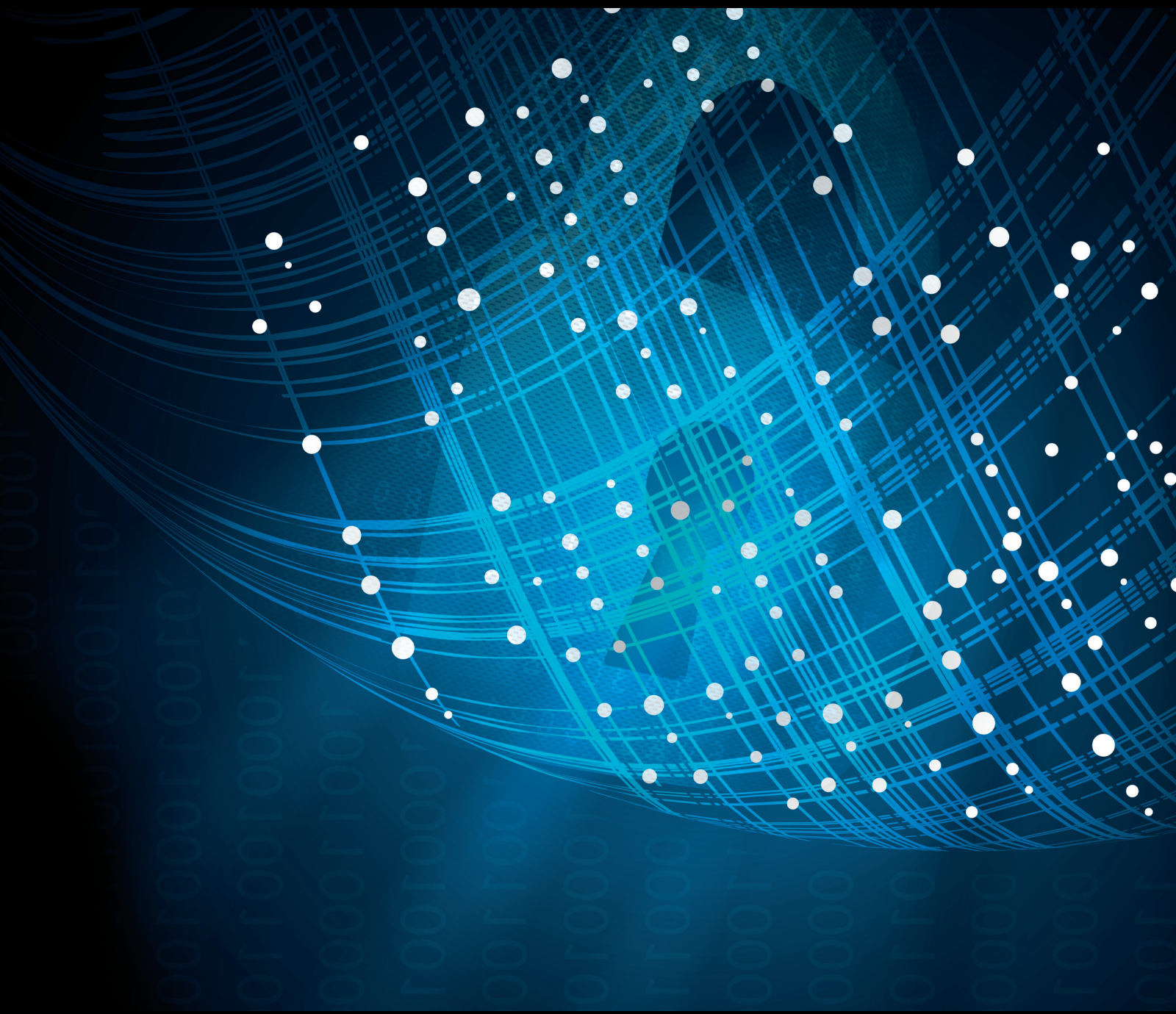
Security and Communication Networks

Advanced Blockchain in Sensors for Logistics and Supply Chain 4.0

Lead Guest Editor: Chun-ho Wu
Guest Editors: Yung Po Tsang and W. H. Ip



Advanced Blockchain in Sensors for Logistics and Supply Chain 4.0

Security and Communication Networks

Advanced Blockchain in Sensors for Logistics and Supply Chain 4.0

Lead Guest Editor: Chun-ho Wu
Guest Editors: Yung Po Tsang and W. H. Ip

Contents

Hindawi
Security and Communication Networks
Volume 2023, Article ID 1525998, 16 pages
https://doi.org/10.1155/2023/1525998

Research Article

Enhanced Multiset Consensus Protocol Based on PBFT for Logistics Information Traceability

Linchao Zhang,[1] Lei Hang,[2] and Dohyeun Kim[1]

[1]*Department of Computer Science, Jeju National University, Jeju, Republic of Korea*
[2]*Business School, Shanghai Normal University Tianhua College, Shanghai 201815, China*

Correspondence should be addressed to Dohyeun Kim; kimdh@jejunu.ac.kr

Received 26 September 2022; Revised 20 October 2022; Accepted 24 November 2022; Published 22 February 2023

Academic Editor: Y. P. Tsang

In the recent years, the global logistics industry has greatly driven the development of the world economy. At the same time, a large amount of data information is generated. Due to the frequent occurrence of logistics information leakage and forgery, it is necessary to find solutions that can accurately trace logistics information and ensure the security and authenticity of logistics information. The birth of blockchain technology has transformed the logistics industry from quantitative change to qualitative change. The technical characteristics of blockchain technology, such as distributed storage ideas, decentralization, immutability, and complex encryption consensus algorithm, endow it with a wide range of application prospects in the logistics industry. This paper proposes an enhanced multiset consensus algorithm based on PBFT (practical Byzantine fault tolerance) for logistics information traceability and storage on the logistics blockchain. The application of the proposed multi-set consensus algorithm in the topology structure composed of multiple sets can improve the consensus efficiency of logistics information in the blockchain. We improve consensus capability and transaction speed, avoid redundant consensus message packets occupying a large bandwidth, and efficiently process logistics information generated at any time. We ensure the traceability of logistics information and achieve efficient and accurate traceability, and the efficiency and security of the proposed algorithm are analyzed. This paper aims to solve the problems of traceability, trustworthiness, and efficient processing of blockchain applications in logistics information to operate the logistics network efficiently. This paper compares the proposed algorithm with the PBFT-related expansion algorithm regarding bandwidth occupation, delay, and throughput. The results show that the MPBFT consensus algorithm significantly improves the efficiency of the logistics blockchain network.

1. Introduction

With the rapid development of e-commerce, the logistics industry and various Internet technologies have become more in-depth, and the logistics industry has become more intelligent. However, many problems in the logistics industry, such as the authenticity of data information and logistics traceability, still need to be solved urgently. Currently, there is a lot of fake data in the logistics industry; at the same time, with the gradual maturity of big data technology, logistics data information has become increasingly important national confidential information. Due to the characteristics of the logistics industry involving multiple regions, it is very suitable for applying decentralized blockchain technology. The data in the blockchain are encrypted and stored in a distributed form and cannot be tampered with. Therefore, the logistics industry is exploring how to use blockchain technology better to protect logistics information's privacy, prevent information from being tampered with, and improve traceability.

This paper aims to study the application of blockchain technology in logistics information traceability scenarios. "Logistics information" refers to the corresponding data generated by each link of logistics circulation. To efficiently trace these data, this paper designs a logistics information traceability architecture based on a multiset consensus algorithm, which stores all logistics information indirectly on the blockchain to build a decentralized logistics blockchain.

According to the characteristics of logistics informatization, combined with the research status and application progress of blockchain technology in the logistics industry in domestic and foreign literature, a multiset consensus algorithm is proposed to improve the efficiency of logistics blockchain information traceability and information authenticity and introduced the blockchain logistics-related solutions, as shown in Table 1.

How to ensure the security of logistics data is a crucial issue. On the one hand, establishing a traceable system to monitor the information on items is ideal for both managers and buyers. On the other hand, managing and sharing logistics data are a challenging job. Handling large amounts of data efficiently and keeping it secure are critical. It is inappropriate and impractical to disclose all information about an item, as doing so may reveal the user's private information. It is also not advisable to rely entirely on information from the online world, as there may be some malicious attackers. Therefore, researchers must figure out the right way to manage logistics data. Traditional methods, including data sampling [4, 5], preprocessing [6], statistical analysis [7], and data mining [8], have insufficient security and low efficiency for big data. As mentioned above, as emerging application technology, blockchain is essentially a database with attractive properties such as anticounterfeiting, traceability, and transparency [9]. Based on these characteristics, using blockchain as a new foundation for logistics scenarios and its decentralization will benefit the industry's development. However, there are several key issues related to the physical world. One of the problems is that the network nodes on the blockchain are difficult to bind with physical entities, which we call the traceability problem. Generally speaking, only trusted nodes on the blockchain can be protected, and information fraud cannot be controlled at the level of a physical collection of information, so no matter how reliable the blockchain is, it cannot be used and managed. This article provides logistics traceability and data security protection at the information flow level. Previous studies combining blockchain and logistics scenarios mainly focused on designing different system levels, and a few focused on data reliability before investing in the blockchain. Other work is based on public key infrastructure (PKI) to achieve identity authentication [10]. For the supply of goods, the digital identity issued by the certificate authority (CA) is used to realize the binding of physical goods and network nodes on the blockchain. However, PKI is highly dependent on CAs responsible for the issues and management of private and public key pairs. It is essentially a centralized system and has the disadvantage of being centralized. On the other hand, even with the credentials of the data source and leveraging the blockchain to build the system, it still has problems due to the sheer volume of data. Logistics datasets are usually large scale in practical applications, so an efficient consensus algorithm is required to transmit all information to each node for users to query. This places great demands on the efficiency of the blockchain network.

The main content of this paper is to carry out an in-depth research expansion and feasibility study on the article [11] proposed earlier. Section 1 analyzes the problems in the logistics industry and the significance of logistics information traceability and expounds on the main research content of this paper. Section 2 introduces the background and related research of logistics information traceability studied in this paper. In addition, related consensus algorithms are also introduced. Section 3 is the logistics traceability system architecture based on a multiset consensus algorithm. Section 4 mainly introduces some improvements to the PBFT algorithm, proposes an efficient consensus algorithm for the logistics industry under MPBFT, avoids redundant consensus message packets, and proposes solutions to describe the basic model algorithm. The algorithm improves the PBFT consensus efficiency, reduces the network bandwidth of the logistics system, and further expounds the algorithm of the overall implementation process. In Section 5, the bandwidth test and performance analysis of the proposed MPBFT algorithm are carried out. Section 6 summarizes the work of this paper, puts forward some shortcomings, and puts forward some suggestions for the research and improvement of this paper.

2. Related Work

This section mainly studies the application of blockchain technology in logistics information traceability scenarios. Firstly, the background knowledge of logistics information traceability is briefly introduced. Then, the existing consensus algorithm-related technologies of blockchain are introduced, and the application of blockchain technology in logistics information traceability and the research status at home and abroad are analyzed.

2.1. Background. With the rapid development of the modern logistics industry, the logistics industry generates a large amount of data information, among which problems such as leakage of user cargo information have threatened people's life safety and should not be underestimated [12]. In real life, the user's cargo information can generally be divided into two parts, one is the user's private information and the other is the information generated by the logistics in the process of cargo transportation.

At present, the following security threats still exist in the traceability of logistics information:

(1) It is not easy to guarantee the confidentiality and authenticity of logistics information. The logistics industry generally only pays attention to protecting consumers' private information, such as name, phone number, and address, and does not take protective measures for the logistics information generated during the transportation process, which is prone to generate a large amount of false information.

(2) User authentication is difficult to achieve. In logistics and distribution, it is often sent to the receiving point. There is no shortage of malicious customers

Table 1: Comparison of logistics traceability solutions.

Literature	Important method	Solution
TPLI: A Traceable Privacy-Preserving Logistics Information Scheme via Blockchain [1]	Development prototype verification traceability	Implementing a prototype system using hyperledger
Blockchain-Based Supply Chain Traceability: Token Recipes Model Manufacturing Processes [2]	Proposing the token to calculate the gas cost	A linear relationship between gas cost and the product is proposed to define the relationship between ingredients and products
Research on Traceability Algorithm of Logistics Service Transaction Based on Blockchain [3]	Traceability algorithm of logistics service transaction	Through the proposed algorithm, the end-to-end traceability service of logistics service is realized

who might fake their identities to pick up packages that do not belong to them.

Faced with the above security threats, the research on logistics information traceability is highly significant. Solutions are urgently needed to ensure the traceability of logistics information's efficiency, authenticity, and security.

2.2. Consensus Algorithm. Reference [13] first proposed the problem of how nodes participating in transaction maintenance in distributed ledgers reach consensus. This problem mainly needs to be verified from the following three aspects: whether it has termination, whether it is consistent, whether it is valid, and whether it can. The method to achieve the above three aspects is called the consensus algorithm. The blockchain logistics traceability system and the consensus algorithm mechanism ensure that the information is decentralized and cannot be easily changed. Consensus refers to making most nodes (at least 51%) in the entire network trust that the data are reliable. At present, the mainstream consensus mechanism includes the proof of work (PoW), proof of interest (PoS), proof of entrusted Interest (DPOS), and Byzantine consensus (PBFT), as shown in Table 2.

2.2.1. Proof of Work. POW (proof of work) [14] is the consensus algorithm adopted in the Bitcoin system proposed by Nakamoto and Bitcoin. The consensus algorithm ensures the consistency of transaction records by introducing the method of computing power competition to make nodes reach a consensus. However, one of the biggest shortcomings of the POW algorithm is the serious waste of computing power.

2.2.2. Proof of Stake. A node holds many tokens, the node will want the currency to be stable, and the node will strive to maintain the system's normal operation and ensure the currency's stability. Therefore, the algorithm of accounting node selection to reach consensus can be designed by using the information related to the token held by the node, also known as the proof of stake algorithm (POS). The advantage of the POS consensus algorithm is that it does not need to consume computing resources. Still, the disadvantage is that the nodes holding the largest number of tokens tend to monopolize the nodes, which deviates from the core idea of blockchain.

2.2.3. Delegated Proof of Stake. The DPOS algorithm is similar to the board system. To avoid centralizing some nodes with excessive rights, the algorithm uses "witnesses" to supervise the behavior of nodes [15]. This algorithm is equivalent to partial decentralization, and the core lies in the representative select. The DPOS algorithm eliminates the time transaction need to wait for verification by untrusted nodes, thereby increasing consensus speed.

2.2.4. Practical Byzantine Fault Tolerance. The PBFT algorithm [16, 17] is divided into five stages: request, preparation, preparation, submission, and reply. PBFT algorithm has the consistency protocol needed to reach a consensus. It includes the checkpoint protocol used to restrain nodes and the view-switching protocol needed to switch views after discovering faulty nodes. In a consistency protocol, the system broadcasts messages to other secondary nodes through the primary node and reaches a consensus by returning the message consistency. The checkpoint protocol saves memory by periodically cleaning up contracted transaction data. The view switchover protocol is used to initiate a view switchover to reselect the primary node when the primary node fails. PBFT algorithm has high consensus efficiency and does not require much computing power maintenance.

2.3. Research Status of Consensus Algorithm and Application in Blockchain Traceability. The development of the logistics express industry should be reflected in the huge volume of parcels brought by the current e-commerce industry and should pay attention to the transformation of the logistics industry from quantitative change to qualitative change. The development of the worldwide logistics industry is increasingly moving towards a high-quality stage [18], in which blockchain technology is expected to endow the logistics industry with more intelligence and innovation by relying on its many unprecedented advantages. Many domestic and foreign researchers are discussing the application of blockchain technology in logistics information traceability scenarios, hoping to promote the logistics industry to another development climax.

Reference [19] uses side chain technology to design a supply chain traceability system. The blockchain platform used in this system is Ethereum. The literature focuses on analyzing the design of smart contracts, using smart contracts to manage goods and realizing logistics information's traceability. Reference [20] utilizes the Ethereum blockchain and smart contracts to efficiently execute commercial transactions for soybean tracking and traceability throughout the agricultural supply chain. The scheme utilizes smart contracts to manage and control all participants' interactive supply chain ecosystem transactions. Reference [21] developed a food traceability prototype system using blockchain technology for food safety issues. This document proposes a management architecture for on-chain and off-chain data through which traceability systems can alleviate the data explosion problem of IoT blockchains. Reference [22] proposed a blockchain-based drug traceability framework to prevent drug fraud, and logistics traceability was carried out from the start of drug production, including distribution.

Reference [23] applies blockchain to intelligent pallet management in logistics, proposes a Palletaa architecture, and studies the synergy of integrating alliance blockchain and IoT. A corresponding layered architecture is proposed to construct the system deployment in the industry. The position-inventory-routing problem of the pallet pool is formulated to efficiently manage pallet usage in the logistics industry. Reference [24] discusses the situation of BTCS

Table 2: Comparison of four consensus algorithms.

Consensus algorithm	POW	POS	DPOS	PBFT
Degree of centralization	Decentralization	Decentralization	Partially decentralized	Partially decentralized
Whether to resist Byzantine nodes	Y	Y	Y	Y
Is permission required	N	N	N	Y
System scale (number of nodes)	Unlimited	Unlimited	Unlimited	Limited
Node dynamic changes	Support	Support	Support	No support
Applicable scene	Public chain	Public chain	Public chain	Alliance chain
Consistency	Weak consistency	Weak consistency	Weak consistency	Consistency

from the perspective of industrial application and market competition. First, it expounds on the potential of BTCS and the gap between the ideal and reality of BCTS. Secondly, it discusses the applicability of BTSC, mainly through the game theory model, to the market. The situation was discussed. Reference [25] summarizes the application of blockchain in traceability. First, it analyzes the problems that need to be solved in the traceability scenario, then expounds on the related technologies of blockchain, and points out how these technologies can be applied to the traceability scenario. Literature [26–28] is based on the current social conditions where smartphones are popularized; the anticounterfeiting system is designed using smartphones as nodes of the blockchain. Users only need to install software on their mobile phones to achieve the purpose of traceability and anticounterfeiting.

The encrypted logistics information blockchain must be transmitted to the blockchain in the logistics information blockchain. Due to the decentralized nature of the blockchain, all transactions are negotiated by all nodes on the chain. "The consensus algorithm realizes the process." When the transaction information is uploaded to the chain, the nodes complete the consensus of the transaction data. The data can be added to the blockchain database [29]. References [30–33] all use the consensus algorithm of blockchain technology to realize the traceability query of logistics information. The following focuses on analyzing the research status of the PBFT consensus algorithm.

The consensus problem is the core problem of the blockchain network. The PBFT consensus algorithm can accommodate both faulty nodes and malicious nodes. The number of all nodes must be at least $3f + 1$ (f is the number of malicious/faulty nonresponding nodes), which can ensure security and liveness in an asynchronous system. At the same time, it solves the problem that the original Byzantine fault tolerance (BFT) algorithm is inefficient, but PBFT has high latency in the case of network instability. Reference [34] considers many nodes in the blockchain when for the consensus speed problem, the consensus is carried out in a partially decentralized way. That is, a certain number of "central" nodes are selected. For the selection method of such nodes, the literature uses an improved K-medoids clustering algorithm. However, this method is still too expensive in the consensus process. The literature [35] combines the Gossip protocol to allow half of the nodes in the system to do evil. The blockchain system proposed in this literature has certain scalability, allowing foreign nodes to join the system anytime. However, this paper's model for node selection is not accurate enough, and the time for the system to enter normal operation still needs to be shortened. Reference [36] considers the issue of client latency and proposes an EZ. But consensus algorithm there is no master node, but instead it enables each replica to order requests received from clients. Reference [37] applies blockchain technology to the logistics service supply chain information platform and uses the blockchain network's DBFT (authorized Byzantine fault tolerance) consensus algorithm. In this consensus algorithm, not all nodes on the chain can reach a consensus. Instead, the nodes eligible for agreement are selected by voting on the nodes. The higher the stake a node has, the greater the probability of becoming a consensus node. The literature [38, 39] also focuses on the source of the product. In the blockchain traceability system, the NPBFT consensus algorithm is used, and the communication overhead required for consensus is reduced, thereby improving traceability efficiency.

It can be seen from the above that blockchain technology can be applied to the traceability requirements of logistics information in various scenarios. Among blockchain-related technologies, the consensus algorithm is an important technology. In the next sections, we will analyze the research status of consensus algorithm technologies in blockchain traceability and focus on exploring the research status of the PBFT consensus algorithm.

3. Design of Logistics Information Traceability System Based on Multiset Consensus Algorithm

Aiming at the proposed logistics information traceability problem, this section designs a logistics information traceability system based on a multiset consensus algorithm in combination with blockchain-related technologies. We carry out the overall design of the system. After analyzing the system's requirements, the overall architecture of the system is created, and the system's network is deployed.

3.1. Overall System Design. The design goal of the system in this paper is to solve the problem that the information in each link of the goods circulation is not updated in time, and the transportation process is difficult to trace. Due to the huge amount of logistics information data and real-time changes, an efficient consensus algorithm is needed to ensure that the data can be uploaded to the chain quickly and without errors. This system plans to use an improved PBFT

consensus algorithm (MPBFT), which can reduce the time it takes for transactions to reach consensus, thereby improving consensus efficiency.

This paper uses the supply chain solution provided by IBM [40] to build a blockchain traceability system suitable for logistics. The supply chain solution provides basic logistics equipment management, storage and query and provides cloud services required for gateway service integration, which greatly improves the scalability of required functions. According to the IBM product business model [41], the proposed system is layered, and the logistics traceability system is jointly constructed using IBM-related services and the proposed MPBFT consensus algorithm. The overall architecture of this system is based on the five-layer architecture of the blockchain, adding a storage layer, adding a data analysis platform to the contract layer, and merging the network layer and the consensus layer. The system's overall architecture is shown in Figure 1, divided into the application, contract, storage, network, consensus, and data layer from top to bottom.

(1) Application layer: the application layer is the entrance to the realization of system functions and is mainly responsible for the interaction of system users, including the registration, login, and query operations of administrators and ordinary users.

(2) Contract layer: execute-related smart contracts in the application layer, such as sign-off and delivery reminders

(3) Storage layer: the layer is divided into off-chain and on-chain databases. The off-chain database is a traditional distributed database, mainly deployed in the cloud, and stores the hash data corresponding to the original data of logistics information. The on-chain database is mainly used to serve data information generated by nodes in the blockchain.

(4) Network and consensus layer: the logistics information data files are transmitted through the transmission network formed by 5G, NBIoT, and intelligent gateway, and the block data is sent to the P2P point-to-point network.

(5) Data layer: the data layer is divided into logistics information and block data. The logistics information data is actual transportation route data. Address information and form chain structure blocks through technologies such as digital signatures and Merkle trees.

According to the overall system architecture of Figure 1, the network structure of this system mainly includes cloud, blockchain network, and application. The system network deployment is shown in Figure 2. The raw data of logistics information is stored in a distributed database in the cloud. Different roles access through the MSP access control system of Hyperledger Fabric and access the application data in the blockchain network after CA authentication. Each user terminal can quickly and efficiently query the required information, and the Blockchain ensures the authenticity and validity of the data.

4. Multiset PBFT (MPBFT)

This paper uses a consensus algorithm of PBFT type in the logistics information traceability system based on blockchain. Since multiple nodes are involved in the logistics and transportation process, a large amount of logistics information will be generated, which requires the blockchain to have high performance and bandwidth requirements. Therefore, because of the low efficiency of blockchain logistics traceability and the pain point of the redundant large amount of data, this paper designs a multiset PBFT algorithm, which improves the consensus efficiency of the logistics system, improves the consensus efficiency of transaction information on the chain, and reduces the communication overhead of the system.

4.1. Basic Model of Algorithm. As shown in Figure 3, this paper defines each computer as a separate node. In the MPBFT algorithm, the nodes are divided into different node sets according to the architectural requirements (region, environment, communication), the node sets are connected, and the nodes in each node set adopt the PBFT algorithm consensus. The set of nodes relates to the consensus recorder. In this paper, it is assumed that each node set has four nodes. First, the consensus information is broadcast to the consensus recorder through the master node, and the consensus recorder will send a new consensus message to the nodes in each set. After all, nodes complete the consensus; each node will write the consensus data. After the data have passed the node consensus, the master node will verify and respond to the client, which proves that the transaction consensus is completed.

This paper applies the above consensus model to the blockchain logistics industry, and nodes are divided into different sets according to different geographical locations. Nodes with the same geographical location are divided into the same node set, and nodes in any node set can be used as master nodes to broadcast consensus. To reduce the number of communications, we avoid redundant consensus message packets. The MPBFT algorithm is used to verify the consensus message package between nodes, and there is no need to repeatedly forward the consensus message package across regions. Assume that M set networks are set up according to different cities in the logistics blockchain network N:

(1) Set the number of a set in the blockchain node network to M and denote the set as $S_i, \mathrm{So}\{Si \in \{S, S_2, \ldots, S_M\}\}$

(2) Set the malicious nodes among the N nodes of the cluster as f, so the cluster N must satisfy the following:

$$N \geq \frac{3f + 1}{M}. \tag{1}$$

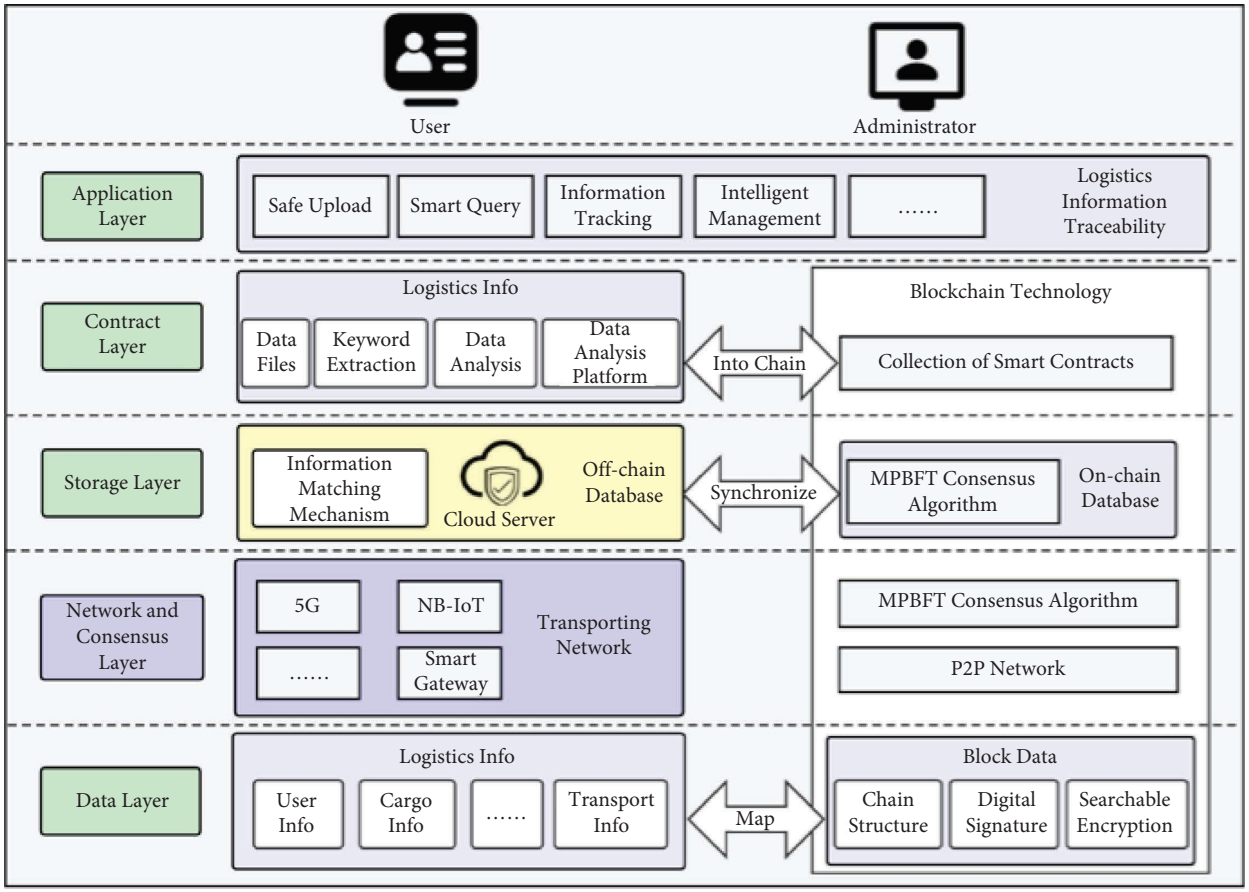


Figure 1: Overall architecture diagram of logistics information traceability system.

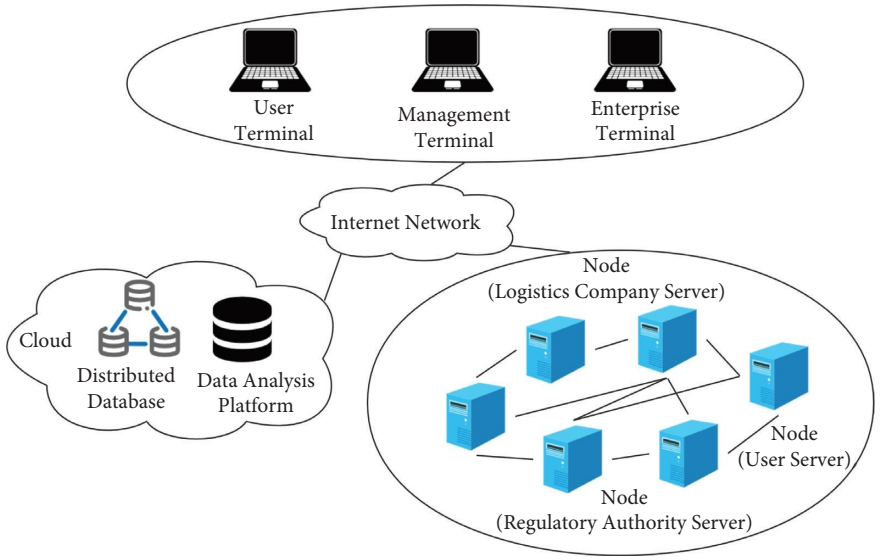


Figure 2: Network deployment diagram of logistics information traceability system.

4.2. MPBFT Algorithm Design. The basic PBFT consensus algorithm requires high-frequency communication to ensure that the consensus message packet can reach all nodes. As the number of nodes increases, the bandwidth and consensus delay will greatly increase. In the event of a faulty node, the communication connection will be lost, and there will also be malicious nodes. In this paper, the forwarding and packet structure optimization of the PBFT algorithm is carried out to improve consensus efficiency and avoid redundant consensus message packets occupying a large

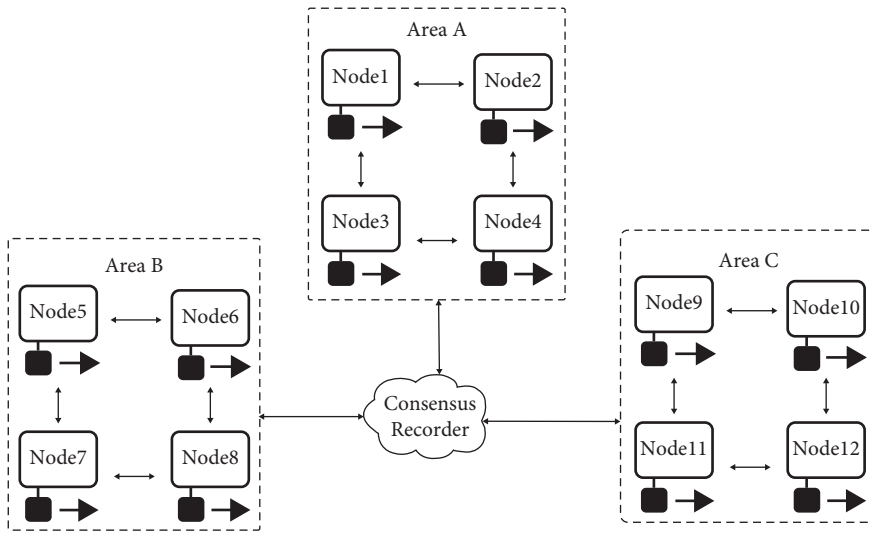


Figure 3: Group division diagram for logistics information traceability.

amount of bandwidth. First, the master node obtains a copy of the node set the record in the network through the consensus recorder. The copy in the consensus recorder needs to be registered with the global node during network construction, and each node will synchronize the copy of the consensus recorder. The MSP management mechanism of the alliance chain is introduced here. Jointly manage the number of nodes and state information in the consensus recorder. The master node sends the transaction packet that needs to be broadcast to the consensus recorder, the consensus recorder sends a new consensus notification to each node, and each node executes the consensus process of PBFT.

As shown in Figure 4, consensus blocks in this paper mainly include the following:

(1) The field Set_Number in the consensus recorder contains all the sets M in the network, the node names in each set, and the consensus state of the nodes.

(2) The Node_Set_Name field represents the node name in the set and records the order between adjacent nodes.

(3) The consensus state field indicates the consensus state of each node, including the verification data (v, n, d, i, m) of each node in the consensus stage, and the consensus recorder compares and confirms the response message packets of each node to determine whether the consensus is successful.

(4) The forward nodes field is used for offline consensus forwarding by the adjacent nodes of the faulty node when a communication failure occurs on the faulty node (introduced below).

(5) We set the timing of each node to synchronize the copy with the consensus recorder, and each node will save the copy to confirm whether the consensus data of the consensus stage is consistent with the consensus data of other nodes and meet the consensus condition of $2f + 1$.

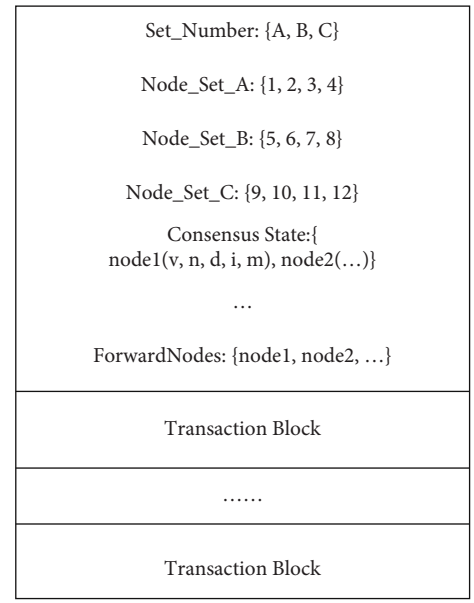


Figure 4: Consensus recorder model design.

The introduction of the consensus recorder in this paper greatly reduces the communication frequency between nodes and the communication bandwidth; each node only needs to obtain the consensus state of each node through the consensus recorder. We have modified the PBFT algorithm process to reduce the number of communications and offline forwarding when a faulty node occurs.

4.3. MPBFT Algorithm Flow

4.3.1. Role Division

(i) Client node is responsible for sending transaction requests

(ii) Primary node is responsible for packaging transactions into blocks and block consensus. There is only one primary node in each round of consensus

(iii) Replica node is responsible for block consensus, there are multiple replica nodes in each round of the consensus process, and the processing process of each replica node is similar

Among them, both primary and replica nodes belong to consensus nodes.

4.3.2. Algorithm Flow. As shown in Figure 5, the basic process of the PBFT algorithm mainly includes the following four steps:

(i) The client sends a request to the master node

(ii) The master node broadcasts the request to other nodes, and the nodes execute the three-phase consensus process of the PBFT algorithm

(iii) After the node processes the three-stage process, it returns a message to the client

(iv) After the client receives the same message from $f + 1$ nodes, the consensus has been completed correctly

The three core stages of the algorithm are the preprepare stage, the prepare stage, and the commit stage. C in the figure represents the client, 0, 1, 2, and 3 represent the number of the nodes, of which 0 is the primary node, and the three marked with an X represents a possible fault node or a malicious node. The behavior shown here is for other nodes. The whole process is rough as follows.

First, the client initiates a request to the master node $0 \ll \text{REQUEST}, o, t, c \gg$ where t is the timestamp, o represents the operation, c is the client, the master node receives the client request, and the master node sends the consensus recorder. When the request packet is sent, the consensus recorder will send a preprepare message to other nodes. Other nodes will receive the preprepare message and start the core three-phase consensus process.

(1) Preprepare Stage. After the replica node receives the preprepare message, there are two choices, one is to accept and the other is not to accept. A typical case of not accepting is if a replica node receives a preprepare message $\ll \text{PRE\_PREPARE}, v, n, d >, m >$, where v represents the view number, v represents the sequence number (the primary node receives the client each request on the side is marked with a number), d represents the message digest, and m represents the raw message data. The v and n in the message have appeared in the message received before, but they d, and m are inconsistent with the previous message, and the request will be rejected now. The rejection logic is that the master will not send two messages with the same v and n but different d and m.

The replica node receives the preprepare message and performs the following message verification:

(i) The signature of the message m is valid, and the message digest d matches the message m: $d = \text{hash}(m)$

(ii) The node is currently in view v

(iii) The node currently has no other preprepare messages on the same (view , sequence n). That is, there is no other m' and corresponding d', $d' = \text{hash}(m')$.

(2) Prepare Phase. After the current node agrees to the request, it will send a prepare message $\langle \text{PREPARE}, v, n, d, i \rangle$ to the consensus state of the consensus recorder and record the message in the log, where i is used to represent the identity of the current node. At the same time, not only one node is going through this process. There may be n nodes that are also going through this process. Therefore, the consensus recorder will record the prepare messages sent by different nodes. The current node synchronizes the copy of the consensus recorder. The current node i verifies whether the data v, n, and d of these prepared messages and the prepared messages sent by itself are consistent. After the verification is passed, the current node i sets prepared (m, v, n) to true and sent to the consensus recorder. Prepared (m, v, n) represents the consensus node believing that the message m in (v, n) whether the prepare phase has been completed. The preparation phase has been completed if the consensus recorder replica receives prepare messages from more than $2f$ other nodes within a certain time frame. Finally, the consensus node i sends the commit message and enters the commit stage.

(3) Commit Stage. The current node i receives $2f$ commit messages $\langle \text{COMMIT}, v, n, d, i \rangle$ from the copy of the consensus recorder and inserts the messages into the log ($2f + 1$ including its own), verifying after these commit messages are consistent with the three data of v, n, and d in the commit message sent by themselves, the consensus node sets committed-local (m, v, n) to true, committed-local(m, v, n). On behalf of the consensus node, it is determined that the message least $2f + 1$ nodes have agreed with the message m in the entire system, and this ensures that at least $f + 1$ nonfaulty nodes have reached a consensus on the message m. Then, the node will execute the request and write the data.

After processing, the node will return the message $\ll \text{REPLY}, v, t, c, i, r \gg$ to the client. When the client collects $f + 1$ messages, the consensus is completed, which is the whole process of the PBFT algorithm.

4.3.3. Communication Disconnection. Suppose there is a communication failure between the node and the consensus recorder to ensure that all nodes are fully connected. In that case, messages need to be forwarded to the faulty node. This process occurs between nodes in the node set. The normal nodes adjacent to the faulty node forward the copy of the consensus recorder.

As shown in Figure 6, the consensus process of adjacent nodes is as follows:

(i) The consensus recorder sends a PBFT message to {node 0, node 1, node 2, node 3} and finds that {node 1, node 3} is not in the connection list (faulty node), then sets the forward nodes field of the PBFT message msg to {node 1, node 3}, and forwards it to

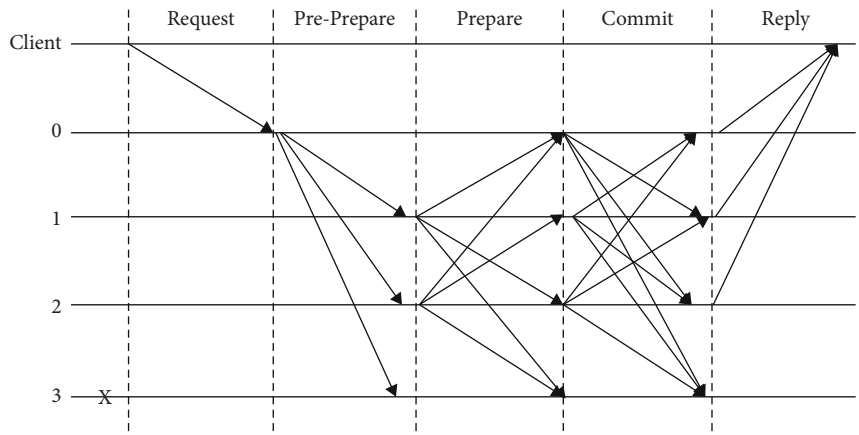


Figure 5: MPBFT consensus algorithm process.

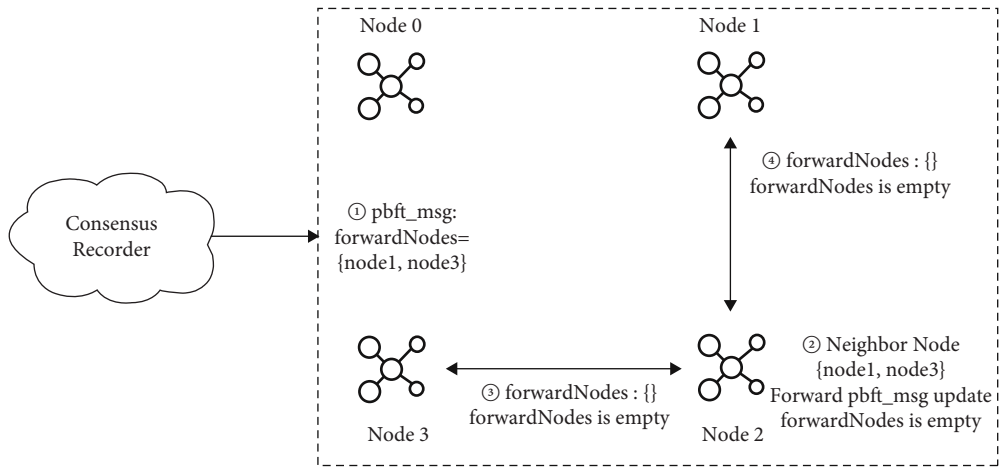


Figure 6: Communication forwarding model of disconnected neighbor nodes in the network.

node 0 and node 2; according to the principle of the proximity of nodes, this paper uses four nodes in the node set as an example.

(ii) If node 2 determines that the forward nodes field is not empty after receiving the PBFT message from the consensus recorder, it traverses the neighbor node list {node 1, node 3} and removes the neighbor nodes from forward nodes.

(iii) Node 2 forwards the updated PBFT message msg to node1 and node 3.

(iv) After node1 and node3 receive the msg, they judge that the forward nodes field is empty, we consider that the message has reached all nodes and do not continue to forward the PBFT message.

As shown in Figure 7, the improved PBFT message forwarding strategy adds the forward nodes field to the PBFT message packet in the copy of the consensus recorder to record the disconnected node information. After receiving the PBFT message packet, other nodes forward the message to the reachable nodes (adjacent nodes) recorded by forward nodes, ensuring that PBFT message packets can reach all nodes as much as possible, reducing redundant PBFT messages in the network and improving network efficiency. Since the message packet of the faulty node is forwarded and received by the adjacent node, the authenticity of the forwarding process of the adjacent node is recorded by the consensus recorder. If the node state of the consensus recorder is $\ll$ PRE_PREPARE, $v, n, d >, m >$, the values of v, n, d, and m are verified, and if they are not the same, it is judged as a malicious node.

4.4. Analysis of Communication Times. This section will compare the number of communications between the MDPBFT algorithm and the classic PBFT algorithm, the COMBFT algorithm [42], and the SPBFT algorithm [43] in the consensus process to verify that the MBFT algorithm has a relatively small number of communications.

Assuming that the number of nodes in the network is N, in the first stage of communication in the basic PBFT algorithm, the client first sends a request to the master node, and then the master node broadcasts the request to the rest of the nodes. The number of communications in the first stage is $(N-1)$ times. In the second stage, the remaining nodes need to respond to the pre-preparation message sent by the master node, broadcast consensus to each other, and

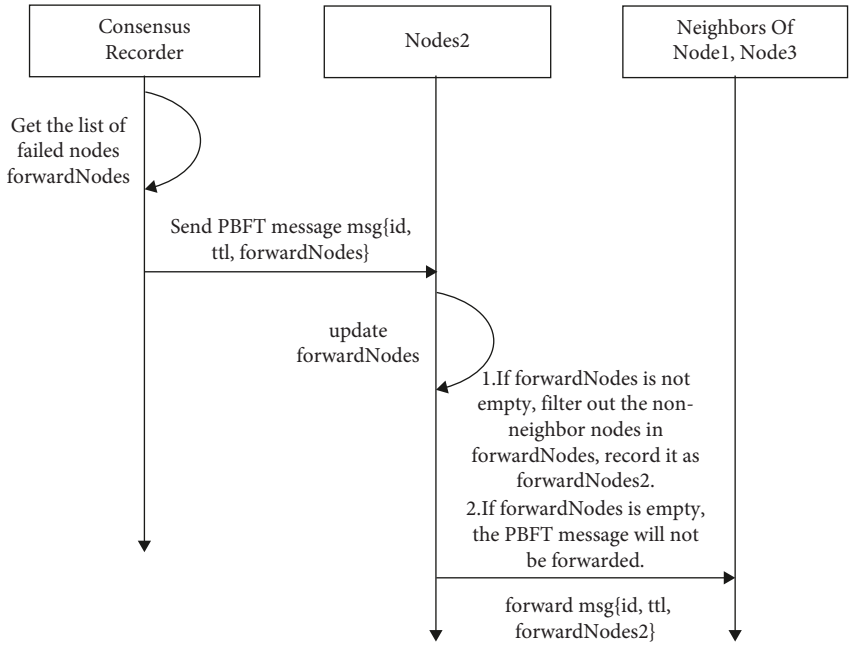


Figure 7: The communication forwarding process of the network disconnecting adjacent nodes.

the number of communications is $(N-1)^2$. All nodes in the third-stage system perform consensus feedback on the second-stage messages. Send an acknowledgment message to the master node, and the number of communications at this stage is $N(N-1)$. Based on the above analysis, it can be concluded that the communication times T_1 for the classical PBFT consensus algorithm to complete a consensus is as follows:

$$T_1 = 2N(N-1). \tag{2}$$

Unlike PBFT, in the COMBFT consensus algorithm, the client sends the message to all nodes when sending a request message. This is the first stage, and the number of communications is N. This mechanism divides the consensus protocol into normal and abnormal cases (with or without malicious nodes). In the normal case, the consensus process is designed into three stages. In the second stage, the master node sends messages to the slave nodes, and the number of communications is $N-1$. In the third stages, all nodes send reply messages to the client, and the number of transmissions is N, and then the number of contacts in the normal case is as follows:

$$T_2 = 3N(N-1). \tag{3}$$

The conflict-ordering mechanism (COM) needs to be implemented in abnormal cases. The SUSPECT phase is added to the consistency protocol. Each slave node sends SUSPECT messages to others except in this phase, and the master node sends messages to the client. The number of communications is $N*(N-1)+1$, and the number of contacts in the abnormal case is as follows:

$$T_3 = N*(N+2). \tag{4}$$

In the SPBFT consensus algorithm, although three stages of consensus are still required, it uses data encoding to assign different data requests to different nodes, so there is no need to broadcast messages to all other nodes in the preparation and confirmation stages. In the algorithm, the requested data is divided into multiple subdata, assuming that the number is also K. In the preliminary stage, the number of communications is still $(N-1)$. In the preparation phase, each node, except the master node only broadcasts the message to the other two nodes related to the news, and the number of communications in this phase is $2(N-1)$ times. In the confirmation phase, each node broadcasts the message to at least the other two nodes, and the number of communications in this phase is at least $2N$ times. Therefore, the number of contacts of the SNCPBFT algorithm is as follows:

$$T_4 = (5N-3)*K. \tag{5}$$

In the MPBFT algorithm, during a round of the consensus process, the node mainly communicates with the consensus recorder. In the first stage, the master node sends a message to the consensus recorder. The number of communications is 1. In the second stage, the consensus recorder sends $(N-1)$ messages. Nodes broadcast consensus messages and carry consensus copies. The third-stage node submits the consensus record to the consensus recorder and verifies whether the consensus of the remaining nodes satisfies the condition greater than $(2f-1)$, where the number of communications $(N-1)$. If the condition is met, each node submits the consensus confirmation result and returns the consensus recorder result $(N-1)$. The consensus recorder returns the result to the master node with a communication count of 1. To sum up,

$$T_5 = 2+3(N-1). \tag{6}$$

We compare T with the above four communication times because when $N \geq 12$ and the node scale is large, there are $T_5 < T_1$, $T_5 < T_2$, $T_5 < T_3$, and $T_5 < T_4$. So overall, the communication times of this scheme are less.

4.5. Security Analysis

4.5.1. The Multiset Architecture Proposed in This Paper Is Safe and Effective

Proof. In the PBFT algorithm, the PRE-PREPARE stage is the stage of requesting sequence number assignment, which is used to ensure that the request has been assigned sequence numbers in the current view. When multiple clients send request information to the nodes in the set, the nodes in the set will assign serial numbers and execute requests in sequence according to the preassigned serial numbers. Due to various attacks, this paper designs the nodes under the multiarea logistics information for identity verification and guarantees the nodes through a third-party identity verification agency. That is, each node that joins the network must be authenticated by a third-party agency. Nodes can be uniquely defined through hash value, key, and DNS name computer mechanism to prevent attacks such as Sybil attack. This method relies on verification by other institutions and will lose some of the node's anonymity. In the preparation stage, the request with the previous serial number will be executed first, and the node initiating the request will broadcasts the preparation message $\langle \text{PREPARE}, m, v, n, t, i \rangle$ through the consensus recorder. This stage is a preliminary consensus; in the confirmation stage, each node gives feedback on the messages broadcast by the consensus recorder. That is, each node sends a confirmation message $\langle \text{PREPARE}, m, v, n, t, i \rangle$ to the sending node through the consensus recorder. During this process, the consensus recorder will record and compare the return information of each node. If there is a malicious node, a node log will be recorded. Through the above process, the consensus validity of the multiset architecture can be guaranteed.

4.5.2. The Security and Data Validity of the Consensus Recorder

Proof. The consensus recorder is in the network and is not controlled by any node. The independence of the consensus recorder is guaranteed by updating the public smart contract. The execution of events (requests, confirmations, verifications) is automatically triggered by smart contracts (when set conditions are met). When a node sends a request, the smart contract of the consensus recorder generates a new consensus log, and the feedback of each node in the confirmation stage is recorded in the log. The smart contract of the consensus recorder automatically verifies the validity of the consensus of the node. It is enough to ensure that the feedback confirmation message satisfies $2f + 1$ benign nodes.

4.5.3. The Messages Responded to by the Node Set in This Paper Are Unique

Proof. There is no direct communication between node sets, and messages need to be transmitted through the consensus recorder. When a node in a set broadcasts a message, the consensus recorder records and relays the broadcast message, waiting for other nodes to feedback confirmation messages; feedback messages between sets are Recorded and verified in the consensus recorder, blocking data forgery communication between collection nodes. When the verification of nodes in a certain set is inconsistent, the malicious node is quickly located and recorded in the consensus recorder. When the verification of all nodes in a certain set is inconsistent with that of other set nodes, $2f + 1$ benign sets are also applicable.

5. Performance Analysis

This section compares the MPBFT algorithm proposed in this paper with the PBFT algorithm, SPBFT algorithm, and COMPBFT algorithm [42] regarding network bandwidth consumption and network delay. The experimental results illustrate the communication of the algorithm in this paperless overhead. The experiment's configuration in this paper is a Windows 10 system with an i7-4558U processor and 8 G.B. memory. The experimental simulation is carried out through MATLAB R2017a, and the number of nodes is 50, 100, 150, and 200. The size of the transmitted data is the same.

5.1. Network Bandwidth. Since the block size is constant, the required network bandwidth increases with the number of nodes. Different algorithms occupy different bandwidths. Algorithms with less communication time can occupy less bandwidth and thus consume less energy. The changes in network bandwidth and the number of nodes for the four algorithms are shown in the following figure. PBFT and SPBFT algorithms have three-stage message broadcasts, COMBFT has four groups of broadcasts, and MPBFT reduces the number of broadcasts and geographic distance through consensus repeaters. Therefore, the bandwidth occupied by the network is smaller than the other three algorithms.

5.2. Network Delay. Network latency is an important indicator reflecting the running speed of the blockchain system. The lower the network latency, the higher the system efficiency, the faster the consensus, and the higher the transaction efficiency. The relationship between the network delay and the number of nodes of the four algorithms is shown in Figure 8. It can be seen from the figure that with the increase in the number of nodes, the network delay is prolonged to a certain extent, and the network delay of the PBFT algorithm increases the most, which also explains the reason for improving the PBFT algorithm. As can be seen from the figure in this paper, the proposed MPBFT algorithm has a low delay and is relatively stable, which also

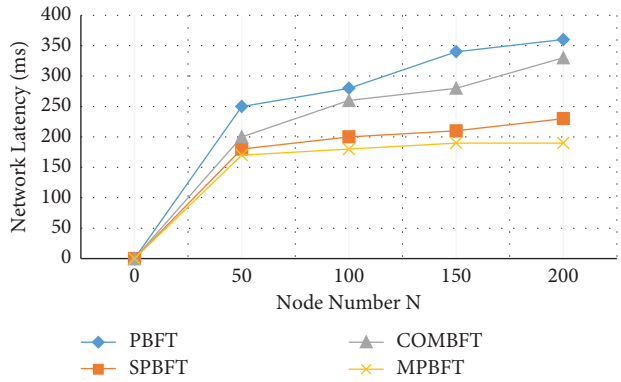


Figure 8: Comparison of network delays of four algorithms with different numbers of nodes.

shows that the scheme in this paper is more suitable for systems with a large number of nodes.

5.3. Throughput. Throughput is an important indicator reflecting the transaction rate of the blockchain system. The higher the throughput, the more the transactions per unit of time and the higher the consensus efficiency. The relationship between the throughput ratio of the four algorithms and the nodes is shown in Figure 9. It can be seen from the figure that as the number of nodes increases, the network throughput of the global environment will gradually decrease. When there are 200 nodes, the throughput of MPBFT is high. On the other three nodes, the MPBFT decline rate reflects that the multiset architecture can effectively improve the throughput of the multinode case. This also shows that the MPBFT consensus algorithm is relatively stable.

5.4. Algorithm Comparison. It can be seen from Figures 8–10 that PBFT, SPBFT, COMBFT, and MPBFT have low latency, high bandwidth, and high throughput in the 200-node MPBFT network. As shown in Table 3, the performance of the MPBFT consensus process is better than traditional algorithms (PBFT, SPBFT, and COMBFT) is more prominent. MPBFT consists of 3-stage communication and consensus recorder, which can reduce the consensus delay to a greater extent. The channel capacity is determined by the internal structure of the block. Only the block serial number needs to be agreed upon between the node sets. After the consensus is completed, the data in the block serial number is synchronized. Therefore, more block serial number data can be carried out during the consensus process. Scalability of consensus algorithms in the process of adding nodes, PBFT, SPBFT, and COMBFT all directly add nodes globally, while MPBFT adds nodes to the set, and when the consensus set reaches its peak, it expands the new set. When many nodes are added, the MPBFT global consensus performance is less affected. In

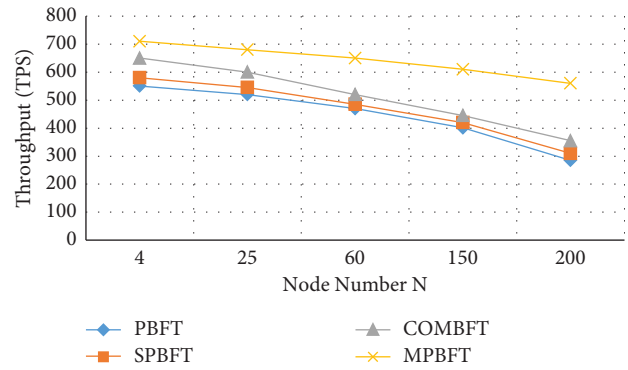


Figure 9: Throughput comparison of four algorithms with different numbers of nodes.

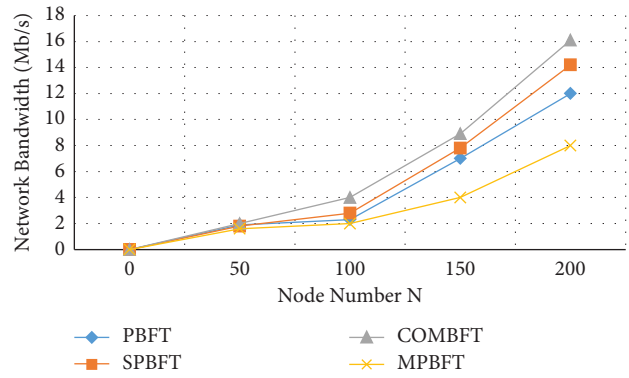


Figure 10: Comparison of network bandwidth of four algorithms with different numbers of nodes.

terms of applicability, PBFT, SPBFT, and COMBFT are not suitable for long-distance geographic location consensus, and the global consensus network delay is greatly affected by communication. MPBFT adopts a multiset architecture and deploys consensus sets based on geographic locations, which greatly reduces communication delays.

Table 3: The proposed algorithm is compared with the traditional algorithm.

Consensus algorithm	Throughput	Latency	Channel capacity	Scalability	Adaptability
PBFT	Low	3-stage medium latency	Low	Add nodes performance drops	Low latency short distance
SPBFT	Low	3-stage medium latency	Low	Add nodes performance drops	Low latency short distance
COMBFT	Medium	4 stages high latency	Medium	Add nodes performance drops	High fault tolerance short distance
MPBFT	High	3 stages and consensus recorder, low latency	High	Add nodes performance stable	High latency long distance

6. Conclusion

This paper first introduces the theory and technology involved in the blockchain logistics information traceability system. According to the characteristics of the logistics industry, a more efficient multiset consensus algorithm MDBFT is proposed, and the basic model and the entire implementation process of the algorithm are described. The feasibility of the algorithm is demonstrated by analyzing the communication times of the MDBFT algorithm. Through the comparative experiment and simulation of network bandwidth and network delay, it is verified that the algorithm can improve the consensus efficiency of logistics information, thereby ensuring the information's authenticity and traceability efficiency.

This paper proposes a logistics information traceability system based on blockchain. By improving consensus efficiency, an efficient traceability process is completed. With the development of blockchain technology, the system still needs to be perfected in practical application. This paper only improves the efficiency of logistics information traceability from consensus efficiency. However, there are still many factors that affect the efficiency of traceability, and further research is needed. This paper only considers the geographic information generated by the general logistics and circulation links and studies the traceability of general transportation route information to ensure the authenticity of the information traceability. In the future, the model can be further optimized. For complex logistics links, such as cold chain transportation, cross-border transportation, and other complex scenarios, various information such as temperature, humidity, and weather can be added.

Data Availability

The PBFT consensus time data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was supported by the Energy Cloud R&D Program through the National Research Foundation of Korea (NRF), funded by the Ministry of Science, ICT (grant no. 2019M3F2A1073387), and Institute for Information & Communications Technology Promotion (IITP) (grant no. 2022-0-00980; Cooperative Intelligence Framework of Scene Perception for Autonomous IoT Device).

References

[1] X. Lin, P. Jing, C. Yu, and X. Feng, "TPLI: a traceable privacy-preserving logistics information scheme via blockchain," in *Proceedings of the 2021 International Conference on Networking And Network Applications (NaNA)*, pp. 345–350, IEEE, Lijiang City, China, October 2021.

[2] M. Westerkamp, F. Victor, and A. Küpper, "Blockchain-based supply chain traceability: token recipes model manufacturing processes," in *Proceedings of the 2018 IEEE International Conference on Internet Of Things (iThings) and IEEE Green Computing And Communications (GreenCom) and IEEE Cyber, Physical And Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 1595–1602, IEEE, Halifax, NS, Canada, July 2018.

[3] S. Liang, M. Li, and W. Li, "Research on traceability algorithm of logistics service transaction based on blockchain," in *Proceedings of the 2019 18th International Symposium on Distributed Computing And Applications For Business Engineering And Science (DCABES)*, pp. 186–189, IEEE, Wuhan, China, November 2019.

[4] M. Schwarz, M. Lipp, D. Moghimi et al., "Cross-Privilege-Boundary Data Sampling," 2019, https://arxiv.org/abs/1905.05726.

[5] S. Wu, M. A. Rizoiu, and L. Xie, "Variation across scales: measurement fidelity under twitter data sampling," in *Proceedings of the international AAAI conference on web and social media*, vol. 14, pp. 715–725, California, CA, USA, May 2020.

[6] S. Ramírez-Gallego, B. Krawczyk, S. García, M. Woźniak, and F. Herrera, "A survey on data preprocessing for data stream mining: current status and future directions," *Neurocomputing*, vol. 239, no. C, pp. 39–57, 2017.

[7] P. Ranganathan, C. S. Pramesh, and R. Aggarwal, "Common pitfalls in statistical analysis: logistic regression," *Perspectives in clinical research*, vol. 8, no. 3, pp. 148–151, 2017.

[8] S. A. Alasadi and W. S. Bhaya, "Review of data preprocessing techniques in data mining," *Journal of Engineering and Applied Sciences*, vol. 12, no. 16, pp. 4102–4107, 2017.

[9] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," *Business & Information Systems Engineering*, vol. 59, no. 3, pp. 183–187, 2017.

[10] L. Xu, L. Chen, Z. Gao, Y. Chang, E. Iakovou, and W. Shi, "Binding the physical and cyber worlds: a blockchain approach for cargo supply chain security enhancement," in *Proceedings of the 2018 IEEE International Symposium on Technologies For Homeland Security (HST)*, pp. 1–5, IEEE, Woburn, MA, USA, October 2018.

[11] L. Zhang, L. Hang, and D. Kim, "Design of logistics information traceability system based on blockchain," in *Proceedings of the Korea Information Processing Society Conference*, pp. 244–247, Seoul Republic of Korea, December 2022.

[12] L. Barreto, A. Amaral, and T. Pereira, "Industry 4.0 implications in logistics: an overview," *Procedia Manufacturing*, vol. 13, pp. 1245–1252, 2017.

[13] M. Pease, R. Shostak, and L. Lamport, "Reaching agreement in the presence of faults," *Journal of the ACM*, vol. 27, no. 2, pp. 228–234, 1980.

[14] S. Nakamoto and A. Bitcoin, "A peer-to-peer electronic cash system," *Bitcoin*, vol. 4, no. 2, 2008.

[15] D. Larimer, "Delegated proof-of-stake white paper," *IEEE Access*, vol. 7, pp. 10–1109, 2014.

[16] M. Castro and B. Liskov, "Practical byzantine fault tolerance," *OsDI*, vol. 99, pp. 173–186, 1999.

[17] M. Castro and B. Liskov, "Practical Byzantine fault tolerance and proactive recovery," *ACM Transactions on Computer Systems*, vol. 20, no. 4, pp. 398–461, 2002.

[18] J. Borràs, A. Moreno, and A. Valls, "Intelligent tourism recommender systems: a survey," *Expert Systems with Applications*, vol. 41, no. 16, pp. 7370–7389, 2014.

[19] H. T. Nguyen, T. Almenningen, M. Havig et al., "Learning to rank for personalised fashion recommender systems via implicit feedback," in *Mining Intelligence and Knowledge Exploration*,Springer, Berlin, Germany, 2014.

[20] L. Marin, M. Pawlowski, and A. Jara, "Optimized ECC implementation for secure communication between heterogeneous IoT devices," *Sensors*, vol. 15, no. 9, pp. 21478–21499, 2015.

[21] Z. Dong, J. Chen, Y. Chen, and R. Shao, "Food traceability system based on blockchain," in *Proceedings of the 2020 International Conference On Aviation Safety And Information Technology*, pp. 571–576, Weihai, China, October 2020.

[22] X. Liu, A. V. Barenji, Z. Li, B. Montreuil, and G. Q. Huang, "Blockchain-based smart tracking and tracing platform for drug supply chain," *Computers & Industrial Engineering*, vol. 161, Article ID 107669, 2021.

[23] C. H. Wu, Y. P. Tsang, C. K. M. Lee, and W. K. Ching, "A blockchain-IoT platform for the smart pallet pooling management," *Sensors*, vol. 21, no. 18, p. 6310, 2021.

[24] S. Ni, X. Bai, Y. Liang, Z. Pang, and L. Li, "Blockchain-based traceability system for supply chain: potentials, gaps, applicability and adoption game," *Enterprise Information Systems*, vol. 16, no. 12, Article ID 2086021, 2022.

[25] J. M. Song, J. Sung, and T. Park, "Applications of blockchain to improve supply chain traceability," *Procedia Computer Science*, vol. 162, pp. 119–122, 2019.

[26] A. S. Omar and O. Basir, "Smart phone anti-counterfeiting system using a decentralized identity management framework," in *Proceedings of the 2019 IEEE Canadian Conference of Electrical And Computer Engineering (CCECE)*, pp. 1–5, IEEE, Edmonton, AB, Canada, May 2019.

[27] M. Rajesh, "Anti-counterfeiting and traceability mechanism based on blockchain," *Recent Trends in Intensive Computing*, vol. 39, p. 134, 2021.

[28] N. C. K. Yiu, "Toward blockchain-enabled supply chain anti-counterfeiting and traceability," *Future Internet*, vol. 13, no. 4, p. 86, 2021.

[29] T. McConaghy, R. Marques, A. Müller et al., "Bigchaindb: A Scalable Blockchain Database," *White paper BigchainDB*, Springer, Berlin, Germany, 2016.

[30] W. Yu and S. Huang, "Traceability of food safety based on block chain and RFID technology," in *Proceedings of the 2018 11th International Symposium on Computational Intelligence and Design (ISCID)*, vol. 1, pp. 339–342, IEEE, Hangzhou, China, December 2018.

[31] Z. Xie, H. Kong, and B. Wang, "Dual-Chain Blockchain in Agricultural E-Commerce Information Traceability Considering the Viniar Algorithm," *Scientific Programming*, vol. 2022, Article ID 2604216, 2022.

[32] C. Xu, K. Chen, M. Zuo, H. Liu, and Y. Wu, "Urban fruit quality traceability model based on smart contract for Internet of Things," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 9369074, 10 pages, 2021.

[33] Z. Wang, T. Wang, H. Hu, J. Gong, X. Ren, and Q. Xiao, "Blockchain-based framework for improving supply chain traceability and information sharing in precast construction," *Automation in Construction*, vol. 111, Article ID 103063, 2020.

[34] Y. Chen and F. Liu, "A Multi-Blockchain System Application Based on Improved PBFT Consensus Mechanism for Online Rumor Co-governance," 2022, https://assets.researchsquare.com/files/rs-2188736/v1_covered.pdf?c=1667892603.

[35] S. Coretti, A. Kiayias, C. Moore, and A. Russell, "The Generals' Scuttlebutt: Byzantine-Resilient Gossip Protocols," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, Los Angeles CA USA, November 2022.

[36] B. Arun, S. Peluso, and B. Ravindran, "ezBFT: decentralizing Byzantine fault-tolerant state machine replication," in *Proceedings of the 2019 IEEE 39th International Conference On Distributed Computing Systems (ICDCS)*, pp. 565–577, IEEE, Dallas, Texas, USA, July 2019.

[37] A. Litke, D. Anagnostopoulos, and T. Varvarigou, "Blockchains for supply chain management: architectural elements and challenges towards a global scale deployment," *Logistics*, vol. 3, no. 1, p. 5, 2019.

[38] S. Brotsis and N. Kolokotronis, "Blockchain-Enabled digital forensics for the IoT: challenges, features, and current frameworks," in *Proceedings of the 2022 IEEE International Conference on Cyber Security And Resilience (CSR)*, pp. 131–137, IEEE, Rhodes, Greece, July2022.

[39] Z. Tian, M. Li, M. Qiu, Y. Sun, and S. Su, "Block-DEF: a secure digital evidence framework using blockchain," *Information Sciences*, vol. 491, pp. 151–165, 2019.

[40] "Internet of Things architecture," 2022, https://www.ibm.com/cloud/architecture/architectures/iotArchitecture/reference-architecture.

[41] D. A. Horn and G. Bone, "Developing a business model for product environmental stewardship within IBM," in *Proceedings of the IEEE International Symposium on Sustainable Systems And Technology (ISSST 2010)*, p. 1, IEEE Computer Society, Arlington, VA, USA, May 2010.

[42] Y. Rong, W. Wu, and Z. Chen, "Combft: conflicting-order-match based byzantine fault tolerance protocol with high efficiency and robustness," in *Proceedings of the 48th International Conference On Parallel Processing*, pp. 1–10, Kyoto Japan, August 2019.

[43] B. Choi, J. Y. Sohn, D. J. Han, and J. Moon, "Scalable network-coded PBFT consensus algorithm," in *Proceedings of the 2019 IEEE International Symposium on Information Theory (ISIT)*, pp. 857–861, IEEE, Paris, France, July 2019.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 7011145, 24 pages
https://doi.org/10.1155/2022/7011145

Research Article

An Exploratory Study on the Design and Management Model of Traditional Chinese Medicine Quality Safety Traceability System Based on Blockchain Technology

Dacan Li,[1,2] Yuanyuan Gong,[3] Xianhui Zhang,[4] and Min Huang[5]

[1]*Institute of Social Governance, Hebei University of Economics and Business, Shijiazhuang 050061, China*
[2]*Hebei Collaborative Innovation Center on Social Governance by Morality and Laws, Shijiazhuang 050061, China*
[3]*School of Public Administration, Hebei University of Economics and Business, Shijiazhuang 050061, China*
[4]*Dongzhimen Hospital, Beijing University of Chinese Medicine, Beijing 100700, China*
[5]*Shanghai Public Health Clinical Center, Shanghai 201508, China*

Correspondence should be addressed to Yuanyuan Gong; yuanyuan@heuet.edu.cn

Received 7 March 2022; Revised 5 May 2022; Accepted 6 May 2022; Published 1 June 2022

Academic Editor: Chun-ho Wu

Aiming at the problems of long life cycle complex roles of participants, diverse risk factors, poor supervision coverage and difficult information traceability of TCM (Traditional Chinese Medicine) supply chain, this paper constructs a TCM quality safety traceability system based on blockchain technology by analyzing the business process and supervision characteristics of TCM supply chain. Blockchain technology is a new application mode of computer technology such as distributed data storage, peer-to-peer transmission, consensus mechanism, encryption algorithm, and other computer technologies. It has the characteristics of "decentralization, nontampering, transparent and open, and data traceability." The function of nontampering, hash function, and time stamp can effectively solve the traceability problem of TCM supply chain. Through the analysis of the blockchain TCM traceability principle and network structure, combined with the actual business process of TCM traceability, this paper designs the blockchain TCM quality safety traceability system, analyzes its overall structure, data storage mode, digital signature, consensus algorithm, and main functions, and preliminarily constructs a new model of TCM quality safety traceability management based on blockchain technology. Using blockchain technology to realize the quality safety traceability of TCM, we can complete the omnidirectional, multiangle, and wide coverage of the data and information in whole supply chain of TCM breeding and seedling raising, planting, innovation and research and development, processing of TCM pieces, circulation of TCM, and consumption, so as to realize that the main body of responsibility of TCM can be put on record, the production records can be queried, product flow can be traced, quality safety can be forewarned, main responsibility can be identified, regulatory information can be shared, and product source can be traced.

1. Introduction

TCM is the treasure of Chinese civilization and the crystallization of Chinese civilization for more than 5000 years. It has an extensive clinical application value and has formed a unique theoretical system, which plays an important role in the national health [1, 2]. The quality safety of TCM has always been a hot issue of national and social concern. The State Council of CPC Central Committee attaches great importance to the quality safety control of TCM. In the field of traceability of the quality safety of TCM, the state encourages producers and traders to use information technology to establish a traceability system for medicines, and encourages information technology enterprises as a third party to provide professional product traceability services to producers and operators. In the description of key tasks, it is emphasized that "we should establish and perfect the medicine information traceability system and form a complete traceability and supervision chain for the whole variety and the whole process [3]. The Chinese Government

issued the Opinions on Promoting the Inheritance and Innovation of TCM on October 20, 2019 [4], pointing out that it is necessary to vigorously promote the quality improvement of TCM and the high-quality development of the industry, strengthen the quality control of TCM, and strengthen the quality safety supervision of TCM, establish multisectoral collaborative supervision mechanism, explore the establishment of the whole process of traceability system in the production and circulation of Chinese herbal medicine, Chinese herbal pieces, Chinese patent medicine, and gradually realize that the source of key varieties of TCM can be traced, the whereabouts can be traced, the responsibility can be investigated.

The quality safety of TCM directly affects the development of the whole traditional Chinese medicine industry, and the establishment and perfection of TCM quality safety traceability system play a decisive role in improving the quality of TCM [5]. Due to the wide variety of Chinese herbal medicine, opaque breeding information, numerous industrial chain links, "Information silos" between participants, imperfect quality safety standards, and lack of unified quality safety supervision standards, it is difficult to supervise the Chinese herbal medicine supply chain, which makes it difficult to guarantee the quality of Chinese herbal medicine in the market [6].

Therefore, it is imperative to strengthen the quality safety control of TCM supply chain, and to build the quality safety supervision and traceability system of the whole supply chain by using the new generation of information technology, so as to ensure the quality safety of TCM from breeding, production and processing, innovative research and development, product circulation, sales and other links [7]. Blockchain technology has the characteristics of nontampering, traceability, safety, and credibility. The construction of TCM traceability system based on blockchain technology is expected to realize the supervision and management of the whole supply chain of TCM, so that the supply chain of TCM can be traced, the source of TCM can be inquired, the direction of products can be traced, and the main responsibility can be clarified in case of safety accidents, so as to promote the sustainable and healthy development of TCM industry. This paper mainly analyzes and designs the technical principle, business process, technical hierarchy, functional structure, data storage, and network architecture of TCM traceability system based on blockchain technology, aiming to provide basic methods and ideas for the research and application of blockchain technology in the field of TCM traceability.

This paper designs the blockchain TCM quality safety traceability system, analyzes its overall structure, data storage mode, digital signature, consensus algorithm and main functions, and preliminarily constructs a new model of TCM quality safety traceability management based on blockchain technology.

This paper mainly analyzes and designs the blockchain technology-based TCM tracing technology principle, tracing business process, overall structure, data storage, digital signature, consensus algorithm and main functions, and preliminarily constructs a new model of TCM quality safety traceability management based on blockchain technology, which provides basic methods and ideas for the research and application of blockchain technology in TCM traceability.

2. Problems in Conventional TCM Supply Chain Model

The supply chain of TCM involves the whole process from the planting of medicinal materials to the arrival of medicine in the hands of consumers. The space span is large and the time span is long. It is difficult to achieve effective supervision, resulting in frequent safety problems of TCM, such as excessive content of harmful heavy metals in TCM and fatal events of TCM injections, which undermine the trust of the people. After in-depth market research, it is found that the difficulty in tracing the drug supply chain data lies in the inability to ensure the accuracy of the traceability data and the lack of a trust consensus recognized by the public [8]. Drug safety is the foundation of people's livelihood. The TCM supply chain mainly has the following problems.

2.1. There Are Many Supply Chain Nodes and Many Unstable Factors. TCM supply chain includes breeding, production and processing, logistics, marketing, pharmacies, hospitals, and other links. In this process, there are unstable factors in all links of the supply chain. The final quality of TCM may be affected by many factors such as natural environment, processing conditions, man-made operation specifications, storage conditions, and logistics. There are many hidden risks in the whole supply chain [9]. Once a certain link changes, it is highly likely to affect the final drug quality, and then affect the stable development of the whole supply chain.

2.2. The Credibility of Information Is Low, and the Traditional Contract Is Difficult to Play a Binding Role. There are many participants in the TCM supply chain. Although each participant will sign a contract to restrict each other, due to many factors, the contract in the TCM supply chain cannot achieve the effect of restricting all parties. On the one hand, there is a high possibility of breach. The market supply-demand balance of TCM is affected by both natural environmental factors and market factors. The supply-demand relationship fluctuates greatly, resulting in large price fluctuation. The possibility of breach by all parties driven by interests will also increase, which virtually increases the breach risk of TCM. Even if there is no breach of contract, the information is easy to be tampered with. In the traditional operation mode of TCM supply chain, due to the limitation of technology, both the information of the product itself and the contract information are relatively easy to be tampered with. At the same time, all participants have the motivation to tamper with the information for the sake of interests. In addition, due to the lack of comprehensive supervision of the contents of the contract, when one party breaches the contract, the other party cannot even find it in time. The effect of restricting each link in the supply and marketing of TCM products only by contract is not ideal [10].

2.3. The Information Is Opaque and It Is Difficult to Achieve Fairness. Because the information available to participants in each link of the TCM supply chain shows asymmetry, the interests of all participants cannot be guaranteed, and adverse selection may occur at any time, so it is difficult for all participants to achieve relative fairness and equality in profit distribution. In the existing TCM supply chain, it is difficult for all participants to achieve relative fairness and equality in profit distribution. In the existing TCM supply chain, due to a series of reasons such as different qualifications, asymmetric information of enterprises at different positions in the supply chain, it is difficult for both parties to trade according to the real market value of TCM [11]. For example, in many cases, the most upstream of the TCM supply chain is the grower, and the information source channel of the grower is limited. When signing the contract with the grower, the production and processing enterprise of TCM often lowers the purchase price, infringing on the interests of the grower, resulting in the impact on the fairness of the supply chain model of TCM.

2.4. It Is Difficult to Supervise, Manage, and Trace the Responsibility. As there are many links in the TCM supply chain and the information is opaque, once the final drug has problems, the responsibility traceability is difficult to achieve [12].

The supply chain model of TCM should have the ability of flexibility, efficiency, equality, supervision, stability, and risk control. According to the characteristics of TCM and the change of market demand and the relationship between participants, it should be able to properly deal with the relationship and problems between participants, and promote the health and stability of the supply chain model of TCM. However, due to many links in the TCM supply chain, strong product characteristics, and complex influencing factors, it is very difficult to carry out the supervision and governance of the TCM supply chain.

2.5. Supply Chain Data Audit I s Difficult to Carry Out. The existing TCM supply chain includes multiple links, such as planting, R&D, production, sales, and logistics. The data information of each link is controlled by their own enterprises. Enterprises in different links have mastered part of the information of trading activities, so that the seemingly complete supply chain information is actually scattered in different links and chain nodes. When the audit work is carried out, the difficulty of the audit work will be greatly increased due to the noncooperation of some enterprises and the incomplete and irregular account records of some enterprises [13].

In recent years, the safety of TCM has been widely concerned by the society. Inferior TCM products have brought a great threat to people's life and property safety, but the subsequent accountability is difficult to continue because of the lack of reliable evidence or difficulty in locating the responsible party, which has seriously infringed on the rights and interests of consumers. In the TCM supply chain, the difficulty of mutual trust increases the cost of cooperation between participants, while the participants maintain their own databases and lack unified standards, which make the data of TCM in different circulation links chaotic, and the centralized operation mode is easy to cause information opacity, resulting in low reliability of traceability information [14].

The blockchain is a new decentralized data structure [15, 16], which is jointly owned, managed, and supervised by all nodes in the blockchain. It does not accept the control of a single aspect. The data is permanently recorded after being linked and cannot be tampered with. It has inherent technical advantages in solving the reliability problem of the traceability system. As the rise in counterfeit products and scandals about product quality can negatively impact the entire supply chain, introducing blockchains can help reestablish trust and transparency, improve the quality and speed of supply chain management, improve the transparency and traceability of inventory in the supply chain, and reduce risks [17–20].

With the increase of fake and shoddy drugs and drug quality scandals, it will have a negative impact on the whole supply chain. The introduction of blockchain will help to reestablish trust and transparency, improve the quality and speed of supply chain management, improve the transparency and traceability of inventory in the supply chain, and reduce risks [21–23].

3. Blockchain TCM Quality Safety Traceability Technology

3.1. Blockchain Technology. Blockchain is not only a hot topic but is also widely adopted in many sectors and disciplines [24]. Blockchain technology is a distributed storage database technology [25, 26], which is decentralized, tamper-proof, traceable, transparent, open, secure, and credible [27–29]. Blockchain technology is a distributed ledger that integrates cryptography, mathematics, hash function, and computer network technologies [30, 31]. Data in blockchain is distributed over the entire network and is organized by multiple centers to form a shared Internet database, and the node in the whole network maintains the blockchain data together [32]. The data is transparent and cannot be forged. In blockchain technology, data blocks are stored in chain structure, data storage nodes are distributed in network, and data information in nodes is updated by consensus algorithm. Cryptography is used to secure the storage and transmission of blockchain data, which is a new distributed database technology [33, 34].

Blockchain technology is a new distributed storage technology, which is characterized by peer-to-peer (P2P), distributed storage, asymmetric cryptographic algorithm, smart contract, timestamp and consensus trust, which uses a variety of computer combination technology and mathematical methods to achieve mutual trust between nodes [15, 35]. In blockchain technology, each node is independent from each other and has equal status. Consensus algorithm is adopted to verify and update data in distributed nodes. The data of blockchain is stored in chain structure, which makes every block data link up with each other, and every change of data information is recorded because of the time stamp mechanism, so as to ensure the authenticity of the data.

In blockchain network, the data is stored in "BLOCK." The data block includes block head and block body. The block head stores the hash function value of the previous

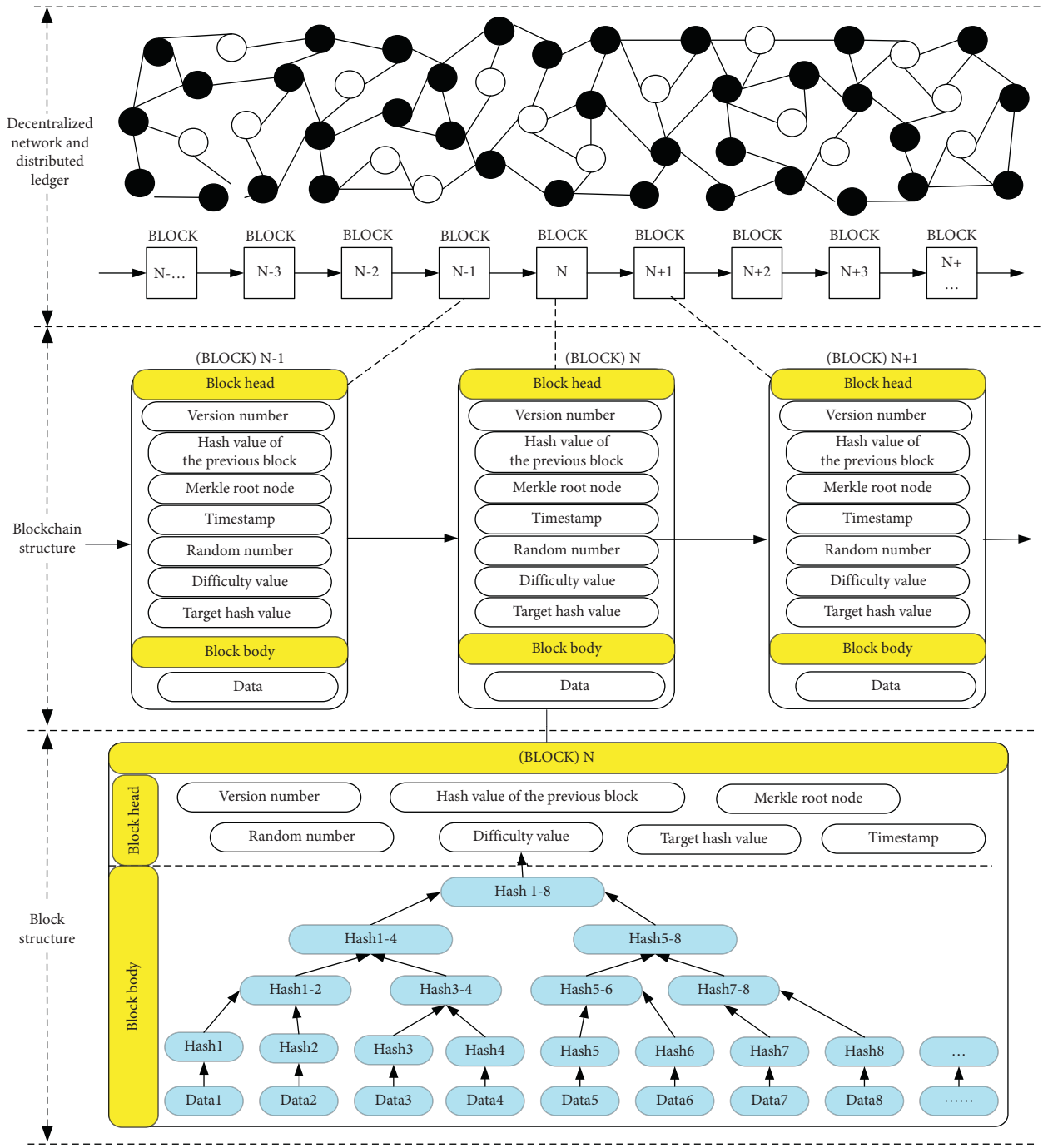


Figure 1: Technical structure of blockchain.

block, Merkle tree, timestamp, random number, version number, and other records; the block body stores the data information in blockchain. From the perspective of the basic data structure blocks of blockchain, all data are encapsulated independently in the form of blocks, but linked in turn. Each block is connected in chronological order through a chain structure. Each new block records the hash pointer of the previous block, and the hash function values between blocks are concatenated into a linked list [30, 36]. The technical structure of blockchain is shown in Figure 1.

3.2. Principle of Blockchain TCM Quality Safety Traceability. The information of TCM from breeding, production and processing to circulation and sales is opaque, and there is the problem of data islands, which makes it difficult to supervise and control the quality of TCM entering the market [22, 37]. However, when the blockchain technology is introduced, the whole process supervision of the TCM supply chain can be realized, ensuring that the use of TCM materials is traceable from the source of planting and breeding to the terminal consumption.

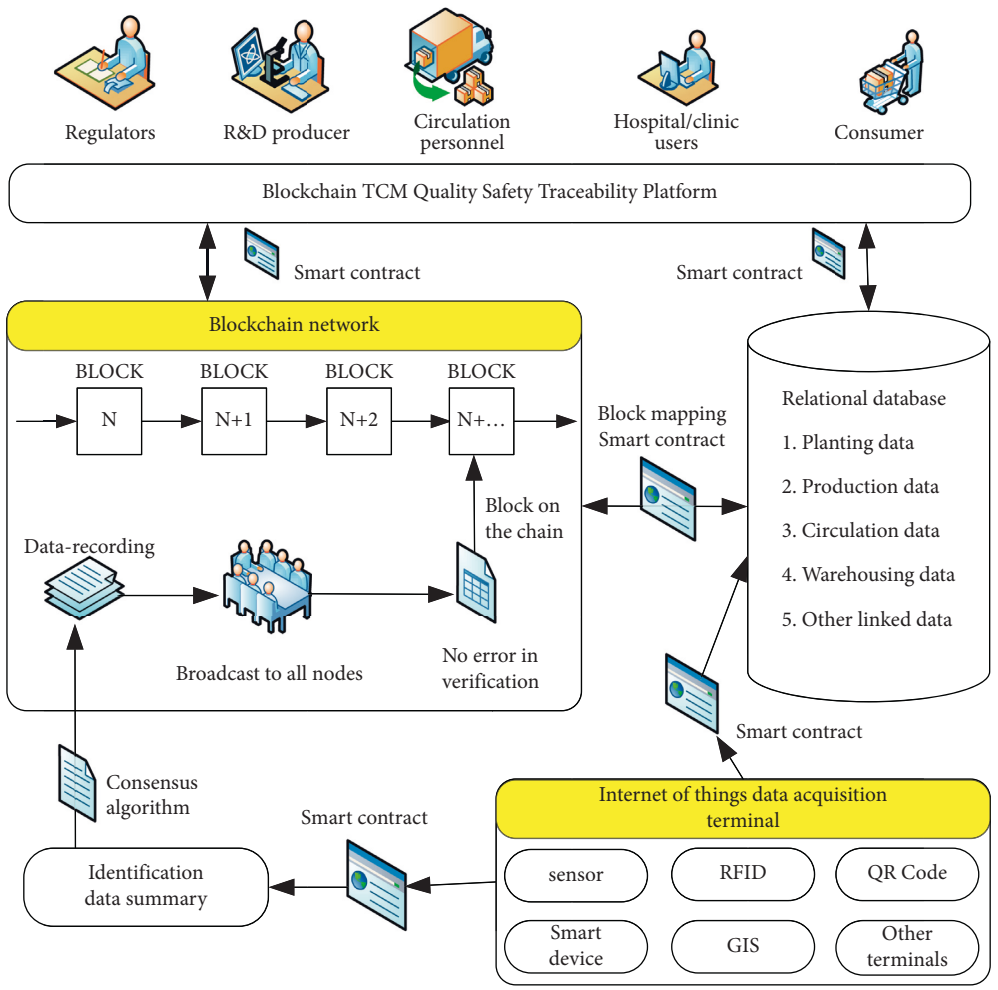


Figure 2: Technical principle of blockchain TCM quality safety traceability.

The whole supply chain of TCM includes various data information such as breeding, production and processing, logistics, and consumption. The source data information in the supply chain is generally collected by Internet of Things devices [38–40], and then hash operation is carried out to form the traceability code. The source data and hash traceability code are stored in the traditional relational database and blockchain, respectively. When the data acquisition terminal (sensor, two-dimensional code, RFID, etc.) collects the data of the supply chain, it first processes the data information by hash operation, and broadcasts the data information to the entire network combined with intelligent contract and consensus algorithm. Each node completes the confirmation and signature of data information. After confirmation, it is stored in the new block and connected to the main chain to form the traceability blockchain. The distributed nodes in the blockchain network jointly maintain the block data, which can realize the centralized sharing of data [41]. Each block contains a time stamp, that is, the blockchain is formed by orderly connection of data blocks in time dimension, so data can be traced back [42, 43]. The technical principle of blockchain TCM quality safety traceability is shown in Figure 2.

After the data of TCM supply chain is entered into the block, each block data is connected to the main chain in chronological order through hash function, and each node stores the whole database. Combined with cryptography technology, it can ensure that the data of TCM traceability blockchain is safe. TCM traceability blockchain has the characteristics of openness and transparency. The authorized participants can obtain the data information of the whole supply chain of TCM from breeding, production and processing to circulation and sales, so as to ensure the centralized sharing, integrity, and reliability of the data flow [44].

3.3. Network Structure of Blockchain TCM Quality Safety Traceability Platform. Network architecture refers to the physical layout of various devices interconnected by transmission media. The platform network architecture adopts a decentralized network layout, which can complete the whole supply chain traceability of TCM [45]. The network deployment of blockchain TCM quality safety traceability platform is shown in Figure 3.

Users mainly include users of government regulatory departments, TCM planting departments, R&D and

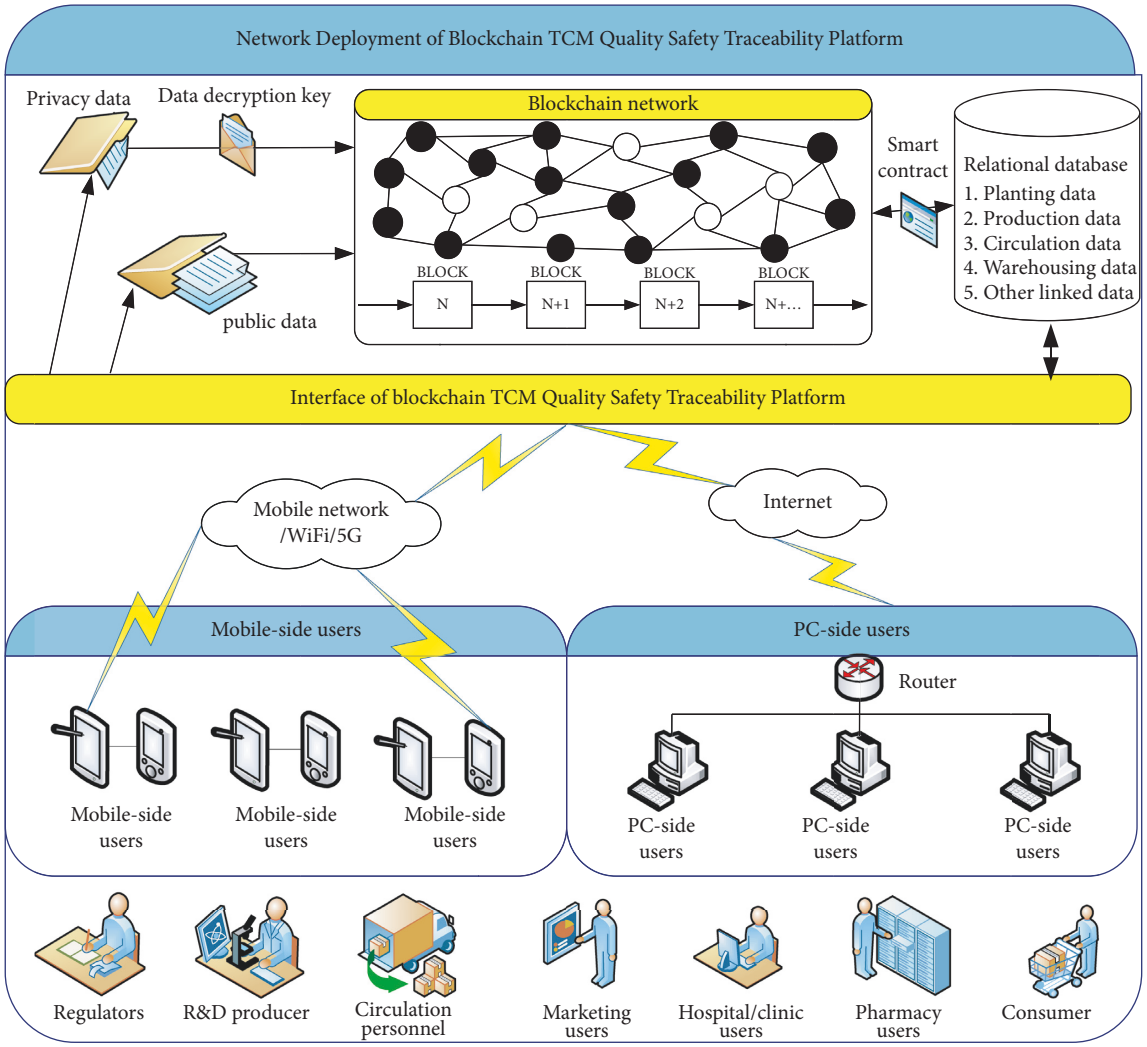


Figure 3: The network deployment of blockchain TCM quality safety traceability platform.

production departments, circulation departments, marketing departments, hospitals and clinics, pharmacies, consumers, and users in other links of TCM supply chain. Each user can access the blockchain TCM quality and safety traceability platform through the PC or mobile terminal.

4. Design of Blockchain TCM Quality Safety Traceability Platform

With the mature application of blockchain technology and the national policy support for the traceability of TCM, this platform provides a new idea to solve the problems existing in the quality and safety traceability of TCM, such as isolated island of data information, easy tampering of data, difficult traceability of data information, and difficult confirmation of responsible subjects [23, 44].

4.1. Blockchain Technology Platform Selection. According to the network scope, blockchain platform can be divided into public chain, private chain, and alliance chain [45–47]. In public blockchain, anyone can read the data, send transactions, and participate in the consensus process, such as Ethereum platform. The private chain is on the contrary. The permission to write data to the private chain is owned by only one institution/organization, and the reading permission is selectively open to the public. Alliance chain is a blockchain between public chain and private chain, which can be regarded as "semidecentralized," such as hyperledger blockchain. The consensus process of alliance chain is controlled by a number of preselected nodes, which usually have corresponding entities/organizations. Node participants join the network through authorization and form a stakeholder alliance to jointly maintain the operation of the blockchain. The comparison of public chain, private chain, and alliance chain is shown in Table 1.

Based on the comparison of each blockchain platform and the actual demand of TCM supply chain business, the TCM traceability platform is realized on the basis of alliance chain. The platform is Hyperleder Fabric.

4.2. Business Process Analysis of Blockchain TCM Quality Safety Traceability. The core of TCM quality safety

Table 1: Comparison of public chain, private chain, and alliance chain.

Blockchain type	Public access	Degree of decentralization	Efficiency
Public chain	Anybody	High	Low
Private chain	Private	Low	High
Alliance chain	Part	Middle	Middle

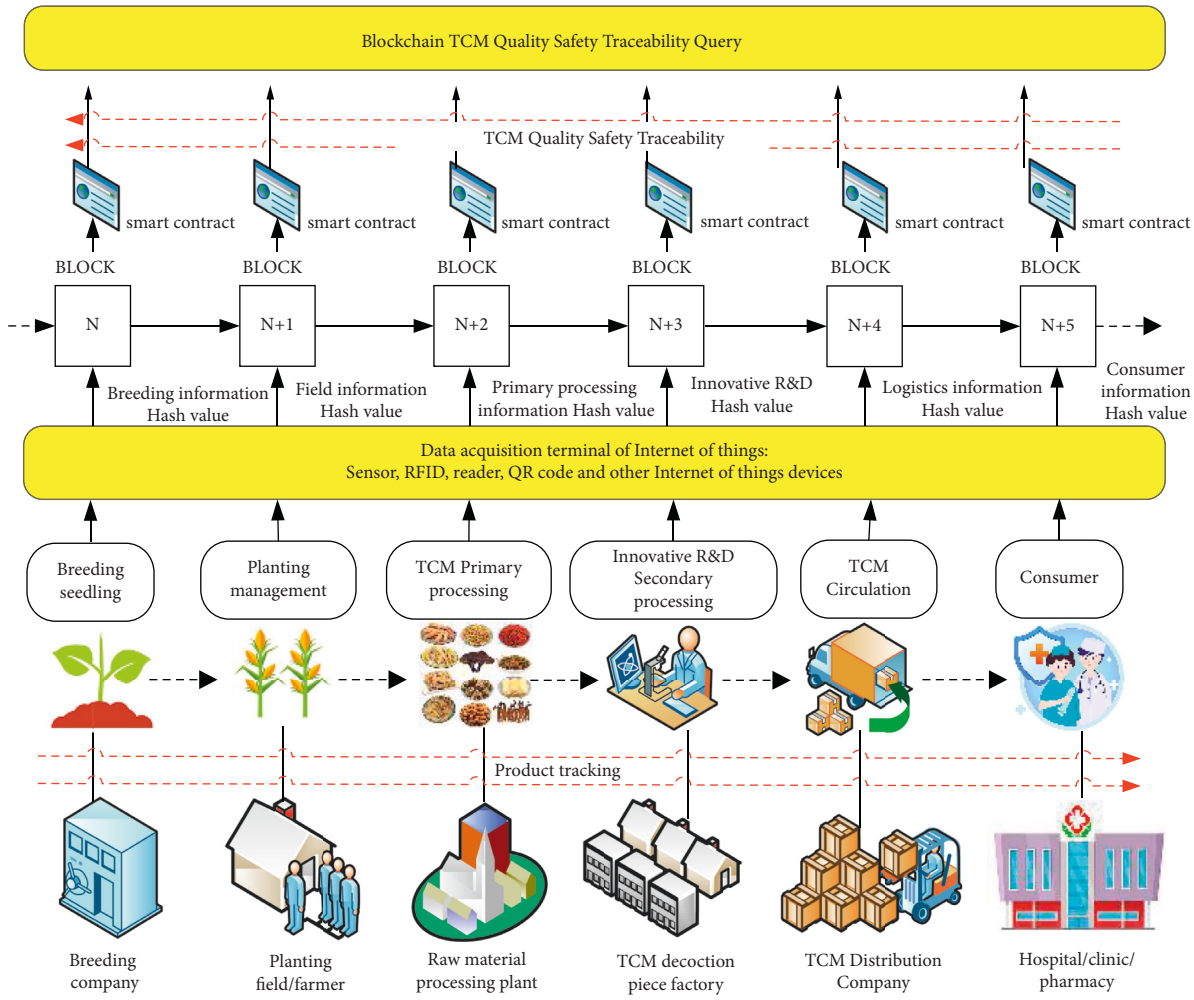


Figure 4: Business process of blockchain TCM quality safety traceability platform.

supervision lies in the controllable whole process of TCM supply chain. There are many participants in the process of TCM traceability, including the breeding, planting, harvesting, primary processing, warehousing, transportation, production, circulation, consumption, and other processes. The business process of blockchain TCM quality safety traceability platform is shown in Figure 4.

(1) Planting stage: It mainly provides seed selection management, environmental monitoring, growth tracking, and other functions. Seed selection management focuses on recording seedling name and seedling purchase information. The growers upload basic information such as species, planting area of TCM, as well as trading information with suppliers such as fertilizer vendors and seed vendors to the tracking platform.

(2) Storage stage: As the main information maintenance body in the storage link of TCM, storage enterprises are responsible for uploading information such as the warehousing time, storage methods, pest and mold prevention, and control records to the tracing platform [48]. The humidity detector can be installed in the warehouse for real-time monitoring. When the moisture content of TCM exceeds or falls below the standard range, the storage environment can be adjusted in time to ensure the quality and safety of TCM.

(3) Processing stage: It is the key to the quality safety of TCM, mainly providing technological process, environmental analysis, equipment management, and other functions. For example, the technological process focuses on recording the name, time, and

person in charge of each processing process of TCM. For the TCM products that have passed quality and safety monitoring, the two-dimensional code and barcode on the package, including the product name, product specification, and manufacturer, shall be uploaded to the traceability platform, so as to provide the quality and safety traceability inquiry channel for consumers.

(4) Logistics stage: It mainly provides the functions of TCM product flow, inventory management, environmental monitoring, etc. The environmental monitoring mainly focuses on the internal environment of TCM transportation vehicle, including temperature, humidity, and other information. Through real-time monitoring, logistics enterprises ensure the quality and safety of TCM in the process of logistics transportation, and ensure that all indicators of TCM are within the qualified range.

(5) Sales stage: It mainly provides TCM sales and after-sales management functions, in which TCM sales mainly records the name, quantity, price, sales time, hospital, drugstore, and other information of TCM; the after-sales management mainly records the information of return and exchange [49].

(6) Supervision stage: It is mainly managed by government departments, introducing relevant laws and regulations, technical standards, grade classification standards of TCM products, and part of the smart contract is thus constructed.

In the process of blockchain TCM quality safety traceability, firstly, the Internet of things acquisition terminal (including sensor, RFID, reader, GIS, bar code equipment, monitoring equipment, QR code, etc.) is required to collect the data of the whole supply chain of TCM, and then hash operation and digital signature are carried out. After passing the consensus algorithm, the hash value is uploaded to the blockchain, and the detailed data information of the whole supply chain of TCM is stored in the relational database under the chain. In the whole supply chain of TCM, member departments, government regulators, and consumers can view the traceability data of the whole supply chain of TCM by calling the blockchain quality and safety traceability platform of TCM.

4.3. Overall Architecture Design of Blockchain TCM Quality Safety Traceability Platform. Blockchain TCM quality safety traceability platform uses Internet of things technology and mobile Internet technology for real-time data collection, and uses blockchain technology for data storage, call, mining, and sharing [29, 50–52]. The overall architecture of blockchain TCM quality safety traceability platform studied in this paper adopts the classic six level blockchain structure, including data layer, network layer, consensus layer, incentive layer, contract layer, and application layer, as shown in Figure 5.

(1) *Data Layer*. The data layer stores the data information in the whole supply chain of TCM, mainly including two parts: one part is the distributed block data in the blockchain network, and the other is the relational database. The distributed block data records data blocks, hash functions, data abstracts, timestamps, Merkle trees, asymmetric encryption, digital signatures, public and private keys, chain structures, and other information. The relational database mainly stores the data information verified by the smart contract and the mapping relationship information between the blockchain networks [53].

(2) *Network Layer*. Blockchain network system mainly adopts peer-to-peer mechanism, data transmission, and verification mechanism. In essence, it is a P2P network. Network resources are allocated through the peer-to-peer mechanism. It does not need the traditional central node service mode, and all resources are jointly managed by each node. The communication protocol used in network layer is the data transmission Gossip protocol of the super ledger platform to improve the consensus speed and network security; the Internet of things devices use RFID, two-dimensional code, and other communication mechanisms; the transmission and communication mechanisms used in software operation mainly include Ethernet, WiFi, 5G mobile network, etc.

(3) *Consensus Level*. For blockchain, consensus layer mainly includes consensus algorithm mechanism, which is the unified rule of blockchain network and needs the consensus of all nodes to maintain and update the general database. Blockchain mainly uses POW, POS, DPoS, and other consensus mechanisms. With the increase of application scenarios involved in the TCM supply chain, the types of consensus mechanisms also increase. This traceability platform adopts the PBFT (Practical Byzantine Fault Tolerance Algorithm).

(4) *Incentive Layer*. Various incentive measures are used to reward the nodes that actively complete data processing in the blockchain network. For example, the economic incentive measures can be incorporated into the traceability system. The nodes that actively complete data processing will be given economic incentives, and the nodes that do not comply with the rules will be punished.

(5) *Contract Level*. Contract layer is the basis of blockchain programming, including scripts, algorithms and smart contracts of blockchain implementation. The smart contract is integrated into the traceability platform through the programming code, and the constraints are set without the endorsement of a third party, so that the real-time operation can be realized. After the TCM supply chain is collected through the Internet of things, the automatic uplink storage of data is completed through the intelligent contract and algorithm

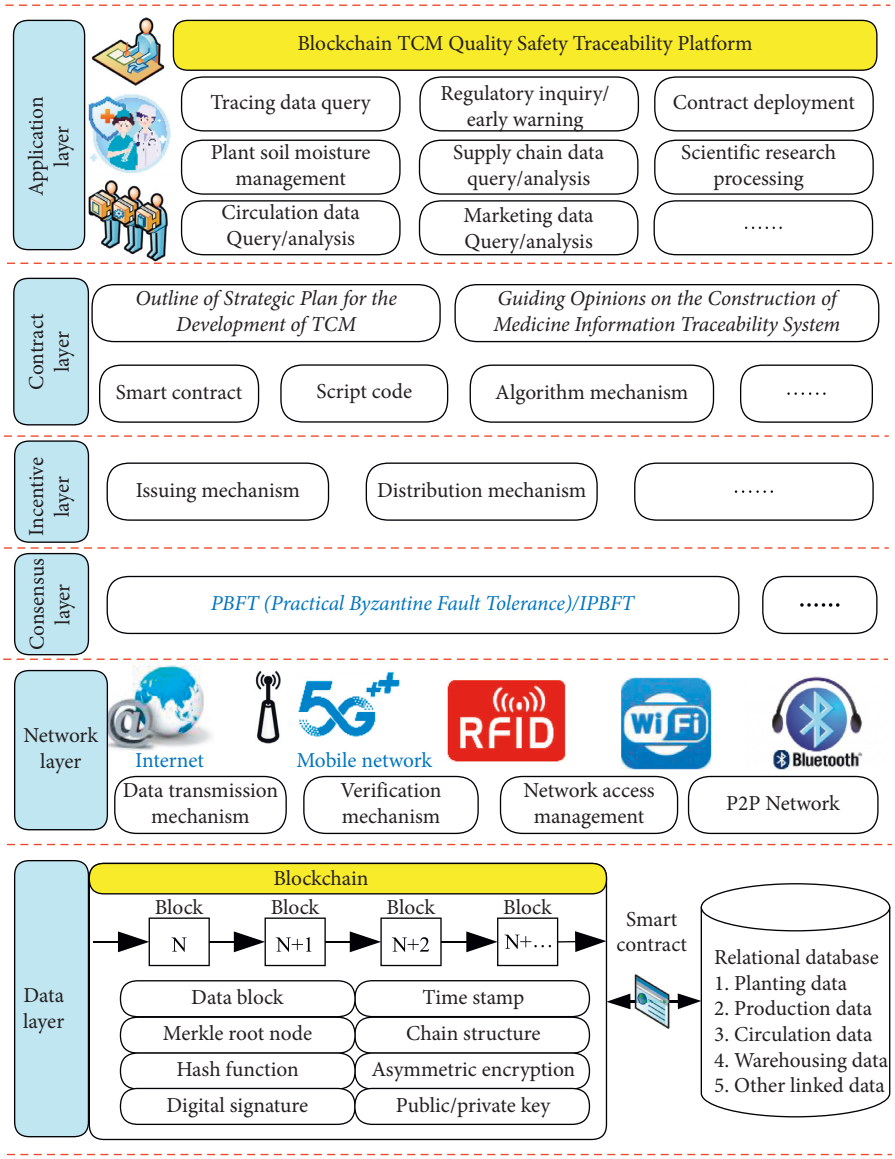


Figure 5: Layer architecture of blockchain TCM quality safety traceability platform.

mechanism [54]. In the blockchain TCM traceability system, the contract also includes the national traditional Chinese medicine law, the quality and safety management measures of TCM, the supervision and management measures of TMC, and other constraint mechanisms.

(6) *Application Layer*. Application layer mainly provides users with TCM data traceability management window through mobile terminal and the PC terminal application. On the basis of the existing blockchain network, application layer designs a complete TCM quality safety traceability platform through API interface provided by the underlying blockchain. The object mainly includes the government regulatory department of TCM, consumers, and other members in the whole supply chain of TCM. It is used to realize the business requirements of data information traceability and data analysis of TCM [53, 55].

4.4. Data Storage Design of Blockchain TCM Quality Safety Traceability Platform. The blockchain TCM quality safety traceability platform needs to collect the data of the whole TCM supply chain, which is very huge. In addition, due to the existence of various unstructured data information, if all the data of the whole TCM supply chain is stored in the blockchain, it will cause high operation cost and low operation and query efficiency [56]. The traceability platform studied in this paper adopts the storage mode of "blockchain" + "off-chain database." Off-chain database is a traditional relational database," which is managed by the government regulatory department and stores the data information of the whole TCM supply chain. Blockchain stores the data summary, timestamp, digital signature, hash tracing identification code, and other information of the original data of the whole TCM supply chain. The storage mode of "blockchain" + "off-chain database" cannot only improve the computing efficiency of blockchain, but also

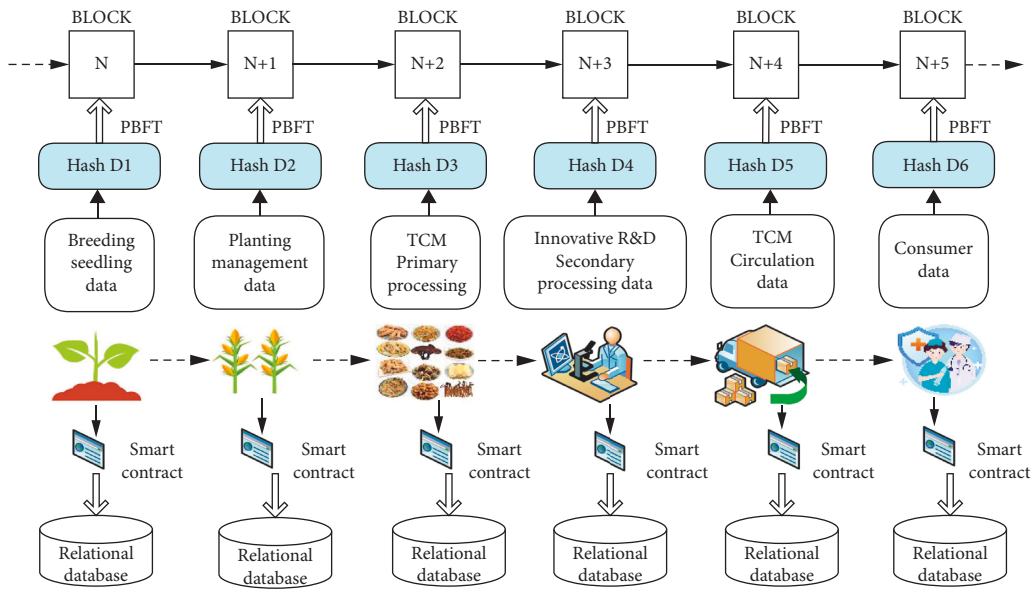


Figure 6: Data storage mode of blockchain TCM quality safety traceability platform.

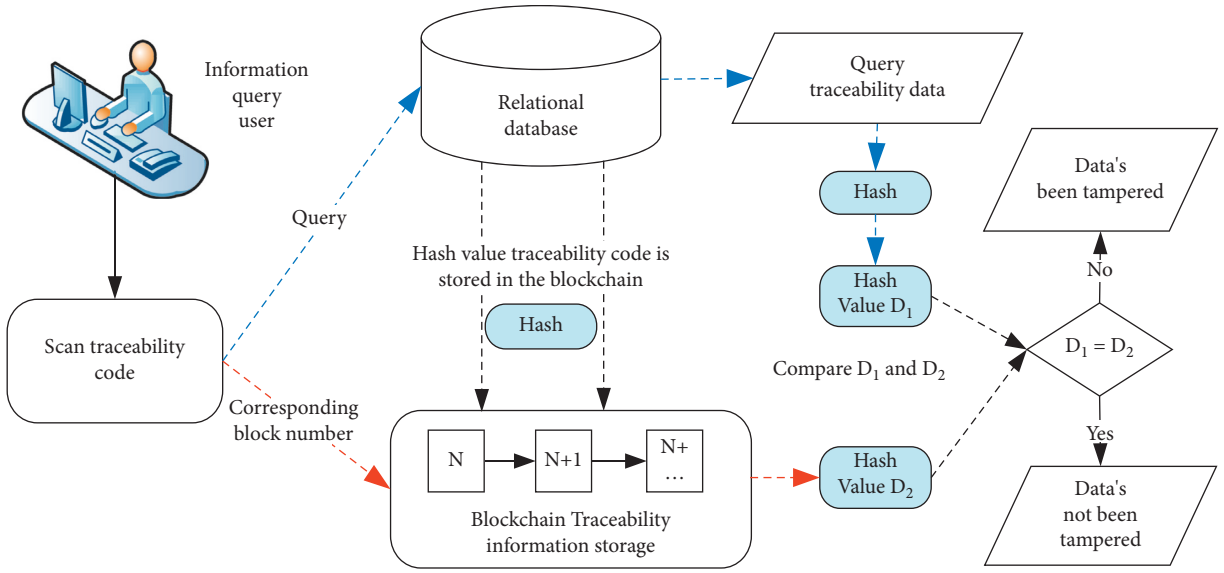


Figure 7: The query process of blockchain TCM quality safety traceability platform.

ensure the security and credibility of data [57]. The data storage mode of blockchain TCM traceability platform is shown in Figure 6.

The hash operation value (traceability code) of the original data stored in the blockchain is generated by hash calculation according to the relevant source data of the whole supply chain of TCM. Once the source data in the database under the chain is tampered, the trace code calculated through Hash will change, which is inconsistent with the corresponding trace code stored in the blockchain, so that it can be known that the data has been tampered [58]. The query process of blockchain TCM quality safety traceability platform is shown in Figure 7.

Taking the traceability query of traditional Chinese medicine supply chain information as an example, the fields of traceability information stored in the local database include: id, BatchNumber, TCMName, QualityGrade, OperationContent, OperationNumber, Operator, OperationTime, and BlockNumber. Where id is the unique identification [59] of the record information, and BlockNumber is the block number of the hash value of the traceability information on the blockchain. The specific traceability fields of the local database are shown in Table 2.

4.5. Digital Signature Design. The secure management and access control of IoT devices can be strengthened through the deployment of digital signatures and smart contracts using blockchain [60]. Blockchain uses digital signature algorithm to guarantee the authenticity of the participants

Table 2: The traceability fields of the local database.

Number	Field name	Field type	Field length	Null (true/false)
1	Id	Int	max	False
2	BatchNumber	Varchar	30	False
3	TCMName	Varchar	30	False
4	QualityGrade	Varchar	20	False
5	OperationContent	Varchar	500	False
6	OperationNumber	Varchar	20	False
7	OperationTime	Data time	10	False
8	Operator	Varchar	20	False
9	BlockNumber	Int	max	False

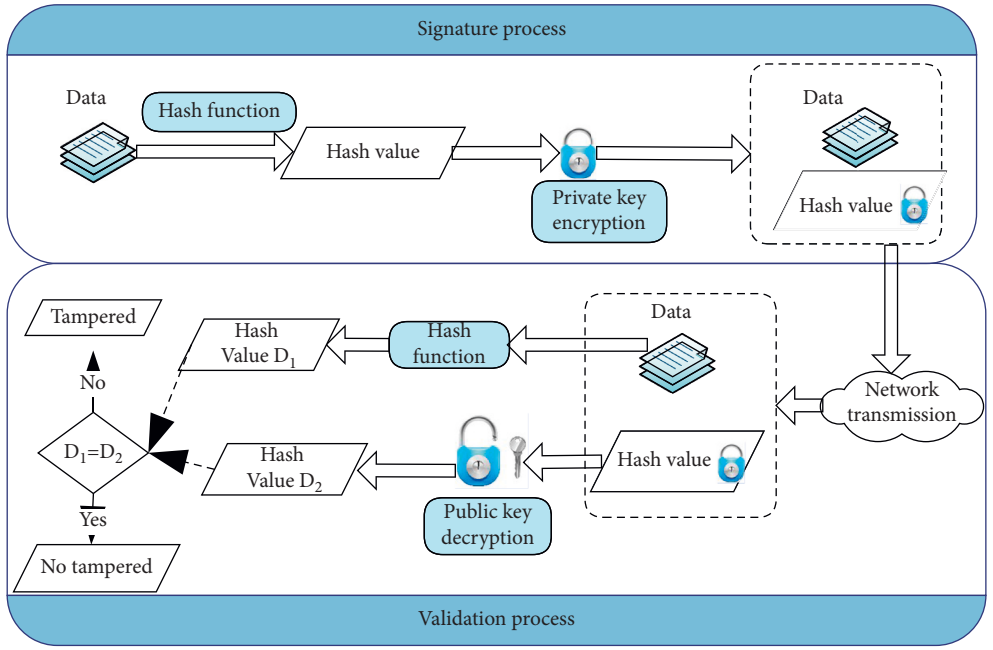


Figure 8: Digital signature process.

and the integrity of the message. Encryption is an effective technique to protect data security [61]. In blockchain technology, digital signatures use asymmetric encryption algorithm, including public and private keys [6]. The public key is the part of the key pair that can be exposed, while the private key can only be kept by the owner and is not exposed to the public. Digital signature is encryption with private key and decryption with public key. The signature + Verification process for digital signatures is shown in Figure 8.

The process of "signature + verification" of digital signature can be summarized as follows: the sender calculates the hash value through hash function, encrypts the hash value with the sender's private key, generates digital signature, and sends the data and signature to the receiver through network transmission. The receiver performs hash function on the received data, decrypts the received digital signature using the public key, and compares the generated D_1 and D_2 values. If the data is equal, it has not been tampered, otherwise it has been tampered. The digital signature algorithm used in this paper is ECDSA (elliptic curve digital signature algorithm) [62], and the process of signature calculation is shown in Figure 9.

If user A sends signature message to user B, they must reach a consensus on the curve parameters. The process of signature calculation is as follows:

Step 1. Take G as the base point on the elliptic curve and n as the integer order of G.

Step 2. User A creates a key pair, which is composed of private key d_A and public key Q_A. The private key d_A is randomly selected in the interval [1, n-1], and the public key Q_A is the product of elliptic curve point and scalar, as shown in formula (1).

$$Q_A = d_A * G. \tag{1}$$

Step 3. User a transfers the elliptic curve equation, base point G and public key Q_A to user B.

Step 4. Select an encrypted random integer k from the interval [1, n-1], and calculate the curve points (x_1, y_1), as shown in formula (2).

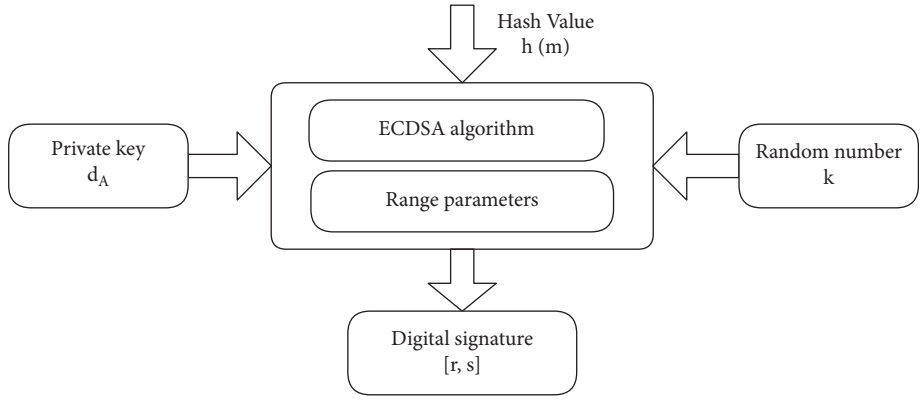


Figure 9: The process of signature calculation.

$$(x_1, y_1) = k * G. \tag{2}$$

Step 5. (*r*, s) is a pair of signature values, and the signature value *r* is calculated, as shown in formula (3). The mod function is the modulo operation. If $r = 0$, then return to step 4; instead, move on to the next step.

$$r = x_1 \bmod n. \tag{3}$$

Step 6. After calculating *r* value, input message digest h(m), private key d_A, signature value *R*, and random number *k*, and calculate signature value *s* according to formula (4). If $s = 0$, return to step 4; otherwise, the signature calculation is completed.

$$S = k^{-1}[h(m) + d_A * r] \bmod n. \tag{4}$$

4.6. Consensus Algorithm Design. The existence of consensus mechanism can keep the data unchangeable even when the blockchain network is attacked maliciously. Compared with the traditional centralized database, blockchain can complete each transaction without the intervention of the third-party certification authority, and each transaction is safe and reliable, but the premise is that users must follow the consensus agreed in advance [63].

PBFT (Practical Byzantine Fault Tolerance) consensus algorithm is a general solution to ensure the consistency between distributed system and Byzantine fault nodes [64]. Compared with consensus algorithms such as POW/POS/DPOS, it has the advantages of high efficiency and low energy consumption [65]. For the system with *n* nodes, PBFT consensus algorithm requires that when the data information input by the non-Byzantine nodes is the same, the result should be the same; for the transaction request, all the non-Byzantine nodes can receive, and under the premise of security, it is allowed to have no more than 1/3 failure nodes, that is, $n \geq 3f + 1$, it can be considered as an agreement [66, 67], where *n* is the total number of nodes and *f* is the number of failed nodes. PBFT consensus algorithm is suitable for alliance chain scenario.

PBFT algorithm is used to ensure the consistency among the alliance chain nodes [68]. The transmission of PBFT algorithm is shown in Figure 10.

C is the request node, 0, 1, and 2 are normal servers, and 3 is invalid server. The execution of the algorithm is as follows:

(1) Request: Node C sends a request to the master node, which is recorded as 0.

(2) Pre-prepare: After C requests the master node server 0, the server 0 passes to the secondary nodes 1, 2, and 3.

(3) Prepare: After secondary nodes 1, 2, 3 receive the delivery record, 1 continues to send to 023, 2 to 013, and 3 cannot be send.

(4) Commit: If nodes 0, 1, 2, and 3 receive more than a certain number of the same requests in the preparation phase, they will enter the submission phase and deliver the submission request.

(5) Reply: In the submission phase, if nodes 0, 1, 2, and 3 receive an excessive number of the same requests, they will give feedback to node C.

The time complexity of PBFT consensus algorithm is $O(n^2)$. N nodes in the network broadcast messages in the process of reaching a consensus, and each node needs to send messages to n-1 nodes, which makes PBFT algorithm show poor consensus performance when the number of nodes exceeds a certain number. Therefore, PBFT is only applicable to systems with a small number of nodes [69].

In view of the analysis of the problems existing in PBFT algorithm, this paper chooses to add the integral penalty mechanism to improve the algorithm [70], which is referred to as "IPBFT" consensus algorithm for short. By selecting a part of trusted nodes to form a verification node list L, the node is given the initial *Integration value* (*IV*) = 1. Each node needs to provide services to other nodes to maintain the integration. In each round of consensus, the best block is selected to verify the node packaging, and the coefficient λ is used to reduce the integration of the worst block packaging verification node, i.e., $IV = \lambda IV_i$, $\lambda \in (0,1)$. When the integral of nodes in the verification node list L is lower than a specified value ε, the node will be removed from the list.

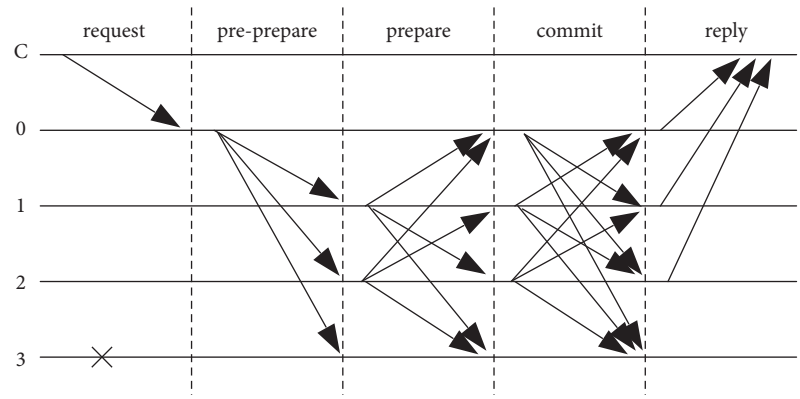


Figure 10: The transmission of PBFT algorithm.

When the remaining nodes in the list are less than 2/3, the list will be dissolved and a new verification node list L will be generated.

$P_L = \{P_1, P_2, P_3, \ldots, P_n\}$ is the set of verification nodes, the candidate set to be verified of P_i is $C(P_i)$, and the combined candidate set to be verified is

$$(CP_L) = \sum_{i=1}^{n} C(P_i). \tag{5}$$

The submitted terminal's packaged blocks $B_i = \{px_1, px_2, px_3, \ldots px_m\}$, $px_j \in C(P_L)$, the other verification combinations, and revenue sets obtained are represented as $O_i = \{\varphi_{i1}, \varphi_{i2}, \varphi_{i3}, \ldots \varphi_{in}; \mu\}$, and each terminal verification combination $(\varphi_{i1}, \varphi_{i2}, \varphi_{i3}, \ldots \varphi_{in})$ consisting of the blocks B_i packaged by a certain terminal P_i, the verification result of P_i submitted by P_i by any P_k participating in the verification is expressed as φ_{ik}, which satisfies the following relationship [69]:

$$\begin{aligned} \varphi_{ik} &= \begin{cases} 1, & \forall px_j\left(px_j \in B_i \wedge px_j \in C(P_L)\right), \text{Verified by } P_k, P_i \text{ submitted block is legal.} \\ -1, & \exists px_j\left(px_j \notin B_i \vee px_j \notin C(P_L)\right), \text{Verified by } P_k, P_i \text{ submitted block is illegal.} \end{cases}, \\ P_k &\xrightarrow{\varphi_{ik} = 1} P_i\colon \mu_i = \mu_i + 1, \\ P_k &\xrightarrow{\varphi_{ik} = -1} P_i\colon \mu_i = \mu_i - 1. \end{aligned} \tag{6}$$

4.7. Functional Structure Design of Blockchain TCM Quality Safety Traceability Platform. Blockchain TCM quality safety traceability platform mainly serves the upstream and downstream enterprises, government regulatory departments, and consumers in the TCM supply chain, including five functional modules: basic data management, data acquisition management, supply chain management, quality safety supervision, and traceability query. The basic data management is mainly responsible for the role and authority allocation of users, government supervision users, and consumer users in the whole TCM supply chain.

The functional structure of blockchain TCM quality safety traceability platform is shown in Figure 11.

The function of data acquisition is mainly responsible for the data collection and analysis, encryption verification, and other work in the whole supply chain. The function of supply chain management is mainly responsible for the inventory, production and processing, logistics and transportation, and sales management of the whole supply chain. The function of quality safety supervision is mainly responsible for the market access management, quality monitoring, monitoring and early warning management, commodity evaluation, traceability query, block query, authority allocation, and other work of upstream and downstream enterprises in the supply chain. Traceability query function provides product traceability services for consumers and authorized units in TCM supply chain, which can be queried through QR code or traceability code.

5. Analysis and Evaluation

5.1. Comparative Analysis of IPBFT and PBFT Algorithms. In this paper, we choose to add "integral penalty mechanism" to improve the PBFT consensus algorithm, which is called "IPBFT" consensus algorithm for short. Under the same experimental conditions, this paper compares the performance of the traditional PBFT consensus algorithm and the optimized PBFT consensus algorithm.

IPBFT algorithm realizes the dynamic distribution of verification power by adding the integral punishment mechanism, and gives certain punishment to the failed nodes, which improves the security of blockchain network and the efficiency of block generation. IPBFT algorithm uses the selected verification nodes for PBFT consensus, which can effectively reduce the number of consensus nodes and solve the problem that PBFT algorithm requires high network bandwidth.

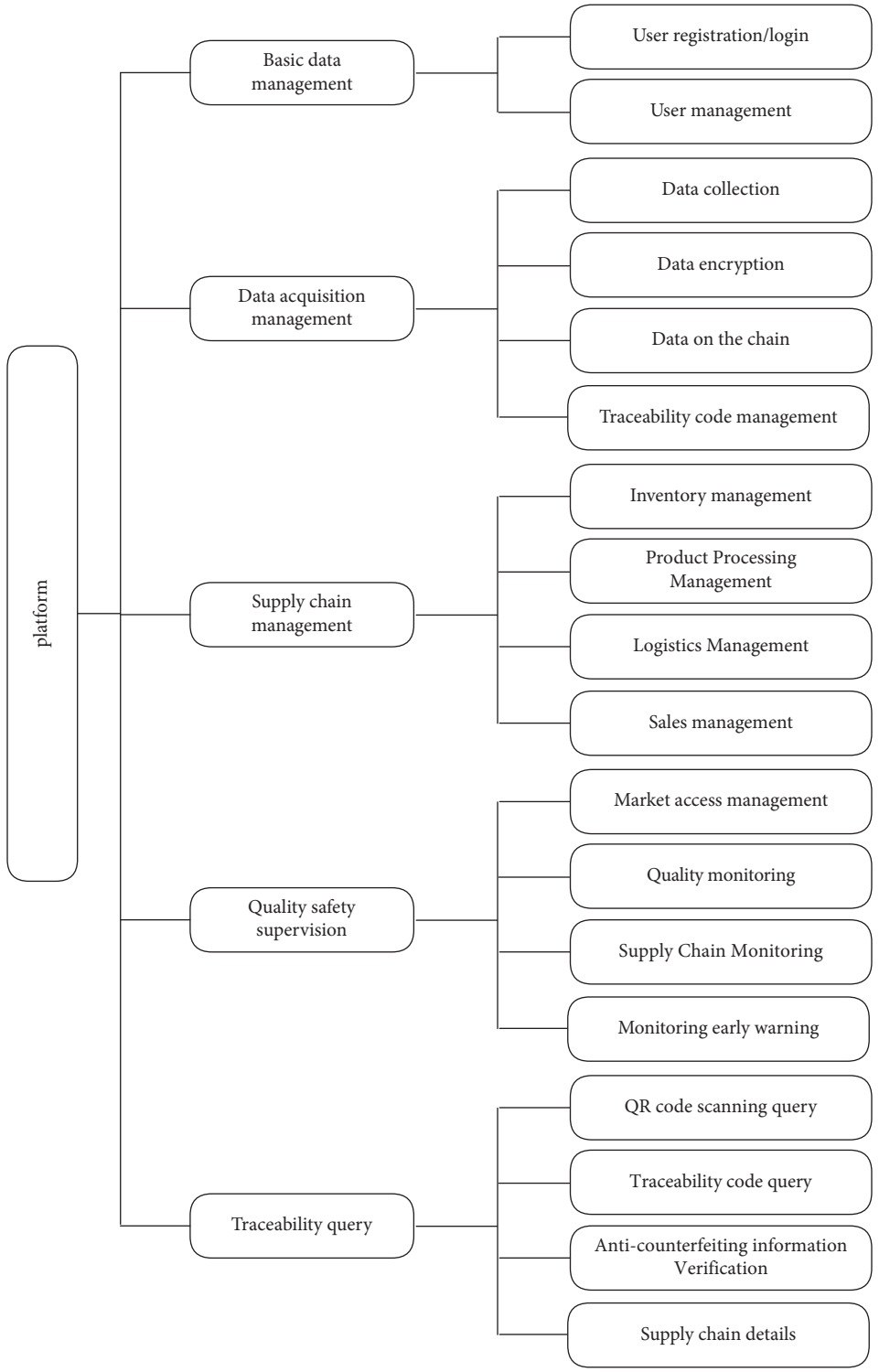


Figure 11: Functional structure of blockchain TCM quality safety traceability platform.

The process of reaching consensus requires each node to transmit data blocks to each other, and each transmission of data blocks needs to occupy a certain network bandwidth. The size of the transmitted data block is set to blocksize (B_s), the total number of nodes in the blockchain traceability system is set to n, and the network bandwidth occupied by all nodes to complete a data block transmission is set to bandwidth (B_w). Then, formula (7) can represent the network bandwidth required by all nodes in the network system to complete a data block transmission [71]:

$$B_w = n(n-1)B_s. \tag{7}$$

Through formula (7), it can be found that when the blocksize (B_s) is fixed, the bandwidth B_w increases with the

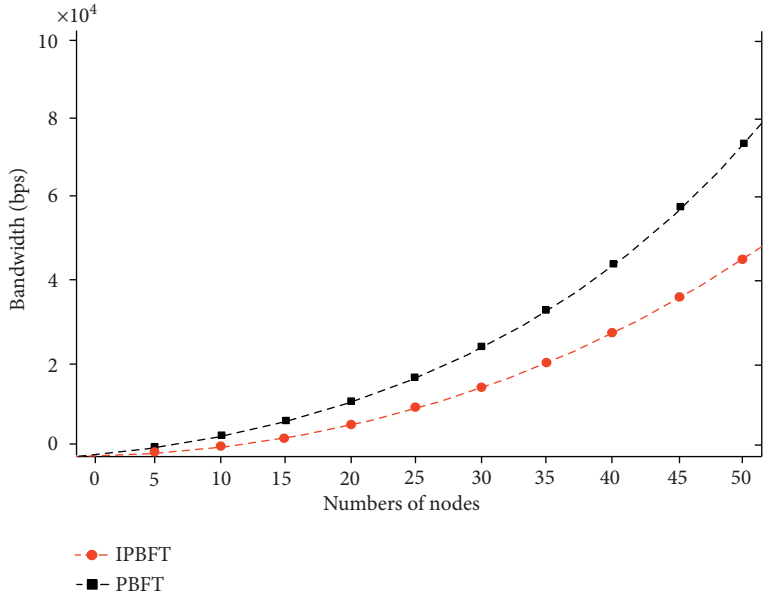


Figure 12: Comparison of network bandwidth consumed by IPBFT and PBFT consensus process.

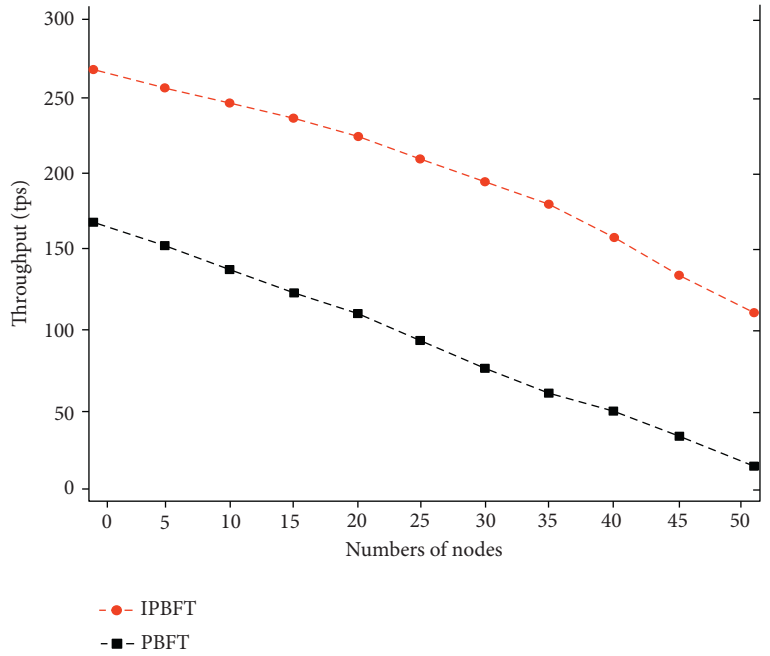


Figure 13: Comparison of throughput of IPBFT and PBFT consensus algorithms.

increase of the total number of nodes n. The IPBFT and PBFT network bandwidth curves are shown in Figure 12, where the abscissa is the number of nodes in the blockchain system and the ordinate is the network bandwidth.

The blockchain TCM quality safety traceability system designed in this paper adopts IPBFT consensus algorithm. Through the comparative analysis of the network bandwidth consumed by IPBFT and PBFT in the consensus process, it can be seen that under the condition of different number of nodes, the bandwidth consumed by consensus is different, and the bandwidth consumed by PBFT is larger. With the increasing number of nodes, the network bandwidth consumed by IPBFT algorithm increases slowly, while the network bandwidth consumed by PBFT algorithm increases rapidly. When the number of nodes in the blockchain system is 50, the network bandwidth consumed in the process of IPBFT reaching consensus is about 5×10^4 bps, while the network bandwidth consumed by PBFT is about 8×10^4 bps.

In the comparative analysis of IPBFT and PBFT, 2000 consensus requests are set and tested with different numbers of nodes. Figure 13 shows the comparison of throughput of

IPBFT and PBFT consensus algorithms with different number of nodes.

According to Figure 13, as the number of nodes in the blockchain system increases, the throughput of both IPBFT and PBFT algorithms shows a downward trend. For example, when the number of nodes is 10, the throughput of IPBFT algorithm is about 250 tps, and when the number of nodes increases to 50, the throughput of IPBFT algorithm is about 110 tps. When the number of nodes is the same, the throughput of IPBFT algorithm is higher than that of PBFT algorithm. For example, when the number of nodes is 20, the throughput of IPBFT algorithm is about 240 tps and that of PBFT algorithm is about 120 tps.

Therefore, it can be seen that under the same experimental conditions, the probability that the main node selected by IPBFT is a reliable node is high and the error probability is small. The throughput of IPBFT algorithm is better than that of PBFT algorithm; IPBFT can effectively reduce the consumption of network bandwidth, reduce traffic, shorten communication time, and accelerate consensus.

5.2. Retrospective Query Efficiency Analysis. The data storage of the traceability platform studied in this paper adopts the storage mode of "blockchain" + "database under the chain." The hash value of the traceability information is stored in the blockchain as the value, and the block number of the block where it is located is obtained; At the same time, the original traceability information and block number are stored in the database under the chain one by one. By reading the traceability information and block number from the data under the chain, the platform hashes the traceability information one by one, obtains the hash value stored on the blockchain through the block number, and compares the two hash values of each traceability information to judge whether the information has been tampered with. The improvement rate of TCM traceability query efficiency is calculated by formula (8) [58], $n_{A,B}$ represent the efficiency improvement rate of A than B; t_A,t_B represent the time required for A and B, respectively,

$$n_{(A,B)} = \frac{t_B - t_A}{t_B} \times 100\%. \tag{8}$$

The data storage and traceability query method designed in this paper is referred to as "A" method in this paper. In the process of designing blockchain data storage, many scholars store the original data directly on the blockchain, which is referred to as "B" method in this paper. For example, reference [58] introduces a key traversal query method, which writes the data information of product growth, processing, logistics and sales into the blockchain one by one, takes the ID of the traceability information as the key value, and stores the traceability information as the value in the blockchain; When querying, take the key as the index and traverse from the latest block to the next block in turn to obtain the matching value. In combination with the traceability business, there are multiple upload records of the traceability information of the product batch. Generally, the batch information is obtained during the query, and the block needs to be traversed according to the key for many times. The number of traversal times is related to the number of product batch traceability records. Due to the value stored in many nodes, the blockchain will have heavy load, high operation cost, and low operation and query efficiency.

In this paper, A and B methods are compared and analyzed, respectively. During the test, the same retrospective query operation is performed under the same conditions, and the query time will float up and down in a certain interval. In order to ensure the objectivity of the data, each group of data is executed 10 times, and its average value is calculated as the final value.

It can be seen from Figure 14 that under the same conditions, two methods A and B are used to query a single traceability record. In order to ensure the objectivity of the time used for traceability query, two methods A and B perform traceability query 10 times, respectively. The experimental results show that the method A is used to query a single trace record for 10 times, and the time of each trace query fluctuates up and down in 20 ms. Method B is used to query a single traceability record for 10 times, and the time of each traceability query fluctuates up and down in 50 ms.

The comparison of the two methods for tracing query time is shown in Figure 15. The ordinate is the Retroactive query time (RQT), and the abscissa is the number of retroactive records (TR).

As can be seen from Figure 15, when the number of trace records gradually increases, the time used by methods A and B gradually increases. When the number of trace records is 200, 400, 800, and 1000, method A takes less time than method B. According to formula (8), when the number of batch traceability records is greater than 200, the traceability query efficiency of method A is about 50% ~ 60% higher than that of method B.

5.3. System Performance Analysis. The main threat to TCM quality and safety traceability platform based on blockchain technology is the illegal tampering of block data. It is assumed that the calculation force of the honest nodes in the whole network is P times of hash value calculation per second, and the block hash value in the current calculation difficulty contains g prefix binary 0. The attacker is a new force, q hash calculations per second. The computation of old blocks for an attacker does not affect the speed of the creation of new blocks, so the calculation of new block hashes does not increase. To simplify the calculation, we assume that no new nodes participate, the probability of an honest node acquiring a new block per second is $p/2^g$, and the probability of an attacker acquiring a new block is $q/2^g$. Z_i is assumed to be the height difference in the ith second, and the possibility of height difference h per second can be divided into three situations [72], that is, the height difference decreases, the height difference increases, and the height difference remains unchanged. The probability of each result is P_1, P_2, P_3, respectively. The probability distribution of change of height difference h per second conforms to multinomial distribution.

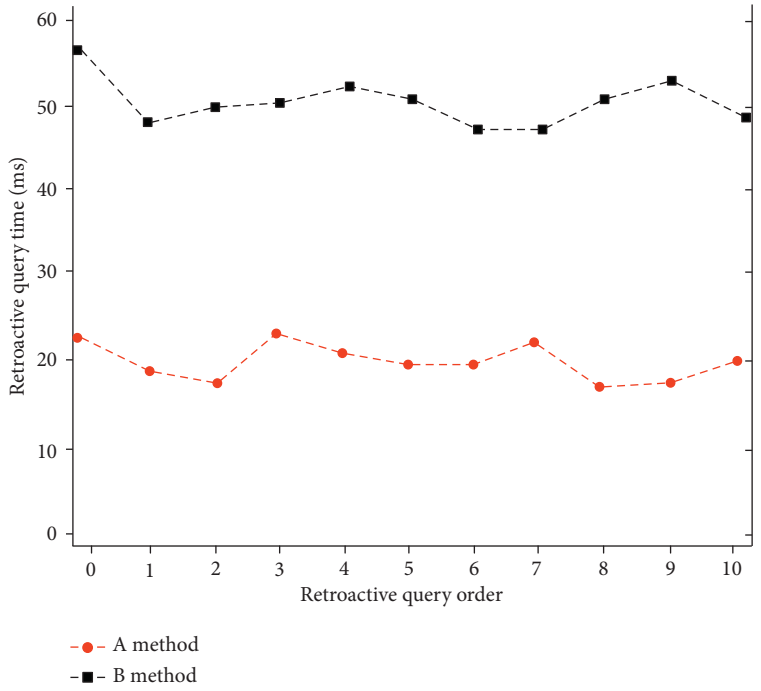


Figure 14: Comparison of the time taken to query a single traceability record in methods A and B.

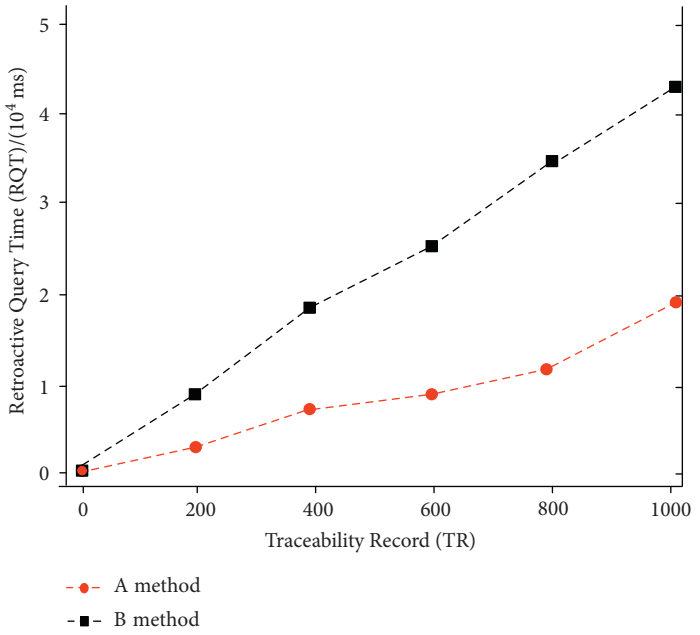


Figure 15: Comparison of tracing query time of methods A and B.

It is assumed that t kinds of results will occur within t seconds, and the number of occurrences of each result is represented by random variables X_1, X_2, X_3, where X_1 represents the number of occurrences of n, X_2 represents the number of occurrences of m, and X_3 represents the number of occurrences of $t-m-n$. The change probability of height difference h between honest node and attack node conforms to multinomial distribution [72].

In T seconds, if the attack node wants to catch up with the honest node, it needs to meet $n \in [0,(t-h-1)/2]$, $m = n + h + k$, and $1 \le k \le t-2n-h$. The probability is the following formula [72–74]:

$$P_{(h)}(t) = \sum_{n=1}^{(t-h-1)/2} \sum_{k=1}^{t-2n-h} t!/m!n!(t-m-n)P_1^n P_2^m P_3^{t-m-n}. \quad (9)$$

Formula (9) shows that the probability of an attacker tampering with block data decreases with the increase of block height difference h. Comparing the computing power

of attacking nodes with that of honest nodes, the probability of an attacker's success is shown in Table 3.

It can be seen from Table 3 that the probability of an attacker successfully tampering with block data decreases with the increase of block height difference h. When the height difference between honest node and attack node is $h = 4$, $ANCP/HNCP = 25\%$, 50%, and 100%, the data tampering success rates of attackers are $P < 0.01\%$, $P < 0.05\%$, and $P \sim 35\%$, respectively. When the height difference between honest node and attack node is $h = 6$, $ANCP/HNCP = 25\%$, 50%, and 100%, the data tampering success rates of attackers are $P < 0.01\%$, $P < 0.01\%$, and $P < 35\%$, respectively; When the height difference between honest node and attack node is $h = 10$, $ANCP/HNCP = 25\%$, 50%, and 100%, the data tampering success rate P of attacker is $P < 0.01\%$, $P \approx 0$, and $P < 35\%$, respectively. Even when the computing power of the attacking node is equal to that of the honest node, the success probability of data tampering of the attacking node is about 35%.

In the application scenario of Chinese herbal medicine supply chain, blockchain nodes are widely distributed, the amount of data in each link of the supply chain is huge, and the block height difference h is often large. Even if the attack node is equal to the honest node, it is almost impossible to complete the block replacement operation of this scale.

This paper uses the testing tool Caliper to test the performance of the blockchain TCM quality safety traceability system. The test mainly includes Write data (WA) and Read data (RA). The test results of throughput, transaction delay, and success rate of the blockchain system designed in this paper are shown in Table 4.

5.3.1. Test Results Analysis of Transaction Throughput and Transaction Success Rate. Write data test is to analyze the performance of written data, and Read data test is to analyze the performance of data query and data reading. According to the actual application scenario, the number of operations of data query and data reading of the blockchain traceability system is higher than that of data writing. Therefore, in the test benchmark configuration file, we set the number of operations of write data type to 2000 and the number of operations of read data type to 4000.

The write data test has conducted 6 rounds of tests, 2000 transactions are conducted to the blockchain system each time, and the six rounds of test send rate (requests per second) are set to 100, 200, 300, 400, 500, and 600, respectively. As shown in Table 4, the set send rate during the sixth round of test is 600 tps, and the actual send rate is 537.6 tps. At this time, the send rate has reached the peak. When the number of requests per second reaches 500, the throughput reaches the peak of about 250 tps. Continue to increase send rate, and the throughput fluctuates around 250 tps. When the send rate is 537.6 tps, there is data of transaction failure, but the overall transaction success rate is more than 99.9%.

The Read data test has conducted 6 rounds of tests, 4000 transactions are conducted on the blockchain system each time, and the six rounds of test send rate are set to 100, 200, 300, 400, 500, and 600, respectively. As shown in Table 4, when the send rate set during the sixth round of test is 600 tps, the actual send rate is 568.5 tps, and the send rate has reached the peak. When the send rate reaches 501.6 tps, the throughput reaches a peak of about 410 tps, and all transactions are successful.

Table 3: Probability distribution of attacker tampering with block data.

h	ANCP/HNCP*	P
$h = 4$	25%	$P < 0.01\%$
	50%	$P < 0.05\%$
	100%	$P \sim 35\%$
$h = 6$	25%	$P < 0.01\%$
	50%	$P < 0.01\%$
	100%	$P < 35\%$
$h = 10$	25%	$P < 0.01\%$
	50%	$P \sim 0$
	100%	$P < 35\%$

*ANCP: Attack node computing power; HNCP: Honest node computing power.

5.3.2. Test Results Analysis of Transaction Delay. In the write data test, when the send rate is about 100 tps, the average transaction delay is within 2 s and the response speed is fast. When the send rate is 537.6 tps, the response speed slows down and the average transaction delay reaches 8.67 s. At this time, the transaction fails.

In the Read data test, when the send rate is about 100 tps, the average transaction delay is within 0.5 s and the response speed is fast. When the send rate is 568.5 tps, the response speed slows down, the average transaction delay is 4.23 s, and all transactions are successful.

According to the above test results, the TCM quality safety traceability system based on blockchain technology designed in this paper has high throughput of data writing and query. When the send rate is about 400 tps, the average delay of read data operation is within 2 s, which can meet the actual business requirements of TCM quality safety traceability.

6. Discussion

Based on the analysis of key business of TCM traceability, combined with the actual needs of Chinese TCM strategic planning, this paper combs and optimizes the organizational structure and business functions, control process and management system, technical support, and implementation blueprint of TCM supply chain, which provides a strong guarantee for effectively improving the traceability management quality of TCM. The blockchain TCM quality traceability management mode mainly includes: National macro policies and laws and regulations of TCM, blockchain TCM quality safety traceability management system, blockchain TCM quality safety traceability service platform, blockchain TCM quality safety traceability standardization, government supervision and inspection, incentive, and punishment mechanism. The blockchain TCM quality traceability management mode is shown in Figure 16.

Table 4: Performance test results.

Test	Name	Succ	Fail	Send Rate	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Throughput
1	WA	2000	0	101.2 tps	1.98	0.79	1.55	101 tps
2	WA	2000	0	203.4 tps	2.31	1.08	1.97	151 tps
3	WA	2000	0	306.2 tps	2.76	1.59	2.35	189 tps
4	WA	2000	0	403.3 tps	3.11	1.98	2.78	220 tps
5	WA	2000	0	501.8 tps	5.72	2.92	4.11	254 tps
6	WA	1999	1	537.6 tps	11.45	4.32	8.67	247 tps
7	RA	4000	0	100.3 tps	0.47	0.21	0.32	98 tps
8	RA	4000	0	203.1 tps	0.87	0.46	0.61	190 tps
9	RA	4000	0	302.5 tps	1.99	0.79	1.31	277 tps
10	RA	4000	0	400.8 tps	2.55	1.37	1.88	345 tps
11	RA	4000	0	501.6 tps	3.87	1.96	2.66	412 tps
12	RA	4000	0	568.5 tps	5.16	3.05	4.23	406 tps

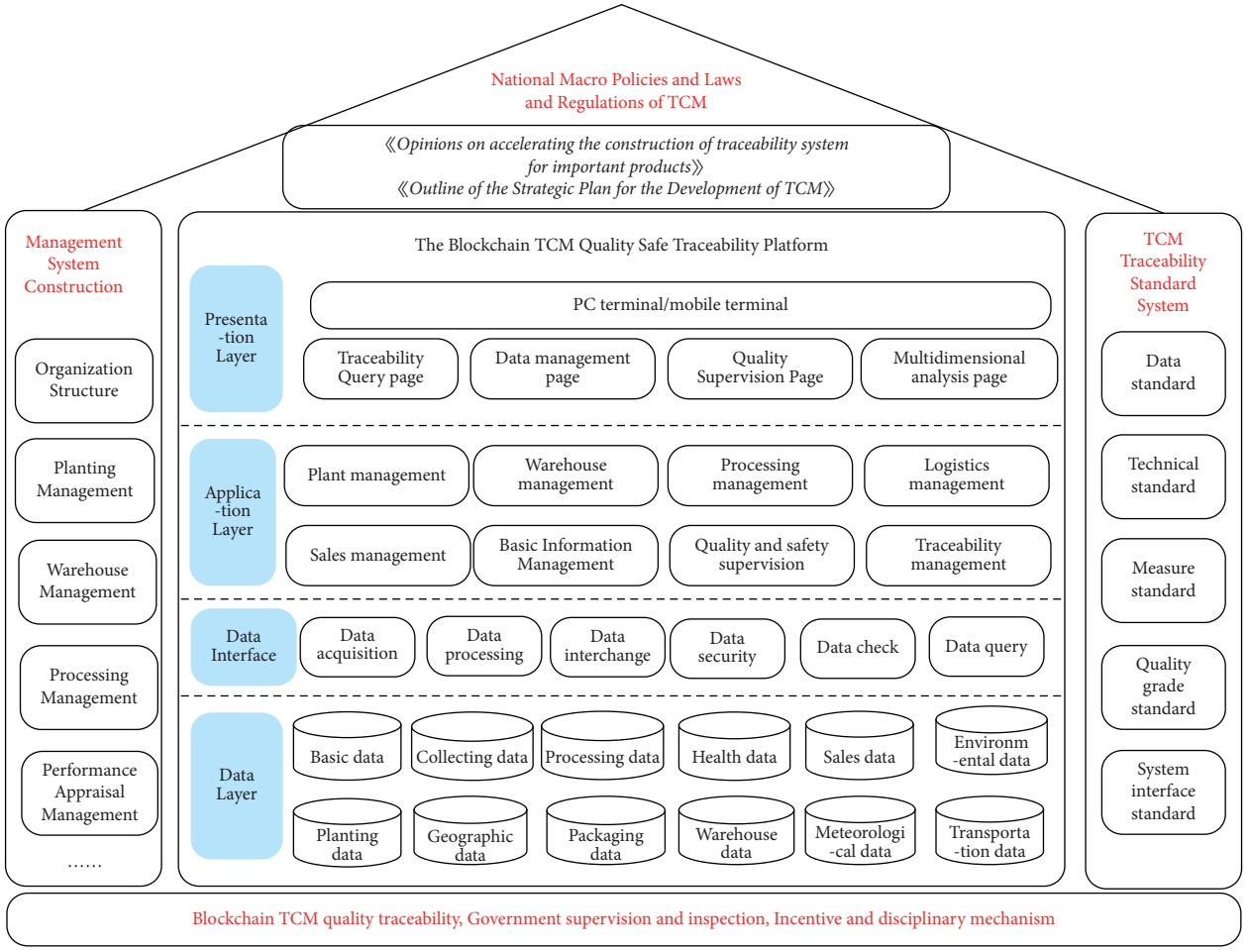


Figure 16: The blockchain TCM quality safe traceability management mode.

6.1. China's Macro Policies and Laws and Regulations on TCM. To support the development of TCM and ensure the quality safety of TCM, the state has introduced a number of relevant policies and measures in recent years. Blockchain TCM quality safety traceability system should be based on policies, laws, and regulations related to TCM. For example, in recent years, China issued *The Opinion about Quickening Construction of Important Product Traceability System*, *Outline of the Strategic Plan for the Development of TCM*, *Guiding Opinions on Promoting the Construction of Information Traceability System for Important Products*, *Guiding Opinions on the Construction of Medicine Information Traceability System*, and many other policies.

It is suggested that the government regulatory authorities should investigate and analyze all links of the TCM supply chain according to the local actual demand, form

legislative basis and suggestions, and formulate relevant supporting policies and guidelines on the TCM supply chain management, so as to make all aspects and links of the TCM supply chain have rules to follow.

6.2. Build a Blockchain Quality Traceability Regulatory Regime of TCM. An efficient regulatory regime can play an important guiding and normative role in the TCM supply chain management and the quality safety traceability, and can further ensure the safe and efficient operation of the whole TCM supply chain. In the process of TCM supply chain management, according to the actual needs, government regulatory departments, TCM breeding enterprises, TCM processing enterprises, TCM agents, public security departments, transportation departments, and individuals should be included in the TCM supply chain management system, which requires the formation of unified system norms under the concept of supply chain collaborative management to guide and restrict the business processes of all links of the TCM supply chain.

According to the national strategic plan, it is necessary to clarify the main body of medicine quality responsibility, establish a unified management standard system for TCM traceability, improve the organizational structure of participating units in all links of TCM supply chain, strengthen organizational leadership, refine objectives tasks, set up traceability management audit mechanism, and regularly carry out technical training, so as to ensure the orderly development of blockchain TCM traceability system management.

Government regulators should cooperate with all units in the supply chain to actively participate in the formulation of TCM supply chain regulatory regime, form a scientific and efficient TCM supply chain regulatory regime, and further improve the safety of TCM in the supply chain. Government regulators should also constantly optimize the working mechanisms for the formulation, implementation, evaluation, and improvement of the blockchain TCM quality traceability regulatory regime and strengthen the whole life cycle management of the system. They should also regularly sort out the system, prepare the plan for legislation, reform and waste, timely revise the management norms in important fields, and constantly enhance the pertinence and effectiveness. The government regulatory authorities should also strengthen the publicity and training of the regulatory regime for all units in the supply chain, regularly carry out supervision, inspection, and comprehensive evaluation of the implementation, and promote the effective implementation of the system.

6.3. Build the Blockchain TCM Quality Traceability Platform. It is necessary to design and develop a TCM quality traceability platform based on blockchain, big data, Internet of Things, 5G, and other information technology means. Starting from the implementation of national macro policies, we will give full play to the role of market supervision and operation regulation, and establish a quality traceability platform for the whole process of circulation of TCM to record the circulation information of medicinal materials in each link. By using the means of "blockchain + traceability of quality of Chinese medicinal materials," the identification and marking system suitable for certification and recognition is established to meet consumers' inquiry and reasonable consumption needs. By means of "blockchain + TCM quality traceability," the identification and marking system suitable for certification and accreditation should be established to meet consumers' query and reasonable consumption needs.

The government TCM supervision department should cooperate with the government information management department to continuously optimize and improve the function and performance of the TCM quality safety traceability system based on blockchain. The construction of TCM quality safety traceability system based on blockchain technology requires medical and research institutions, government regulatory departments, public security organs, transportation departments, charitable organizations, and other departments to reach a consensus and collectively join the blockchain traceability system. The government's TCM regulatory department is responsible for screening and reviewing the internal nodes of the alliance chain, coordinating all parties to form a smart contract in the blockchain system, and using the smart contract mechanism to realize the efficient upload, access and sharing of resources in all links of the TCM supply chain. Users can also spread and share resources in all links of the supply chain through P2P mechanism and encryption algorithm. At the same time, the government regulatory authorities also need to timely receive the user feedback of the blockchain traceability system and scientifically analyze the user feedback, so as to continuously optimize the business process of the TCM supply chain and further improve the collaborative management level of the TCM supply chain.

6.4. Build the Standardization System of Blockchain TCM Traceability Data. The construction of data standardization system is the key link of the TCM quality safety traceability. Due to the poor compatibility of various units and the lack of unified data standards in the TCM supply chain, it has brought many difficulties to the system connection and data integration. It can be seen that the lack of standardization is not conducive to the sharing of data in the TCM supply chain. Therefore, the government's TCM supervision department should take the lead in formulating the data standards of all links of the TCM supply chain, such as actively promoting the design and research and development of business and application standards, process and method standards, credibility and interoperability standards, data format standards, data transmission standards, and system interface standards, which can ensure the unity and standardization of data in all links of the TCM supply chain.

It is necessary to dynamically manage the product catalog of TCM as raw materials, and improve the technical standards covering such traceability elements as information coding, object identification, information identification,

supervision and management of TCM, and its products. It includes the development of blockchain TCM traceability data standards and measurement standards, the establishment of TCM traceability data model, the unified definition of data, in order to achieve data standardization and standardized management.

6.5. Build the Mechanism of Government Supervision, Inspection, Incentive, and Punishment. Make full use of the blockchain TCM to record the information of production and operation entities and product quality safety information, urge enterprises to strictly implement the traceability management system, and strengthen the supervision and inspection of production and operation enterprises and users. Explore and establish the credit supervision mechanism of traceability subject's product quality safety files and "blacklist" of quality dishonesty, form the joint incentive mechanism of keeping promise and joint punishment mechanism of dishonesty, encourage consumers to work together to feed back the quality information of Chinese herbal medicine products, and realize the forward tracking and backward traceability of TCM.

In a word, the blockchain TCM traceability platform can not only supervise the TCM from seed breeding, planting, processing, circulation to transaction, but also realize the whole process data information traceability of TCM from the source to consumers, so as to ensure the quality safety of TCM and promote the healthy development of TCM industry.

In the aspect of TCM cultivation, ensure that the source is known. Through the blockchain traceability platform, we can realize the source traceability and make the source of Chinese herbal medicine clear; we can extend the information traceability to the cultivation base, batch number, and cultivation information of Chinese herbal medicine, so as to ensure the quality of TCM from the source.

In the primary processing and production of TCM, the quality can be checked. The operation process of production records, origin processing, quality inspection, and other key links of TCM is comprehensively standardized, and timely uploaded to the blockchain traceability platform. The technical parameters of relevant processes are defined and recorded. The standardized process can ensure the quality of production links of TCM.

In terms of the circulation and use of TCM, ensure that the destination can be traced. Through the blockchain TCM quality traceability platform, the circulation link and storage link of TCM have been strengthened, and the destination of medicine terminal products can be traced.

7. Conclusion

Based on the blockchain technology, the quality safety traceability platform of TCM covering planting, production and processing, commercial circulation, and hospital use is constructed. With the characteristics of decentralization, openness, transparency and privacy protection of blockchain technology [75], the isolated island of traceability information can be broken, the information asymmetry can be reduced to the greatest extent, and the phenomenon of fraud and violation in TCM industry can be eliminated. It can realize the data traceability of the whole supply chain of TCM from planting and processing to circulation and sales, effectively improve the quality, safety, and credibility of the whole TCM industry, and lay a solid foundation for the modernization and the international market of TCM.

At present, based on the development level of TCM industry, blockchain technology continues to extend from the front end to the planting end in the production of TCM. The management measures at the planting end are managed on the chain to ensure the authenticity of information in planting, transportation, storage, processing, sales, and other links, so that all parties in the supply chain can benefit. The traceability data of TCM based on blockchain technology studied in this paper is structured data. The storage and traceability query of unstructured data such as video is the focus of the next research. In addition, blockchain technology can ensure the credibility and tamperability of the data after being linked to the chain, but cannot guarantee the credibility of the data source. In the next research, we can combine the Internet of things and sensor technology to record the data of the medicine supply chain in real time, reduce artificial fraud, further strengthen the credibility of the data, and improve the quality safety traceability level of TCM.

Data Availability

No data were used in this study.

Conflicts of Interest

The authors declare no conflicts of interest.

Authors' Contributions

Article conceptualization, D.L. and Y.G.; Business process analysis and overall architecture design, D.L. and X.Z.; digital signature and consensus algorithm design, M.H.; writing original draft preparation, D.L.; writing review and editing, Y.G., X.Z., and M.H.; submission, D.L. All authors have read and agreed to the published version of the manuscript.

Acknowledgments

This research was funded by the National Natural Science Foundation of China (82004297); the Humanities and Social Science Research Project of Hebei Education Department (SQ2021051); the Social Science Foundation Project of Hebei Province (HB21ZZ003); the Human Resources and Social Security Research Project of Hebei Province (JRSHZ-2022-02005); the Philosophy and Social Science Project of Xiong'an New Area (XASK20200022); the Project Approved by Shanghai Health Committee (201940014 and 202040046); and the Key Project of Social Governance of Hebei University of Economics and Business (2020ZLZD02 and 2022DZFZXT002).

References

[1] J. Guo, Z. Y. Xuan, and Y. Xie, "Problems and considerations in pharmaceutical researches of new traditional Chinese medicine," *Chinese Traditional and Herbal Drugs*, vol. 51, no. 8, pp. 2267–2272, 2020.

[2] W. W. J. Zhu, X. E. Liang, M. M. Feng, J. X. Chen, and J. J. Qin, "Discussion on the effective ways of the development of traditional Chinese medicine under the background of the belt and road," *Chinese Medicine Modern Distance Education of China*, vol. 19, no. 1, pp. 198–201, 2021.

[3] S. Zhao, M. Shi, S. Zheng, and C. Wen, "Thinking for traceable mode of establishing good price for high quality TCM based on traceability technology of safety and interconnection," *Modern Chinese Medicine*, vol. 19, no. 11, pp. 1515–1518, 2017.

[4] Cpc Central Committee and State Council, "Opinions on promoting the inheritance, innovation and development of traditional Chinese Medicine," *Gazette of the State Council of the People's Republic of China*, vol. 31, pp. 6–10, 2019.

[5] M. Y. Shi, C. B. Wen, X. Q. Wang, and S. T. Zhao, "Development of quality traceability system of traditional Chinese medicine," *Journal of Chengdu University of Traditional Chinese Medicine*, vol. 39, no. 3, pp. 109–113, 2016.

[6] C. H. Xie, W. W. Xiong, G. M. Li, and Y. Yang, "A quality and safety traceability system design for Chinese herbal medicines based on Blockchain technology," *Journal of Yunnan University of Nationalities (Natural Sciences Edition)*, vol. 29, no. 1, pp. 84–90, 2020.

[7] L. Xiao, X. Tan, P. Xie, Y. Tian, and C. B. Wen, "Research of traceability system of traditional Chinese medicine based on block chain," *Lishizhen Medicine and Materia Medica Research*, vol. 28, no. 11, pp. 2762–2764, 2017.

[8] Z. Liu and G. Y. Zhang, "Blockchain + Internet of things promotes food supply chain traceability," *Agricultural Engineering*, vol. 11, no. 2, pp. 51–55, 2021.

[9] F. Gao and J. Shi, "Research on the construction of agricultural products supply chain system based on blockchain," *Heilongjiang science*, vol. 12, no. 2, pp. 136-137, 2021.

[10] M. Qin, Y. Ju, and K. Li, "Research on agricultural products supply chain model based on blockchain technology," *Mall modernization*, vol. 14, pp. 7–9, 2021.

[11] M. X. Dai, "Enterprise supply chain management based on blockchain technology," *China business theory*, no. 16, pp. 105–107, 2021.

[12] H. Lu and Y. H. Xiao, "Discussion on the construction of the whole process traceability system of traditional Chinese medicine pieces," *Journal of China Prescription Drug*, vol. 19, no. 9, pp. 32-33, 2021.

[13] K. R. Zhao, "Discussion on the application of blockchain in the field of financial audit informatization," *China Collective Economy*, vol. 35, pp. 133-134, 2021.

[14] Z. Cao and L. Ding, "Research and design of agricultural product supply chain traceability system based on hyperledger sawtooth," *Modern computer*, vol. 18, pp. 156–162, 2021.

[15] E. de Boissieu, G. Kondrateva, P. Baudier, and C. Ammi, "The use of blockchain in the luxury industry: supply chains and the traceability of goods," *Journal of Enterprise Information Management*, vol. 34, no. 5, pp. 1318–1338, 2021.

[16] K. Raj Kumar Reddy, A. Gunasekaran, P. Kalpana, V. Raja Sreedharan, and S. Arvind Kumar, "Developing a blockchain framework for the automotive supply chain: a systematic review," *Computers & Industrial Engineering*, vol. 157, Article ID 107334, 2021.

[17] M. Kouhizadeh, S. Saberi, and J. Sarkis, "Blockchain technology and the sustainable supply chain: theoretically exploring adoption barriers," *International Journal of Production Economics*, vol. 231, Article ID 107831, 2021.

[18] P. R. Srivastava, J. Z. Zhang, and P. Eachempati, "Blockchain Technology and its Applications in Agriculture and Supply Chain Management: A Retrospective Overview and Analysis," *Enterprise Information Systems*, vol. 27, 2021.

[19] M. Alobid, S. Abujudeh, and I. Szűcs, "The role of blockchain in revolutionizing the agricultural sector," *Sustainability*, vol. 14, no. 7, pp. 4313–4315, 2022.

[20] X. Deng and Y. Ouyang, "Cross-border supply chain system constructed by complex computer blockchain for international cooperation," *Computational Intelligence and Neuroscience*, vol. 2022, Article ID 6221211, 10 pages, 2022.

[21] N. Kshetri, "1 Blockchain's roles in meeting key supply chain management objectives," *International Journal of Information Management*, vol. 39, pp. 80–89, 2018.

[22] J. Y. Park and C. S. Sung, "A business model analysis of blockchain technology-based startup," *Entrepreneurship and Sustainability Issues*, vol. 6, no. 4, pp. 1–12, 2019.

[23] M. Pournader, Y. Shi, S. Seuring, and S. C. L. Koh, "Blockchain applications in supply chains, transport and logistics: a systematic review of the literature," *International Journal of Production Research*, vol. 58, no. 7, pp. 2063–2081, 2020.

[24] V. Chang, S. Gagnon, R. Valverde, and M. Ramachandran, "Guest editorial," *Journal of Enterprise Information Management*, vol. 34, no. 5, pp. 1277–1286, 2021.

[25] C. S. Sung and J. Y. Park, "Understanding of blockchain-based identity management system adoption in the public sector," *Journal of Enterprise Information Management*, vol. 34, no. 5, pp. 1481–1505, 2021.

[26] H. Yi, "A secure logistics model based on blockchain," *Enterprise Information Systems*, vol. 15, no. 7, pp. 1002–1018, 2021.

[27] Y. X. Zhang, J. H. Ding, and M. T. Xing, "Discussion on the development of new agricultural industrial structure based on "blockchain" technology," *Co-Operative Economy & Science*, vol. 8, pp. 26-27, 2020.

[28] B. Q. Yang, "Prevention of Business Risks of Internet Information Security Platforms Based on Blockchain Technology," *Computational Intelligence and Neuroscience*, vol. 2022, Article ID 7671810, 10 pages, 2022.

[29] Y. P. Tsang, K. L. Choy, C. H. Wu, G. T. S. Ho, and H. Y. Lam, "Blockchain-driven IoT for food traceability with an integrated consensus mechanism," *IEEE Access*, vol. 7, no. 1, Article ID 129000, 2019.

[30] A. Hughes, A. Park, J. Kietzmann, and C. Archer-Brown, "Beyond Bitcoin: what blockchain and distributed ledger technologies mean for firms," *Business Horizons*, vol. 62, no. 3, pp. 273–281, 2019.

[31] A. Fusco, G. Dicuonzo, V. Dell'Atti, and M. Tatullo, "Blockchain in healthcare: insights on COVID-19," *International Journal of Environmental Research and Public Health*, vol. 17, no. 19, 7167 pages, 2020.

[32] M. Fang, "Comparison and selection of blockchain and traditional database technology," *China CIO News*, vol. 2, pp. 73–75, 2019.

[33] Y. C. Song and Y. Shen, "System Design for Online Foreign Language Education Based on Blockchain Technology," *Computational Intelligence and Neuroscience*, vol. 2022, Article ID 5180307, 16 pages, 2022.

[34] G. Omar, R. Giordy, P. Luis, S. Augusto, C. Marina, and W. Pedro, "HealthyBlock: blockchain-based IT architecture

for electronic medical records resilient to connectivity failures," *International Journal of Environmental Research and Public Health*, vol. 17, 2020.

[35] Q. Q. Liu and C. Xia, "Research and application of block chain in traceability of agricultural product quality," *Chinese High Technology Letters*, vol. 29, no. 3, pp. 240–248, 2019.

[36] J. N. Zhang, C. Chen, and B. Lu, "Blockchain technology improves data governance of smart city," *China Telecommunication Trade*, vol. 12, pp. 16–19, 2019.

[37] Y. X. Wu, K. Tian, X. Y. Yu, and G. L. Bai, "Dilemma and reform on collaborative governance of Chinese herbal pieces," *Chinese Traditional and Herbal Drugs*, vol. 50, no. 4, pp. 1027–1030, 2019.

[38] F. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," in *Proceedings of the 2016 13th International Conference on Service Systems and Service Management (ICSSSM)*, pp. 1–6, Kunming, China, June 2016.

[39] C. Zhang, S. Li, and J. Qu, "Safety traceability system of characteristic food based on RFID and EPC internet of things," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 15, no. 05, pp. 119–126, 2019.

[40] G. Alfian, M. Syafrudin, U. Farooq et al., "Improving efficiency of rfid-based traceability system for perishable food by utilizing iot sensors and machine learning model," *Food Control*, vol. 110, Article ID 107016, 2020.

[41] Y. Yang, J. Wang, and B. Y. Zhang, "GS1 Standard + blockchain technology helps commodity traceability," *Bar Code & Information System*, vol. 2, pp. 31–33, 2019.

[42] X. Y. Liu and X. C. Wang, "Research on the traceability system of agricultural product quality based on "internet of Things+Block chain," *Journal of Changzhou Institute of Technology*, vol. 31, no. 5, pp. 60–65, 2018.

[43] W. Long, C. H. Wu, Y. P. Tsang, and Q. Chen, "An end-to-end bidirectional authentication system for pallet pooling management through blockchain internet of things (BIoT)," *Journal of Organizational and End User Computing*, vol. 33, no. 6, pp. 1–25, 2021.

[44] Z. cYu, C. cGuo, Y. B. Xie, and D. Xue, "Research on medical anti-counterfeiting traceability system based on blockchain," *Computer Engineering and Applications*, vol. 56, no. 3, pp. 35–41, 2020.

[45] Z. Q. Shen, "Storage design of food traceability system based on blockchain," *Telecom World*, vol. 26, no. 2, pp. 304-305, 2019.

[46] I. C. Lin and T. C. Liao, "A survey of blockchain security issues and challenges," *International Journal on Network Security*, vol. 19, no. 5, pp. 653–659, 2017.

[47] R. N. Wang, M. Luo, Y. H. Wen, L. H. Wang, K. R. Choo, and D. B. He, "The Applications of Blockchain in Artificial Intelligence," *Security and Communication Networks*, vol. 2021, Article ID 6126247, 16 pages, 2021.

[48] Y. W. Chen and T. Qi, "Research on quality traceability system of rice supply chain based on blockchain Technology," *China Southern Agricultural Machinery*, vol. 51, no. 22, pp. 60–62, 2020.

[49] H. B. Zhang and H. X. Feng, "Research on the whole process traceability method of commodity based on consortium blockchain," *Modern Informationn Technology*, vol. 4, no. 1, pp. 60–62, 2020.

[50] Z. P. Feng, R. Zhang, and D. Y. Peng, "Integration of "internet +" and upgrade of Chinese materia medica industry," *Chinese Traditional and Herbal Drugs*, vol. 49, no. 24, pp. 5980–5983, 2018.

[51] W. Hong, Y. Cai, Z. Yu, and X. Yu, "An agri-product traceability system based on iot and blockchain technology," in *Proceedings of the 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*, pp. 254-255, Shenzhen, China, August 2018.

[52] Z. Hao, D. Mao, B. Zhang, M. Zuo, and Z. A. Zhao, "Novel visual analysis method of food safety risk traceability based on blockchain," *International Journal of Environmental Research and Public Health*, vol. 17, 2020.

[53] J. P. Xu, P. C. Sun, X. Zhang, X. Y. Wang, J. L. Kong, and Z. Y. Zhao, "Prototype system of information security management of cereal and oil food whole supply chain based on blockchain," *Transactions of the Chinese Society for Agricultural Machinery*, vol. 52, no. 2, pp. 341–349, 2020.

[54] Z. Kang and J. M. Sheng, "Research on the traceability path of agricultural products circulation from the perspective of Rural Revitalization -- Based on the perspective of blockchain," *China Market Marketing*, vol. 17, pp. 6–8, 2020.

[55] H. L. Yu, B. Y. Chen, D. M. Xu, X. T. Yang, and C. H. Sun, "Research on traceability information protection model of rice supply chain based on blockchain," *Transactions of the Chinese Society for Agricultural Machinery*, vol. 51, no. 8, pp. 328–335, 2020.

[56] T. Feng, X. S. Wang, C. Y. Liu, and J. L. Fang, "Secure Data Collaborative Computing Scheme Based on Blockchain," *Security And Communication Networks*, vol. 2021, Article ID 6630291, 9 pages, 2021.

[57] Y. Chen, A. Zhou, N. Xie, X. Liang, H. Wang, and Y. Shi, "An agricultural product quality safety trace-ability system based on blockchain and the internet of things," *Journal of Agricultural Big Data*, vol. 2, no. 3, pp. 61–67, 2020.

[58] X. T. Yang, M. T. Wang, D. M. Xu, N. Lu, and C. H. Sun, "Data storage and query method of agricultural products traceability information based on blockchain," *Transactions of the Chinese Society of Agricultural Engineering*, vol. 35, no. 22, pp. 323–330, 2019.

[59] M. T. Wang, "Design and Implementation of Fruits and Vegetables Agricultural Products Traceability System Based on Blockchain," *Shanghai Ocean University*, no. 2, pp. 18–23, 2021.

[60] Y. P. Tsang, C. H. Wu, W. H. Ip, and W.-L. Shiau, "Exploring the intellectual cores of the blockchain-Internet of Things (BIoT)," *Journal of Enterprise Information Management*, vol. 34, no. 5, pp. 1287–1317, 2021.

[61] P. Yang, N. Xiong, and J. Ren, "Data security and privacy protection for cloud storage: a survey," *IEEE Access*, vol. 8, Article ID 131723, 2020.

[62] W. Mao and J. Shi, "Design of supervisory system of traceable electronic scale based on blockchain technology," *Journal of Ningbo University of Technology*, vol. 32, no. 4, pp. 36–42, 2020.

[63] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: architecture, consensus, and future trends," in *Proceedings of the IEEE 6th International Congress on Big Data—Big Data Congress*, Honolulu, HI, USA, June 2017.

[64] M. Castro, B. Liskov, and B. Liskov, "Practical Byzantine fault tolerance and proactive recovery," *ACM Transactions on Computer Systems*, vol. 20, no. 4, pp. 398–461, 2002.

[65] C. Agbo, Q. Mahmoud, and J. Eklund, "Blockchain technology in healthcare: a systematic review," *Healthcare*, vol. 7, no. 2, p. 56, 2019.

[66] K. Wang, Z. Chen, and J. Xu, "Efficient traceability system for quality and safety of agricultural products based on

consortium blockchain," *Journal of Computer Applications*, vol. 39, no. 8, pp. 2438–2443, 2019.

[67] J. Wang, X. Zhang, J. P. Xu et al., "Blockchain-Based Information Supervision Model for Rice Supply Chains," *Computational Intelligence and Neuroscience*, vol. 2022, Article ID 2914571, 17 pages, 2022.

[68] L. Fan, Z. Zhang, and H. Zhao, "Research on the model of agricultural products information traceability system based on blockchain technology," *Logistics Sci-tech*, vol. 43, no. 12, pp. 11–14, 2020.

[69] Z. S. Cao, "Design and Development of Traceability Cloud Platform for Gannan Navel orange Supply Chain Based on Blockchain," *Guangdong University of Technology*, no. 3, pp. 9–11, 2022.

[70] Z. L. Zhang, "The Method and Application of Agricultural Product Information Traceability Based on Blockchain Technology," *Shenyang University*, no. 6, pp. 35–37, 2021.

[71] K. X. Guo, "Research and Improvement of Blockchain Consensus Mechanism," *Nanjing University of Posts and telecommunications*, no. 2, pp. 30–44, 2021.

[72] N. Z. Sheng, F. Li, X. F. Li, H. Zhao, and T. Zhou, "Data capitalization method based on blockchain smart contract for Internet of Things," *Journal of Zhejiang University (Science Edition)*, vol. 52, no. 11, pp. 1–10, 2018.

[73] H. B. Tang, T. Zhou, H. Zhao et al., "Archival data protection and sharing method based on blockchain," *Journal of Software*, vol. 30, no. 9, pp. 2620–2635, 2019.

[74] J. S. Gao, S. K. Li, Q. Li, Y. L. Sun, and Z. W. Yin, "The Sharing Model of Cultural Relics Information Resources in Collections Based on Blockchain," *Information Science*, 2022, https://kns.cnki.net/kcms/detail/22.1264.G2.20220407.1117.003.html.

[75] X. R. Zheng and Y. Lu, "Blockchain technology - recent research and future trend," *Enterprise Information Systems*, pp. 1–23, 2021.