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 non-tampering, 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

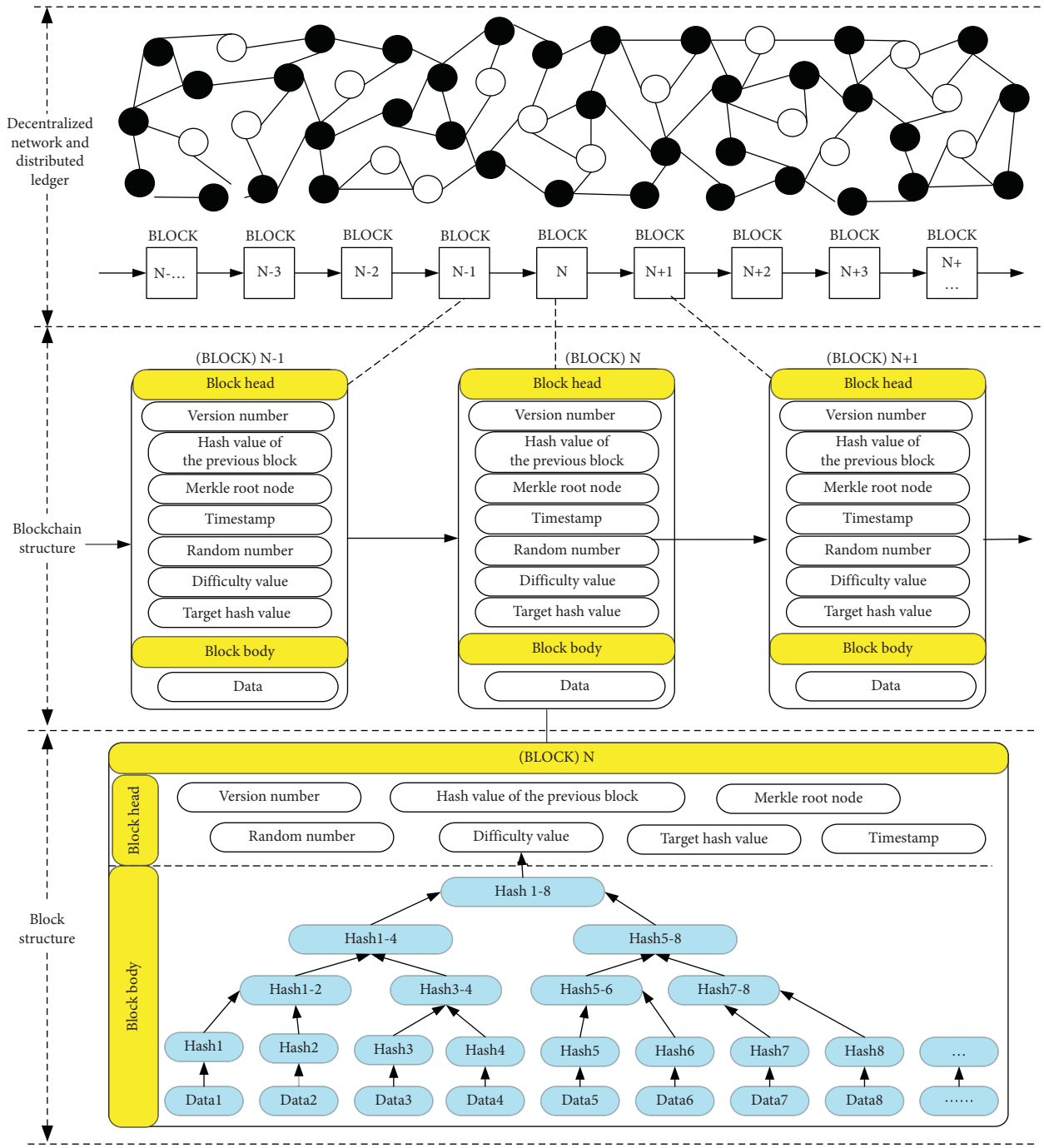

Figure 1: Technical structure of blockchain.

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.

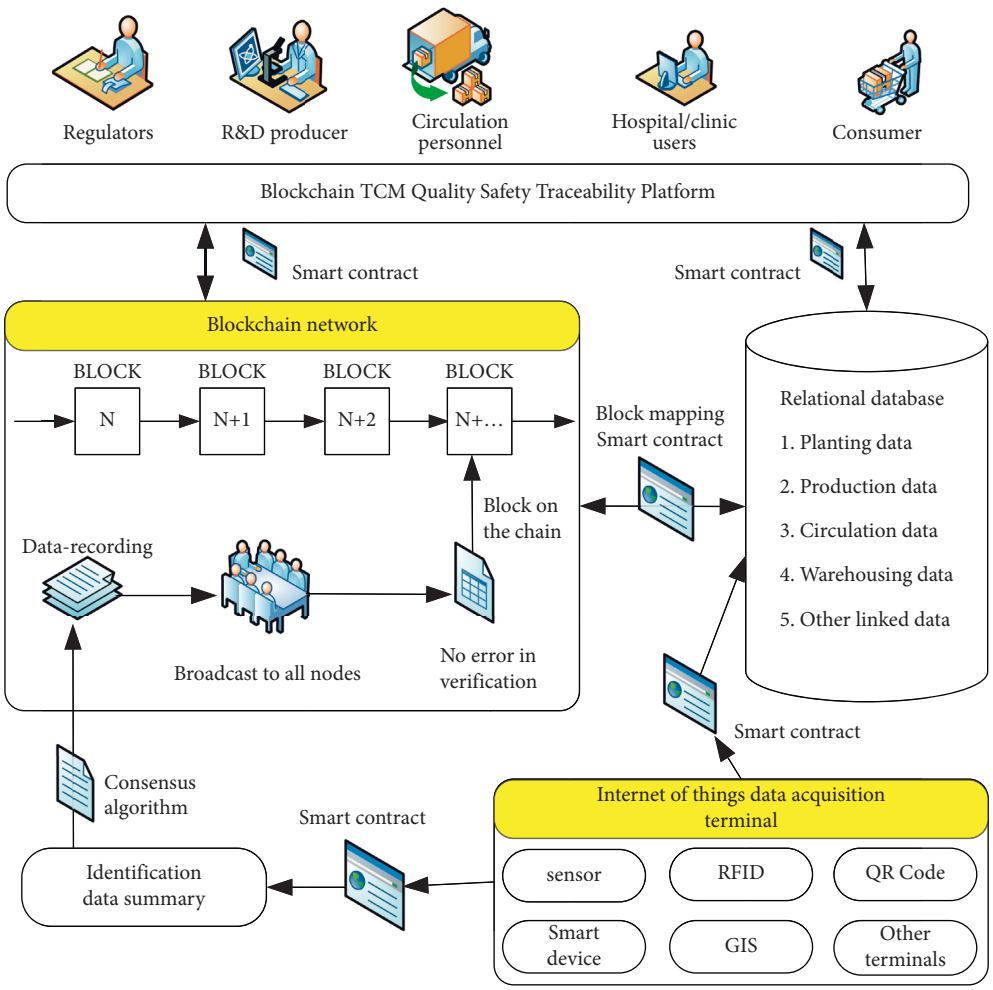

Figure 2: Technical principle of blockchain TCM quality safety traceability.

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

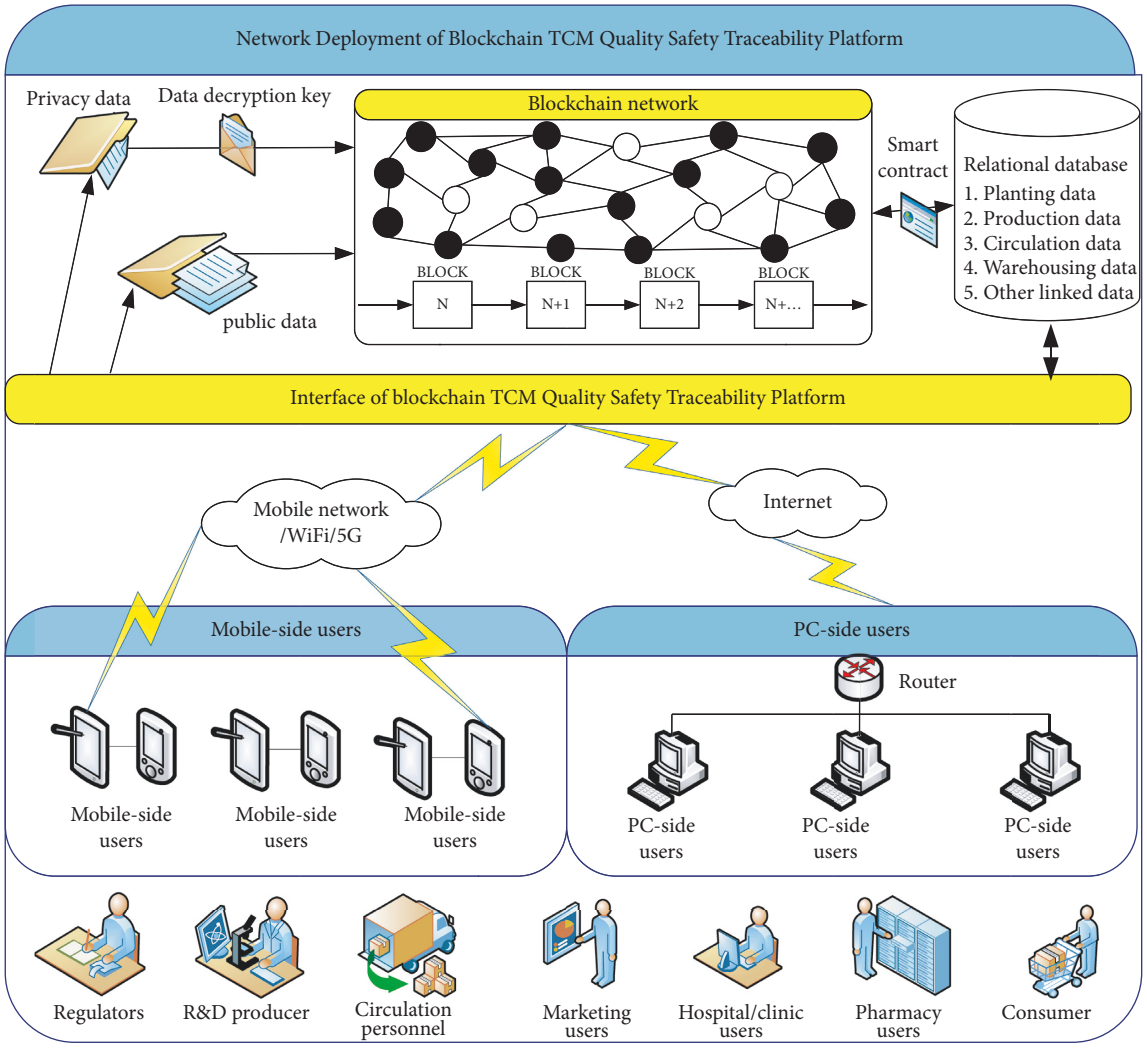

Figure 3: The network deployment of blockchain TCM quality safety traceability platform.

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

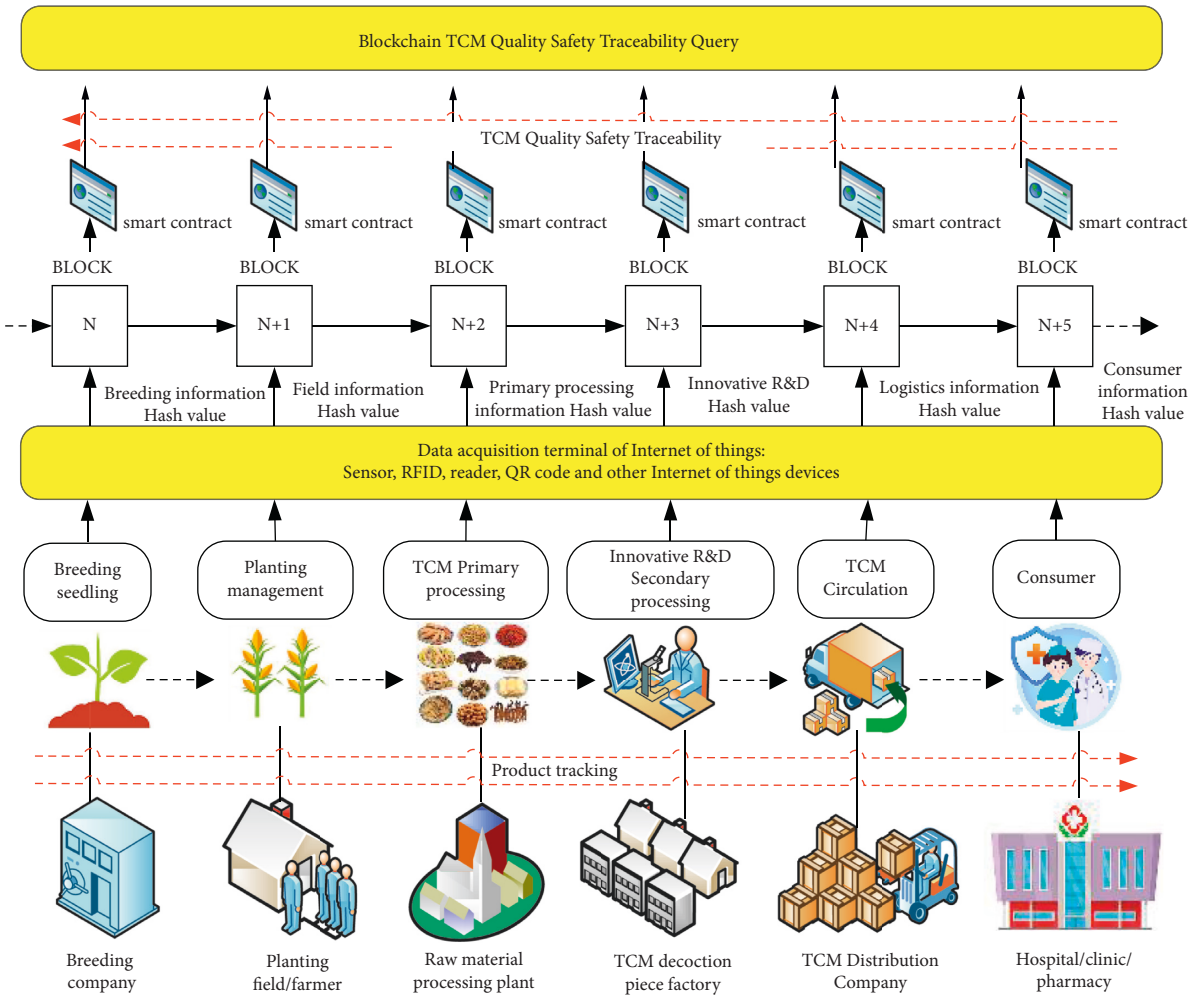

Figure 4: Business process of blockchain TCM quality safety traceability platform.

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

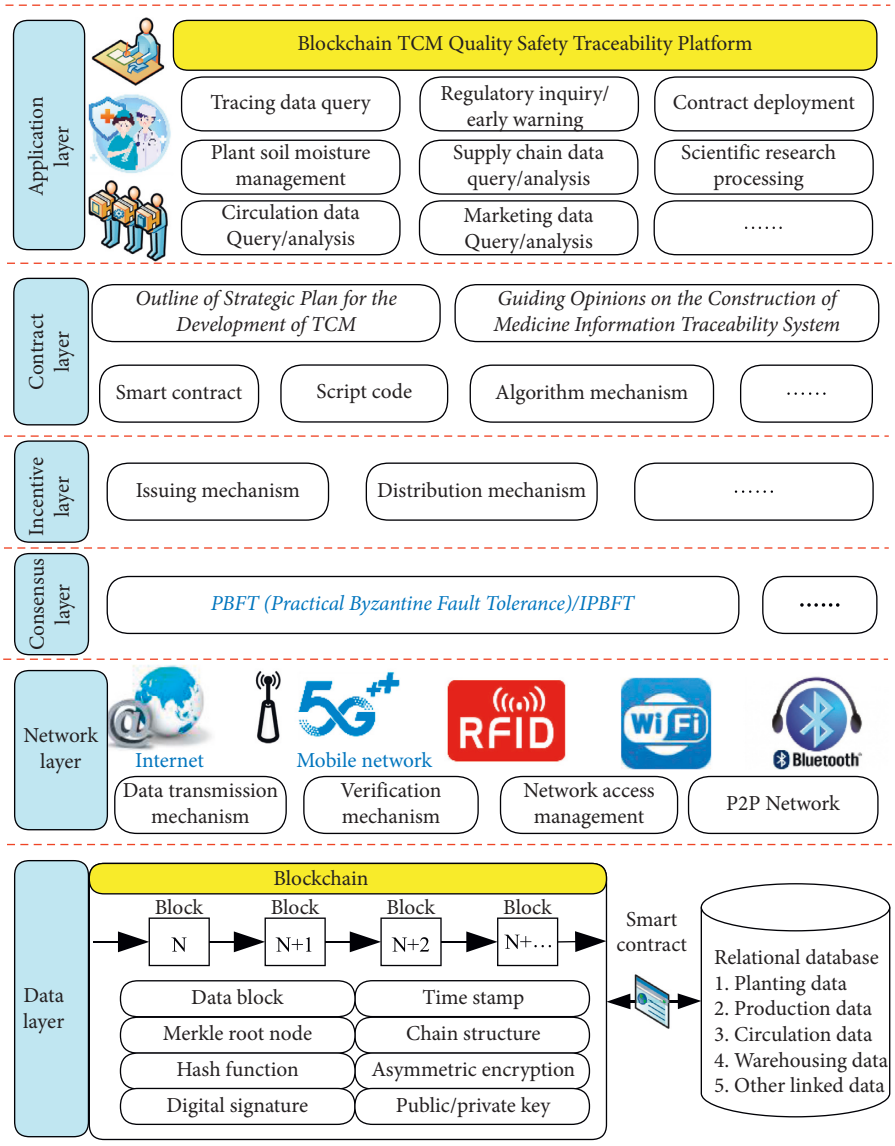

Figure 5: Layer architecture of blockchain TCM quality safety traceability platform.

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

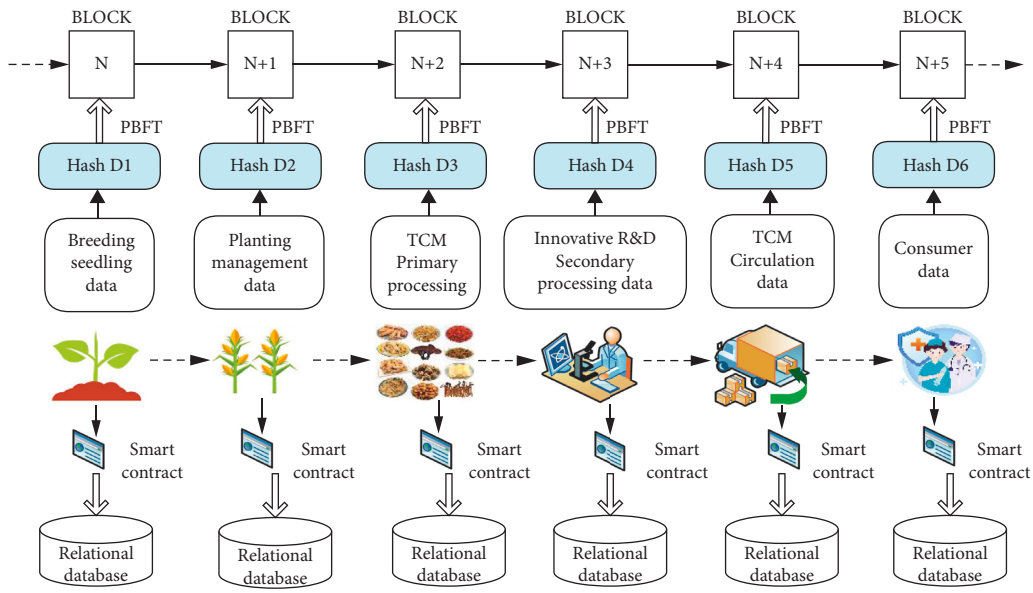

Figure 6: Data storage mode of blockchain TCM quality safety traceability platform.

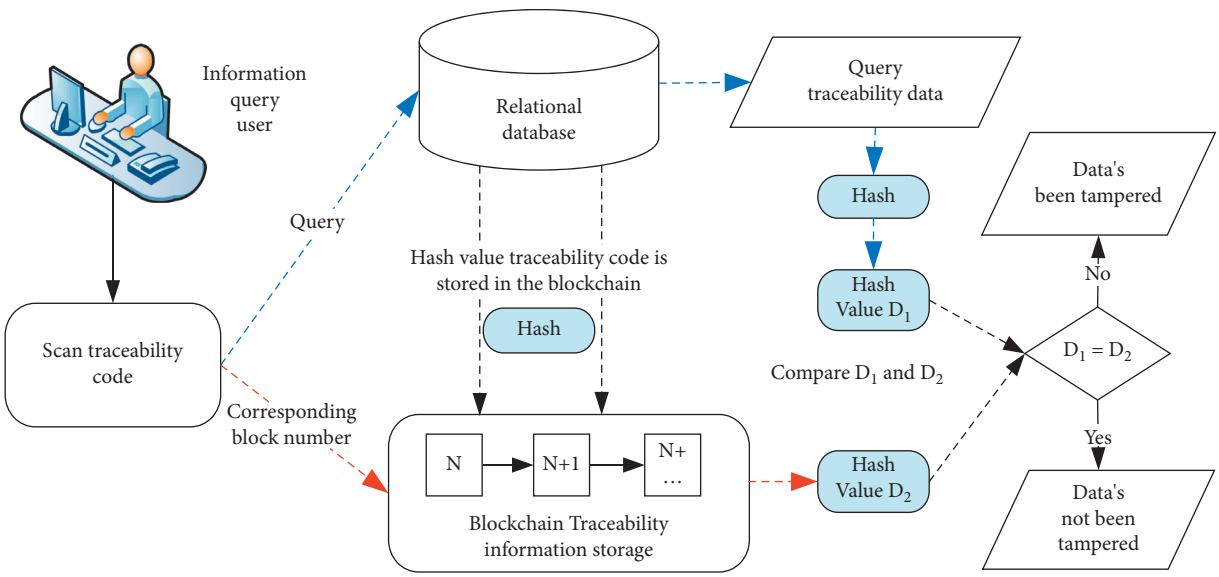

Figure 7: The query process of blockchain TCM quality safety traceability platform.

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

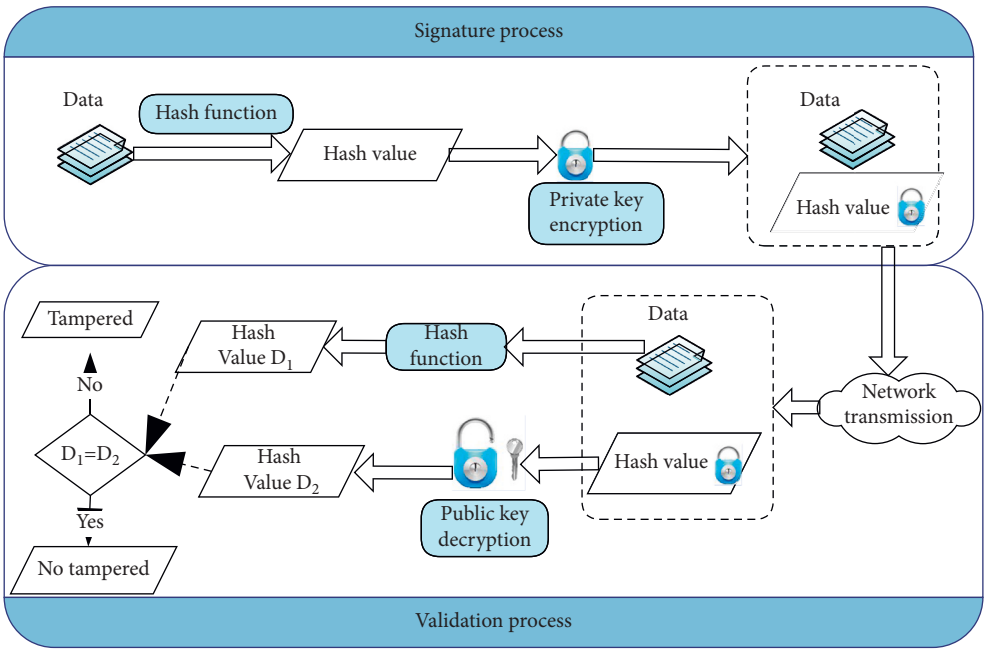

Figure 8: Digital signature process.

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).

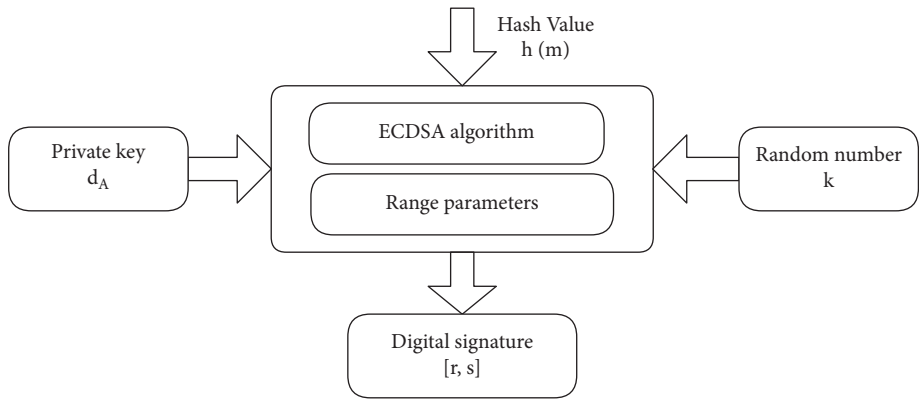

Figure 9: The process of signature calculation.

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

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.

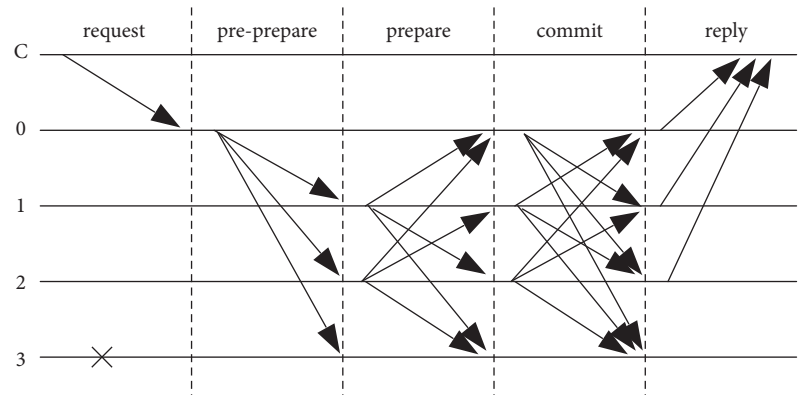

Figure 10: The transmission of PBFT algorithm.

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.

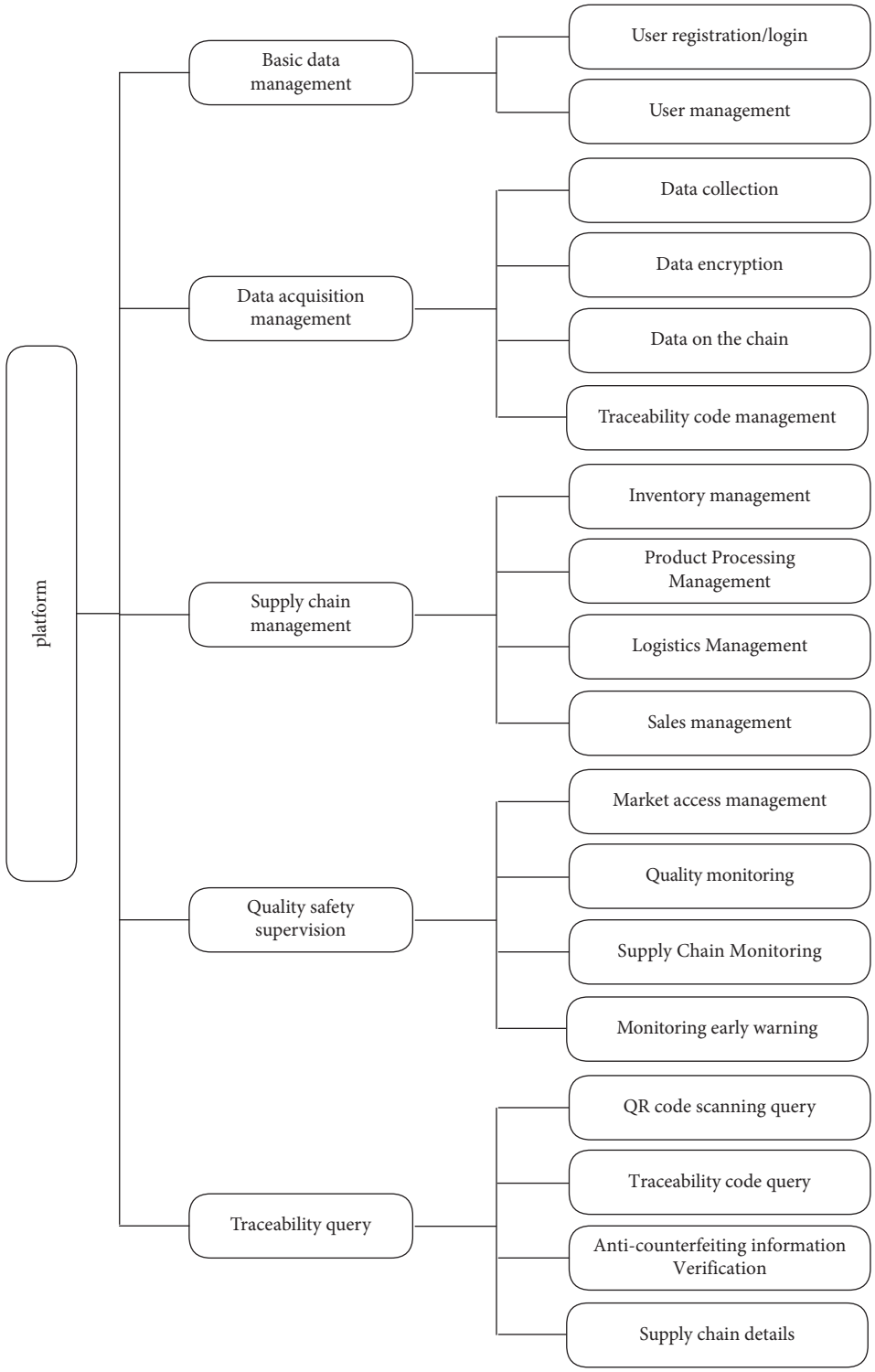

Figure 11: Functional structure of blockchain TCM quality safety traceability platform.

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

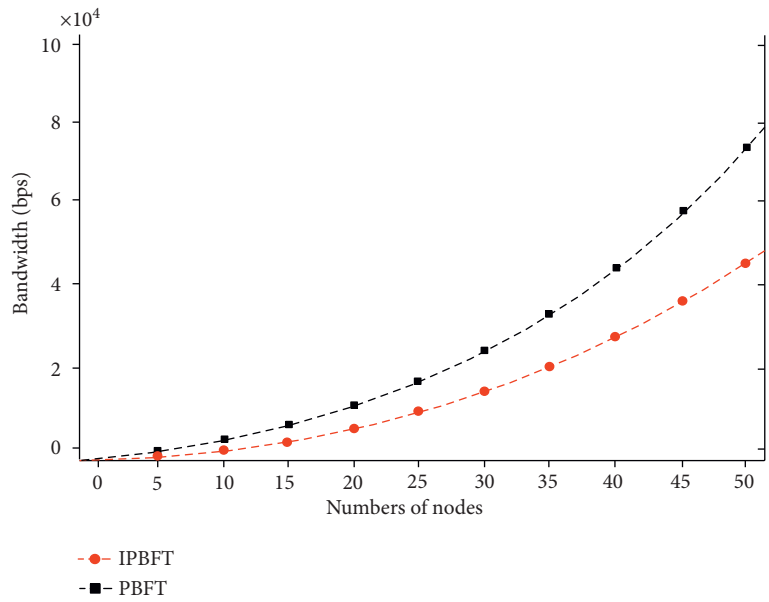

Figure 12: Comparison of network bandwidth consumed by IPBFT and PBFT consensus process.

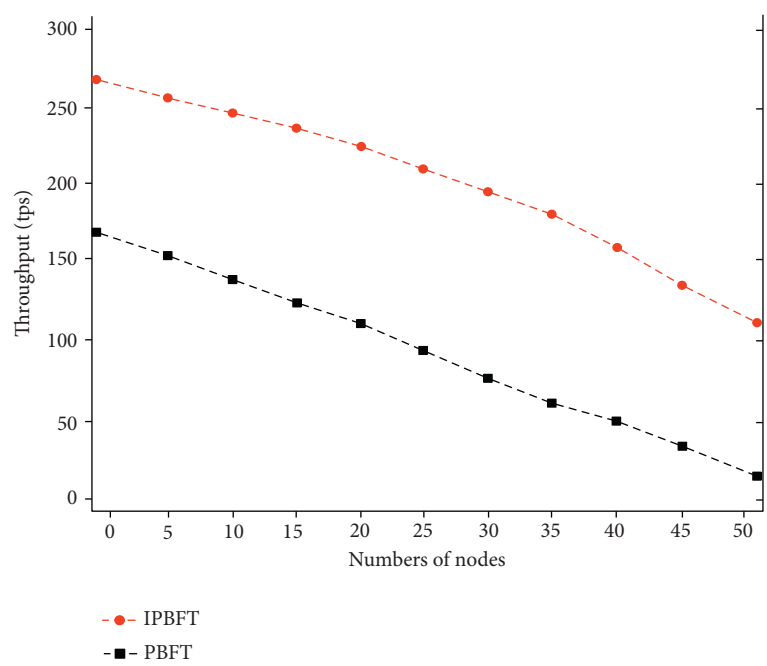

Figure 13: Comparison of throughput of IPBFT and PBFT consensus algorithms.

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.

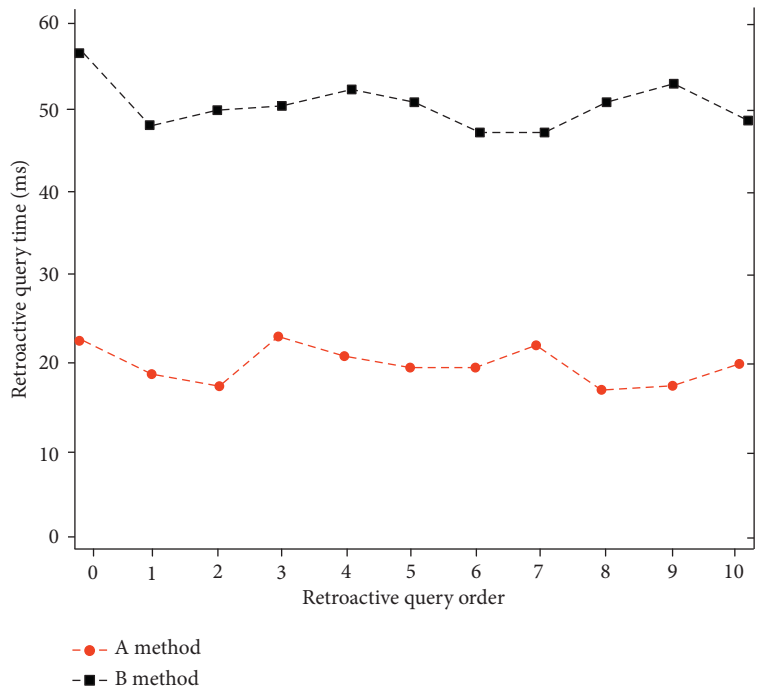

Figure 14: Comparison of the time taken to query a single traceability record in methods A and B.

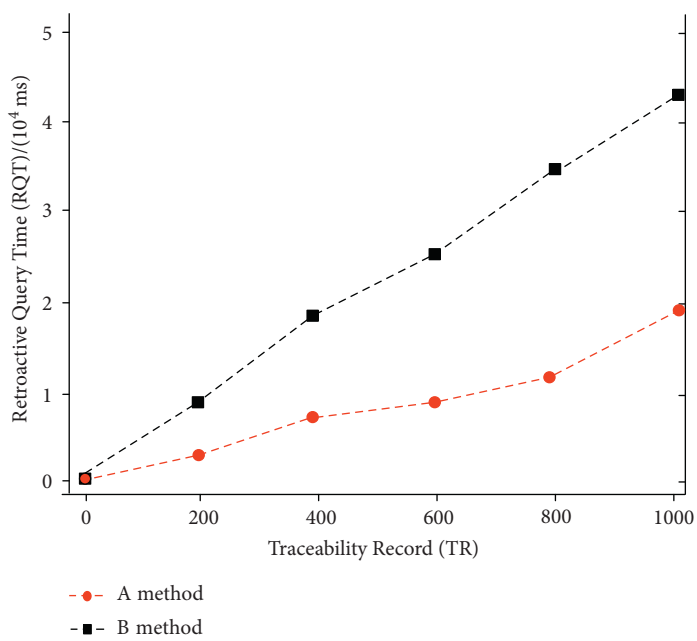

Figure 15: Comparison of tracing query time of methods A and B.

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

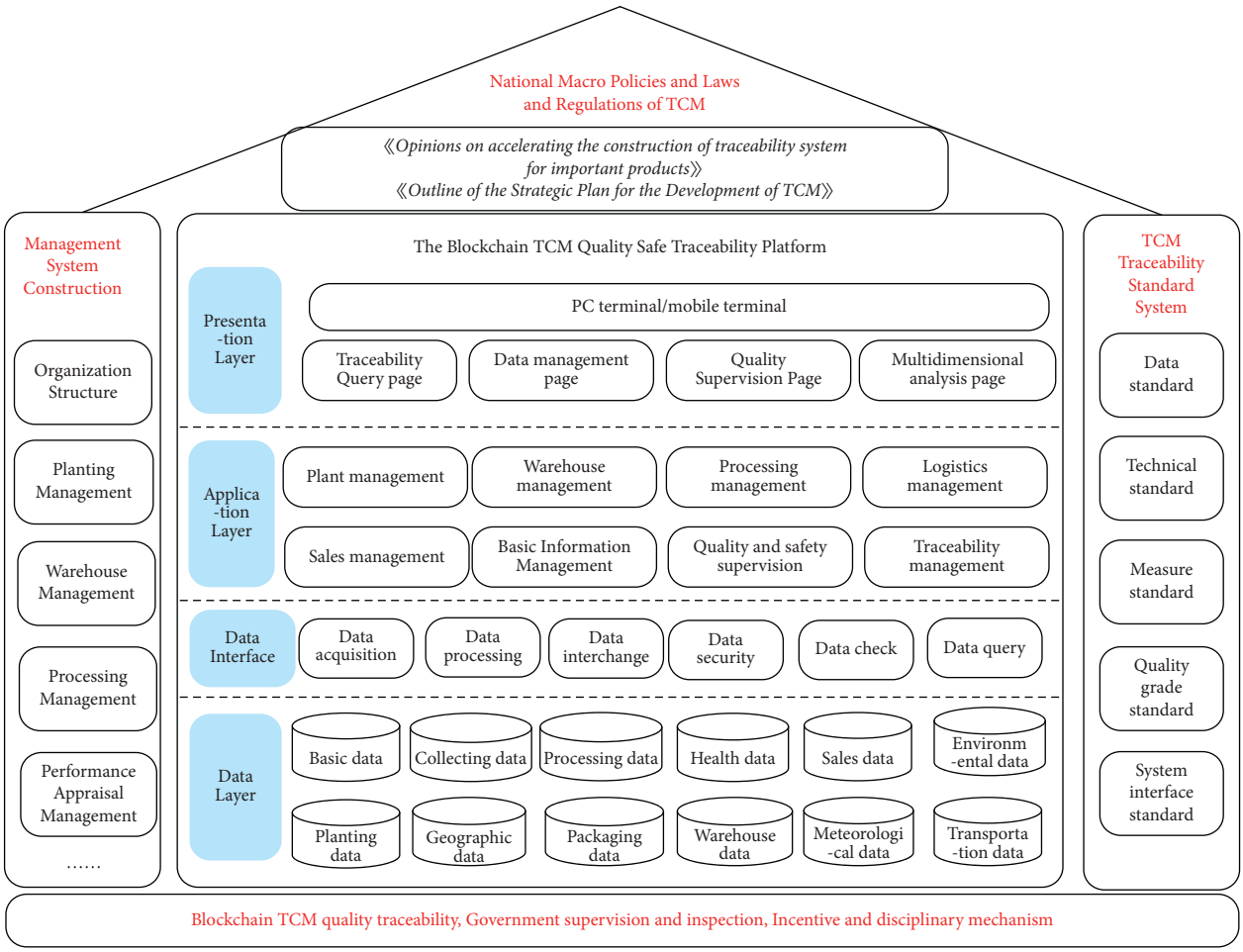

Figure 16: The blockchain TCM quality safe traceability management mode.

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.