Hindawi
Scientific Programming
Volume 2021, Article ID 1455814, 14 pages
https://doi.org/10.1155/2021/1455814

Research Article

Design and Implementation of Data Sharing Traceability System Based on Blockchain Smart Contract

Yang Kang and Qiang Li

College of Artificial Intelligence, Chongqing University of Arts and Sciences, Yongchuan 402160, Chongqing, China

Correspondence should be addressed to Qiang Li; 20160006@cqwu.edu.cn

Received 10 August 2021; Revised 10 September 2021; Accepted 16 October 2021; Published 15 November 2021

Academic Editor: Bai Yuan Ding

"Traceability" is an important method often used in modern supply management. The traceability system is a system based on the Internet of Things technology. In this process, users will share resources through cloud service providers, so how to ensure data security is also one of the issues we consider. Blockchain technology is an emerging technology in the field of information technology. Its decentralized nature, distributed storage, and difficult data modification provide us with fair exchange and sharing of data. Feasible solutions: in this article, we have studied the key issues of fair exchange and safe sharing of data based on blockchain and designed a multigroup data sharing scheme based on alliance chain. To solve the various existing traceability systems problem, this paper designs a new traceability system based on blockchain technology and implements a system prototype to verify the feasibility of the system.

1. Introduction

Imagine we went to a Chinese restaurant for dinner. The waiter led us to the self-service ordering area, there are all kinds of vegetables and meat in front of us, and there is a miniature two-dimensional code in front of these dishes. We scan the two-dimensional code through our mobile phones to obtain the production place, processing process and parameters, logistics information, and so on. This experience undoubtedly increases our dining experience. With the awareness of food safety deeply rooted in people's hearts, many agricultural products-related enterprises began to establish their own agricultural products tracking systems to help consumers track the production and processing data of agricultural products [1], enhance consumers' purchasing confidence, and enhance their own market competitiveness.

Because of its characteristics, blockchain can provide a security framework for transactions on the network [2], and it is also a trusted cryptosystem. Blockchain network system is an infrastructure, which can protect content and track network operations, so it has attracted the attention of many companies or managers. The Personal Health Record (PHR) system is problematic in some cases because it contains a large amount of private data of patients, so it is troublesome for patients to approve medical personnel to enter the system in an emergency. Therefore, the main purpose of a health care management framework based on blockchain technology is tamper protection. In view of the lack of product data sharing, fake and shoddy goods will flood, and how to prevent them has become an important issue [3]. How to use blockchain technology to share product data end-to-end in cross-border environment is to use a structure to track the process of manufacturing goods and prevent counterfeit goods. Although data sharing is practical. Researchers put forward a new CP-ABE scheme with multiauthority and large universe, which is the sharing of multigroup fine-grained data in the cloud Internet of Things system based on blockchain, which can ensure the integrity of data, introduce public audit, and realize tracking [4]. Experiments show that the scheme can be used in large-scale Internet of Things systems in terms of security analysis. Ground rescue needs data transmission support to be efficient and safe. Unmanned Aerial Vehicle (UAV) can perform urgent rescue tasks and share data with the ground, which also involves a

network, unreliable behavior tracking, and so on, which makes the data sharing between vehicles and UAVs pose a security threat [5]. To solve this problem, a lightweight vehicle blockchain-supported secure (LVBS) data-sharing framework is proposed, which not only improves the security but also optimizes the quality of data sharing strategies. In the process of placing orders and arriving goods in online shopping, goods are often exchanged for no reason. Therefore, we propose a decentralized database that can be maintained collectively by using the high reliability and high confidentiality of blockchain, which provides a way for logistics confidentiality and produces a modern logistics environment [6]. An intelligent antiswitching package for logistics system traceability based on blockchain is proposed. Its function is to enable customers to track their location, temperature, and humidity at any time, thus realizing intelligent logistics. Alliance blockchain technology is a multigroup data sharing scheme based on blockchain [7], which enables users to verify each other whether the shared data is valid without a third party. Some existing schemes cannot realize data sharing among different users, and then this scheme solves the problem of data sharing among different groups and has security and reliability. Combined with this epidemic, the potential application and opportunities of epidemic data deposition and sharing are combined to fight against novel coronavirus pneumonia epidemic, and the potential application of blockchain in this area is found. The advantage of blockchain is that it can provide high performance and security for the stored data and can be accessed globally so that the stored related medical data can be shared [8]. Blockchain data sharing is one of the most influential and practical methods available for health care data management. The medical data sharing and privacy protection eHealth system based on blockchain, namely, SpChain [9], has higher security and higher data retrieval rate in EMR sharing and management scheme than the traditional eHealth system based on blockchain. In addition, key blocks and micro blocks are established to store EMRS of patients.

However, these agricultural product traceability systems also have shortcomings, mainly including the following problems:

(1) Low data security:

Traditional agricultural products traceability system mostly adopts B/S design mode; resources are concentrated in a certain institution or organization; system centralization is serious; and data is easy to be tampered with, resulting in low data security.

(2) Low trustworthiness:

Because each node of the agricultural products supply chain is independent, it is easy to produce information gap and form information island, and the trust between them is greatly reduced.

(3) It is difficult to obtain source data:

The core of the agricultural product traceability system is data, which comes from every link of the agricultural product circulation process. Under the traditional supply chain mode, there are no clear requirements and regulations for the participants in the supply chain, leading to great differences among the participants, unbalanced distribution of resources and technologies, unified management standards among each link, and lack of some key technologies, which make it difficult to collect data and information of agricultural products source.

2. Characteristics of Blockchain Technology and Introduction of Related Technologies

Blockchain is a way to organize data skillfully, while blockchain technology [10] is a technology that integrates many outstanding achievements of human intelligence, including database technology and network technology related to distributed books, network technology related to consensus algorithm, and asymmetric encryption technology and software technology related to intelligent contracts. Blockchain technology, which integrates these cutting-edge technologies, has challenged and confronted the mechanism based on central node credit since it was put forward. With the development of time, this characteristic of blockchain technology is becoming more and more obvious, which makes it no longer limited to digital cryptocurrency [11], but widely used in many fields of social and economic life, such as supply chain finance, data authentication, asset management, election voting, and fair security traceability introduced in this paper. Nowadays, blockchain technology has become an important technology that cannot be ignored among many high-end cutting-edge technologies.

2.1. Distributed Book. Unlike the traditional system network structure, the network architecture and data storage of the blockchain system choose distributed books with a decentralized architecture. The transmission of information in the network does not pass through the central node, and each member node retains complete data, which is embodied in the distribution of nodes in entity and the distribution of nonrelational databases on each node in logic. Account book is a storage form of data and a management unit of data. Nonrelational database is the logical carrier of data and account book, and the physical carrier of data and account book is the member node. Blockchain is the underlying form of an account book, that is, the data form of a chain of blocks strung together. After the consensus process, members will reach a consensus and write the same data into the blockchain system, so each member keeps a copy of the data. Because the data in each ledger cannot be deleted, the total amount of data will only increase, which is a great test for the ability of data storage. Still, with the rapid development of technology, this will not be a problem. The breeding nodes, slaughtering nodes, processing nodes, transportation nodes, and sales nodes in the livestock products supply chain are distributed in different places in the physical sense, in line with the distributed ledger technology in the blockchain. In the ideal traceability model, the status of nodes where each link is located is expected to be equal, the information flow

does not pass through the central node, and its network architecture naturally fits the characteristics of distributed books in blockchain technology, so it is reasonable and efficient for livestock products traceability system to select the network architecture based on blockchain technology.

2.2. Cryptographic Algorithm. Cryptography is the core of the blockchain data layer, which escorts the whole data transmission and access of blockchain. Cryptographic algorithms will be used in three places in the blockchain platform of cold chain drug traceability, including hash algorithm and asymmetric encryption algorithm. This section will discuss the principle and selection of these two algorithms.

2.2.1. Hash Algorithm. The secure hash algorithm is an alias of the hash algorithm that maps data of arbitrary length into hash strings of fixed length through certain rules. The more common ones are SHA-256, SHA-384, SHA-512, and so on, which are widely used in various technologies requiring encryption, including blockchain technology [12].

2.2.2. Asymmetric Encryption Algorithm. Asymmetric encryption algorithm comes from the secret way of the key in the cryptographic algorithm. The key consists of a public key and a private key. The keys are generated at the same time, in which the public key is public as its name implies, while the private key is private and needs to be saved by itself. When encryption is needed, one of the same pairs of keys is used to complete the encryption operation, and only the other key can complete the decryption of the message. Asymmetric encryption algorithm plays an important role in blockchain and is the cornerstone of the security of the whole blockchain system. The asymmetric encryption algorithm is mainly used in encrypted communication and digital signature in blockchain [13].

2.3. SM2 Digital Signature Algorithm. SM2 algorithm is an improved national cryptographic algorithm based on ECC published in China in 2010, which includes digital signature algorithm, key exchange protocol, and public key encryption algorithm. It has become the current public key algorithm standard GM/T 0003.2-2012 in China and entered the international standard ISO/IEC14888-3.

2.3.1. Principle of SM2 Digital Signature Algorithm. The elliptic curve equation E, (A, B) selected by the SM2 algorithm is as follows:

$$y^2 = x^3 + ax + b. \tag{1}$$

The Abelian group $(G, +)$ is defined on Ep (a, b), where the unit element O of the group is defined as an infinity point. Let the elliptic curve be $y^2 = x^3 - x$. Take two points P and Q on the elliptic curve $(G, +)$ arbitrarily, make a straight line intersecting the other point R' of the elliptic curve, make a parallel line of y-axis intersecting R through R′, and define $P + Q = R$. In this way, the sum of the additions made by two points on the Abelian group will also be on the elliptic curve and also satisfy the properties of the Abelian group. When the same points P are added, that is, when the two points P and Q coincide, the tangent of the point P is made. Repeat the above operation, and when k points P are added, it is recorded as k_P.

Ordinary elliptic curves are continuous and not suitable for encryption. In the national standard, the elliptic curves with 256 bits in prime number field are used to transform the elliptic curves into discrete points. Let the prime number be P, the prime number field formed by the elliptic curves Fp, and the elliptic equation Erp (a, b):

$$y^2 = x^3 + ax + b (\mathrm{mod}\ p), \tag{2}$$

where a and b are elements in the prime field and satisfy $4a^3 + 27b^2 \neq 0 \ (\mathrm{mod}\ P)$. SM2 can be encrypted by assuming that, in the elliptic curve $P = d_G$, where P and G are two points on Ep (a, b), n is the order of G $(nG = O\ \infty)$, and d is an integer and its value is not higher than order n. Given D and G, it is easy to compute P in the front direction but difficult to compute D in the reverse, according to the definition of Abelian group addition rule. Let the set $\{O, G, 2G, 3G, (n-1)\ G\}$ be a cyclic subgroup generated by G on E: (a, b). If d is selected as the private key and $P = dG$ as the public key, the problem of finding d from P is the discrete logarithm problem (ECDLP) on elliptic curve group, which is the mathematical basis of elliptic curve encryption algorithm [14].

2.3.2. SM2 Digital Signature Scheme. The digital signature scheme designed by SM2 encryption principle is as follows: key generation: input SM2 elliptic curve parameter *parms* (elliptic curve equation Ep, large prime number p, base point G, order n of base point); the private key d is randomly generated and kept secret, and the public key is generated by using the relationship between public and private keys:

$$P = [d]G. \tag{3}$$

In the formula, P is the obtained SM2 public key, which is an important basis for SM2 to be used in encryption and signature. SM2 signature process: input SM2 elliptic curve parameter *parms*, private key d, and message M to be signed, and calculate hash value Z_A at the same time:

$$Z_A = H_{256}(I\ DL_A \,||\, ID_A||a||b||x_G||y_G||x_A||y_A). \tag{4}$$

ID_A is the user's distinguishable identification, IDL_A is the length of ID_A, a and b are the coefficients of elliptic curve, x_G and y_G are the horizontal and vertical coordinates of base point G, respectively, and $x_A||y_A$ is the horizontal and vertical coordinates of public key, respectively.

The hash value Z_A is obtained, and then the hash digest e with the message M to be signed is calculated:

$$e = H_{256}(Z_A||M). \tag{5}$$

Randomly generate $k \in [1, n-1]$ and calculate the elliptic curve point $X1$ from it:

$$X_1 = (x_1, y_1) = [k]G. \tag{6}$$

Calculate the signature parameters r and s to output the signature (r, s):

$$\begin{aligned} r &= (e + x_1) \bmod n, \\ s &= \left((1 + d)^{-1} (k - rd) \right) \bmod n. \end{aligned} \tag{7}$$

SM2 verification process: input *parms*, the public key P owned by the verifier, the message M to be verified, and the signature (R'', S') sent by the signer to obtain the hash digest E of the message M to be verified according to formula (5), and calculate the T value:

$$t = (r' + s') \bmod n. \tag{8}$$

Verify whether t is equal to zero. If it is equal to zero, the verification fails; otherwise, calculate the elliptic curve point $X'1$:

$$X_1' = (x_1, y_1) = [s']G + [r']P_A. \tag{9}$$

Verify whether r' = (e' + $x1'$) mode is true. If it is true, the verification is successful.

2.4. Consensus Algorithm. At present, the consensus algorithms commonly used in blockchain are Pow, Pos, DPos, and PBFT. Pow uses the workload proof mechanism to determine the node accounting right and ensures the consistency of data through a large number of calculations. Pos adds the concept of currency age to the workload proof mechanism and uses currency age instead of computing power to reduce the difficulty of block solution. DPOS uses digital cash holders to generate node sets with bookkeeping rights through elections and adopts rotation bookkeeping to generate blocks. PBFT is a distributed consensus algorithm based on state machine replication. Consensus is completed through three-stage communication between nodes. For the four consensus mechanisms in throughput, the performance of delay and scalability is compared. The application of the consensus mechanism in blockchain ranges from PoW to PoS and then to DPOS and PBFT. In this process, computing power competition is gradually replaced by equity competition. The cost of obtaining node bookkeeping rights is gradually reduced. With the development of the blockchain application, the transaction speed gradually increases. At the same time, the consensus mechanism has gradually evolved from the initial decentralization to the current weak centralization. Each consensus mechanism has different advantages and disadvantages. PoW can realize decentralization to the greatest extent, with safe, reliable, and low consumption of network resources. Still, it consumes too much computing resources. The computational attack is easy to occur, and the consensus time is longer. The emergence of PoS solves the problem of excessive waste of PoW computing power, but it makes the pressure of network traffic increase. The implementation is more complicated. DPOS has made appropriate compromises on centralization. The consumption of network resources is reduced, the consensus time is greatly shortened, and the system throughput is improved. However, due to its weak centralization, the security is reduced, which is prone to security loopholes. The PBFT algorithm solves the problem of a distributed system with Byzantine error nodes and improves the fault tolerance rate of the distributed system. However, due to the existence of a large number of point-to-point communications, it occupies a large number of communication resources [15].

2.5. Smart Contracts. More than ten years before blockchain technology was proposed, the idea of smart contract existed. However, because there was no corresponding underlying technical support at that time, it had been unknown until the blockchain developed into the 2.0 era. Combining intelligent contract with virtual digital cash technology becomes an important part of programmable blockchain technology [16, 17]. Intelligent words in intelligent contracts reflect their ability to judge and execute independently; the word contract shows that it needs certain rules, just like contracts, as the standard of independent judgment. When intelligent contracts judge that a certain behavior conforms to this rule, they will perform corresponding operations accordingly. Self-judgment is the task that computer programming language is good at accomplishing, and self-execution is also well realized by programming language. Because the intelligent contract takes the programming language as the carrier, that is to say, it is a written program in practical application, whether the data triggers its conditions and executes corresponding behaviors is completely determined by the machine, and human intervention is impossible. This is very consistent with the design purpose of blockchain technology to ensure that data cannot be tampered with artificially. After the intelligent contract is integrated into the blockchain technology, all kinds of business can be written into it to judge and execute spontaneously, which greatly reduces the influence of human factors, improves the credibility of transaction data, and makes the blockchain technology not limited to the currency circulation field but gradually integrated into many other leading cities in social and economic life.

3. The Basic Principle of Blockchain Uses Double-Chain Traceability System Design

3.1. Design of Traceability System

3.1.1. System Requirements Analysis. This paper describes the traceability of information in the traditional blockchain production process and eliminates the risk of information tampering in the blockchain production process. Using the decentralized characteristics of blockchain, a decentralized traceability system is constructed.

Simply using an existing high-reliability public chain or a license chain maintained by multiple system participants as a carrier for storing traceability information has drawbacks. It will multiply the cost, and the processing speed will be slow. Storing traceability information in the license chain can

better solve the cost and speed problems. However, storage in the license chain faces the risk of small nodes and easy attack. This requires a much cost to solve the security problem. The public blockchain has the advantage of reliability, but it needs to invest many computing resources. Therefore, this paper will design a traceability scheme combining double chain, public chain, and license chain. The traceability system needs to be able to locate the responsible person; that is, it needs to be able to find the input person of each traceability information. In the traceability system described in this paper, the traceability information is entered by publishing the traceability information of transaction records and storing the traceability information in the blockchain using one's own account. Because publishing transactions in the blockchain requires an account signature, in the license chain, you only need to find the account that published the traceability record to know who has entered the traceability information into the traceability system; that is, the traceability system described in this paper has the function of locating the responsible person.

3.1.2. Overall Design. In the traceability system designed in this paper, the blockchain operated by nodes related to the traceability system is used to store the product traceability records recorded by each traceability node. In order to enable the traceability system to process a large amount of traceability information, a license chain is used to store traceability information in the traceability system described herein. In order to improve the security of the above license chain, license chain block authentication information must be stored in the public chain to check whether the data in the license chain has changed. Universal chains use highly reliable chains, such as Ethereum and Bitcoin. The overall design of the traceability system is shown in Figure 1.

As shown in Figure 1, each node of the source nodes sequentially adds source information to the authorization chain. Hashes of blocks of several license chains are stored in a database in the form of a Merkel tree, the roots of which are stored in the public chain. How the license chain stores traceability information will be described in detail later.

Figure 1 shows that the manufacturer can generate labels for each product. The user can find the location of the product corresponding to the last trace information through the tag, and the trace information can find the faster source information in the license chain. For each source information stored in the license chain, the user can obtain a block title corresponding to the license chain and can verify whether the source information is actually stored in the license chain by Merkel authentication. For a block title in the license chain, the user can compare the block title with the information stored in the shared chain and use Merkel to verify whether the block has been tampered with.

3.1.3. License Chain Design. In the source tracking system described herein, source information is stored in the license chain through transactions. In the source tracking system described herein, source information is stored in the form shown in Table 1. Trace information includes information recorded at a trace node and the transaction number for which the previous trace information is recorded in the license chain. In addition to the above information, the traceability information will also include the signature of the person in charge and the information of the person in charge holding the public key for locating the relevant person in charge.

In this tracking system, the person entering the source information has an account of the license chain. The inputs of the source information start the transaction, which is all through the traceability information recorded in the account. So, the account signature must be used at the beginning of the transaction. At the beginning of the transaction, the mining node of the license chain will verify and protect the legitimacy of the transaction. In the license chain, as long as the account of the transaction with additional record tracking information is found, it can be determined that the recorder of the transaction information is responsible for positioning. The MPT tree stores the correspondence between the product number and the last transaction tracked by the product. This tree is similar to the Ethereum state tree. Each worksheet node records the status of each product, including transaction numbers and book labels. Actions that record the latest product tracking information can be found in the license chain through transaction numbers. Operations that record information from other sources can be found through transactions. Bookmarks are used to prevent labels from being copied. Bookmarks are initialized to false. If the product has been tracked and questioned, its value should be changed. If the value is true, the information stored in the corresponding form node will not change. In this way, consumers who have restored the origin information of the product know that the product has been restored.

3.1.4. Public Chain Design. This paper discusses two methods of storing hash validation of license chain blocks in the public chain.

(1) In the open chain, a hash transaction storing the title of the license chain block is published.

(2) The smart contract expanded in the public chain stores the hash of the license chain block according to this contract.

In this paper, Scenario 2 hopes that, by expanding the intelligent contract on the open blockchain, anyone can observe the logic of the contract and the hash verification of each block of the license chain stored in the contract. If a transaction for a burst column storing a license key block is started directly in the shared chain, other systems need to provide a method of finding a transaction storing a hash of the corresponding block in the shared chain. However, for a blockchain such as Ethereum, the cost of Scheme 2 is too high. The license chain generates a transaction that calls the smart contract every 10 seconds, starts the transaction at the public chain store every 10 seconds, and calls the saved source information of the smart contract. After reducing the occurrence speed of license blocks, the response speed of stored information of the source system will slow down. That

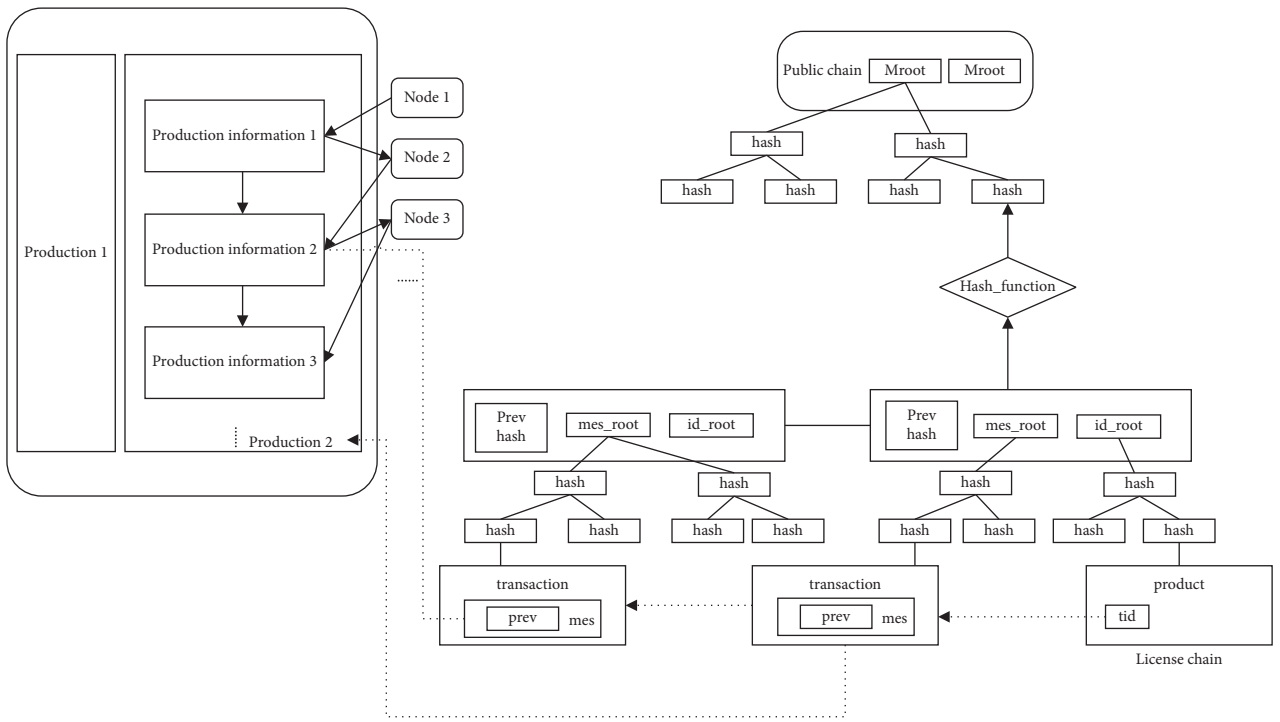

Figure 1: Overall design drawing of the traceability system.

Table 1: Storage structure of traceability records.

Traceability information
Production information
Signature of the relevant responsible person on production information
Record the transaction number of the previous traceability information

is, the source node can store the source information in the tracking system for a long time after starting the tracking information request.

In order to ensure the response speed of the information stored in the tracking system and reduce the cost, the source tracking system in this paper forms a lava tree from several blocks of continuous authorization chains and stores the roots of this lava in the public chain. When verifying whether the block has been tampered with, the block's validity is verified by using the Merkel tree [18] to which the Merkel verification block belongs. In the license chain, the block head acts as the leaf nodes of two Merkel trees, which is used to verify whether a block in the license chain has been tampered with. The block needs to extract all nodes and their siblings on the root node path from the leaf nodes of the corresponding Merkel tree and its leaf nodes. Then, verify that the hash values stored by these nodes in the parent node are all child node information and hash values. If the above conditions are satisfied and Merkel's root coincides with Merkel's root stored in the shared chain, the block corresponding to the permission chain is considered not to have been tampered with. As shown in Figure 2, to verify node a, it is necessary to verify the accuracy of the following formulas:

$$H_c = H(H_B + H_A), \tag{10}$$

$$H_B = H(H_D + H_C), \tag{11}$$

$$H_G = H(H_F + H_E), \tag{12}$$

3.1.5. Entry and Query System Requirements. In the source tracing system described in this article, desktop software is used to enter tracing information. The operation method is that the operator fills in the trace information or selects trace information from the drop-down menu. Then, the QR code recording the source information of the commodity is scanned, and the source information of the commodity is recorded in the tracking system. The specific implementation is described in the next chapter. For the search system, users can query the specific tracking information of products through the Internet.

3.2. Realization of Traceability Prototype System

3.2.1. Implementation of License Chain. Because the amount of complete and used blockchain is too large, in this paper, we build a blockchain that takes Taifang's private chain as a prototype system to store tracking information. This paper will implement and verify the license chain P2P network [19] and consistency algorithm designed [20]. The license chain of the prototype system is shown in Figure 3.

In the prototype system, to save the space of the private chain of Ethernet Square, the tracking information is stored in the coupon chain by using summary information, which

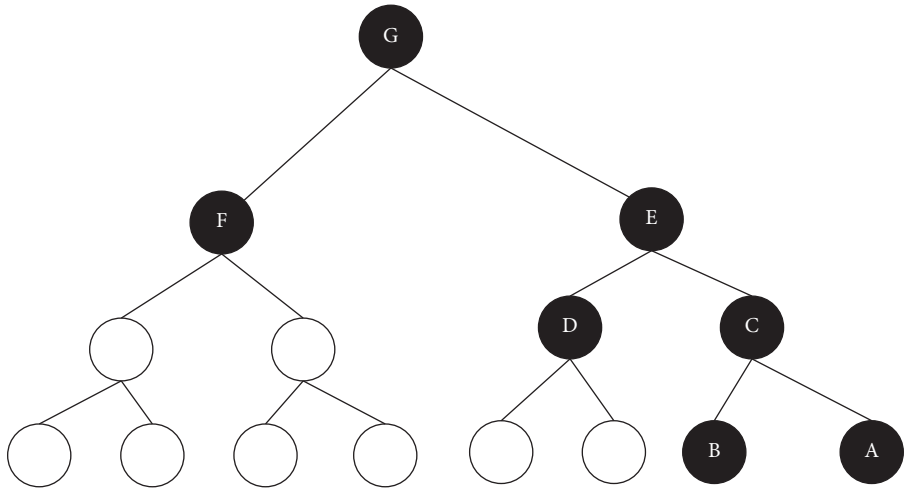

Figure 2: Merkel verification.

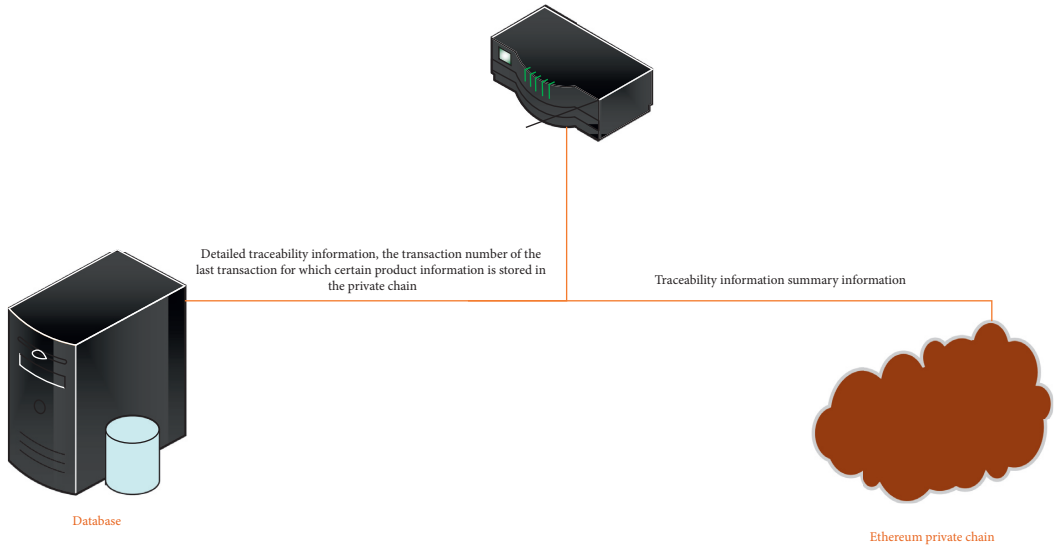

Figure 3: License chain in the prototype system.

includes hash containing source information and link of source information to the database. Detailed source information obtains the above link in the database and stores the detailed source information in a hash value in an Ethernet private chain for verifying the authenticity of the source information stored in the database. The key value of the link value is stored in the database. Here, link represents the detailed source information link, and value represents the detailed source information, both using MySQL VARCHAR type.

3.2.2. Realization of Public Chain. The source tracing system [21] in this paper is to organize the blocks of the permission chain into the form of tag tree and store each private chain block in the Merkel tree with $2n-1$ nodes (including 2 $(n-1)$ leaf nodes). In the Merkel tree described above, each leaf node stores a hash value of one block of the permission chain, and the root node of the Merkel tree is stored in the public chain. The license chain block header is continuously located in the database, which is in the form of key value, and the key value is the node number and the hash value of the value node. For each Merkel tree, assuming that the starting number of Merkel tree is start, the leaf node number of recording the first hash is start $+2n-1$, and then the cut-off hash leaf nodes allowed to be stored are added to the Merkel tree according to the increasing order of leaf node number. In the lava tree described in this chapter, the parent node number of n nodes is $(\text{start}+n)/2$, the sibling node number is $n+1-2*(n\%\ 2)$, and the parent node stores the hash value of all the child nodes. If each Merkel tree has $2N$ leaf nodes, the block of block number N calculates the start (start position) corresponding to the Merkel tree using the following, where int0 represents a downward modification:

$$\text{start} = \text{int}\left(\frac{n}{2^n}\right) * 2^{n+1} + 1. \tag{13}$$

The label key corresponding to the leaf node can also be obtained from

$$\text{key} = \text{start} + 2^n - 1. \quad (14)$$

In the prototype system, Ethernet Square [22] is adopted as a shared chain, and the intelligent contract deployed in Ethernet Square is used to access data. Smart contracts use solity to store the root node of each Merkel. The above contract only allows a specific account to perform storage operations and prohibits changes to data stored in mapping. If each Merkel tree has $2n$ leaf nodes, the block with block number n corresponds to the Merkel tree number: int $(n/2n)$.

3.2.3. Double-Stranded Interaction. In this paper, when investigating trace information. The background will confirm whether the block holding trace information in the verification license chain has been tampered with.

Merkel's verification process is as follows:

Step 1. In the database, find the leaf node of the Merkel tree of the storage block according to the method in Section 3.2.1.

Step 2. Calculate the key values of the sibling node and the parent node from the key values of the leaf node in the first step in the way of Section 3.2.1, and obtain the value values stored by the sibling node and the parent node in the database.

Step 3. Set the node to store the hash value $H1$ and the sibling node to store the hash value $H2$ and verify whether the value H stored by the parent node satisfies $H = H\ (H1, H2)$, if not, Merkel authentication fails.

Step 4. After obtaining the key value of the parent node, repeat the second step until the root node of the Merkel tree is reached.

Step 5. Compare the hash values stored in the Merkel tree root node to the hash values stored in the common chain.

In Step 3, the hash value is calculated using sha256, and in the prototype system, the sha256 function of the OpenSSL library is used. The calculation method of formula (15) is used to calculate $H\ (H1, H2)$. In equation (15), STR1 is a hash value stored in a node with a smaller number and STR2 is a hash value stored in a larger node. When validating, if the stored STR1 node number is odd, you need to exchange the hash value STR2 stored in STR1 and sibling nodes:

$$H(\text{STR}1, \text{STR}2) = \text{sha}256(\text{STR}1 + \text{STR}2). \quad (15)$$

3.2.4. Entry of Traceability Information. The logistics information module in the agricultural product traceability system mainly includes agricultural product ID, industrial and commercial information of sales enterprises, and other data. Upload is when the agricultural product ID is entered through the page, and the industrial and commercial information is obtained through the third-party interface to automatically fill in the interface. Click the upload button and upload the sales information to the blockchain network through the method PutState as shown in Figure 4.

Figure 4 is to realize the data uploading function of different traceability information, which has been mentioned in the article, including data uploading such as agricultural product ID and industrial and commercial information of sales enterprises, among which information such as agricultural product ID can be uploaded to the traceability system through Invoke interface.

3.2.5. Query of Traceability Information. The traceability information query module in the agricultural product traceability system mainly queries the information of each link of the agricultural product supply chain on the blockchain network through the agricultural product ID as shown in Figure 5.

3.2.6. Detection System of Heavy Metal Ions in Soil. For traceability of agricultural products, heavy metal concentration information of soil with crops is usually stored as traceability information in the traceability system. According to the blockchain technology described in this paper, the heavy metal inspection node is used as a tracking node of the source system, and the soil heavy metal ion information is recorded in the source system as an item of tracking information.

As shown in Figure 6, the soil heavy metal detection system described in this section mainly consists of three parts:

(a) Heavy metal ion concentration sensors, including copper and chromium ion concentration sensors.

(b) An analog-to-digital converter.

(c) A heavy metal ion concentration analysis system running on a single chip microcomputer.

4. System Test

The previous chapter discusses mainly building the environment and functional development of detailed design and analysis. This chapter discusses the traceability system of agricultural products function test and performance test, to ensure that the system can run normally and stably. It mainly includes unit, function, and performance tests.

4.1. System Unit Test. System unit test is mainly to test the current chain code file method. The chain code of agricultural products traceability system studied in this paper uses go programming language, so the go test tool used in unit test and unit test file is shown in Table 2.

Let us take product.go as an example. In the chaincode directory, create a new product _ test.go file. The test function is as shown in Algorithm 1.

Execute the go test command, and the test result "pass" indicates that the test succeeded; otherwise, it failed.

4.2. System Function Test. System function test is mainly to verify whether the blockchain network in the agricultural product traceability system is normal, and whether the data

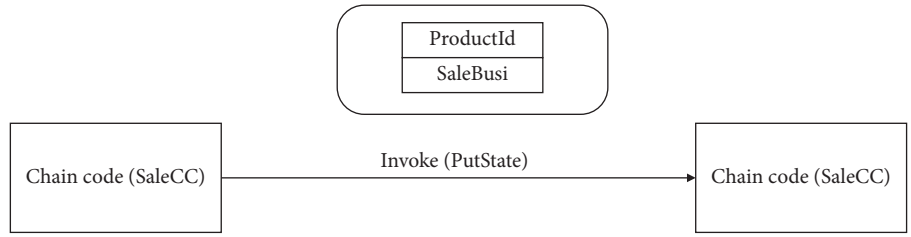

Figure 4: Upload model of agricultural product sales data.

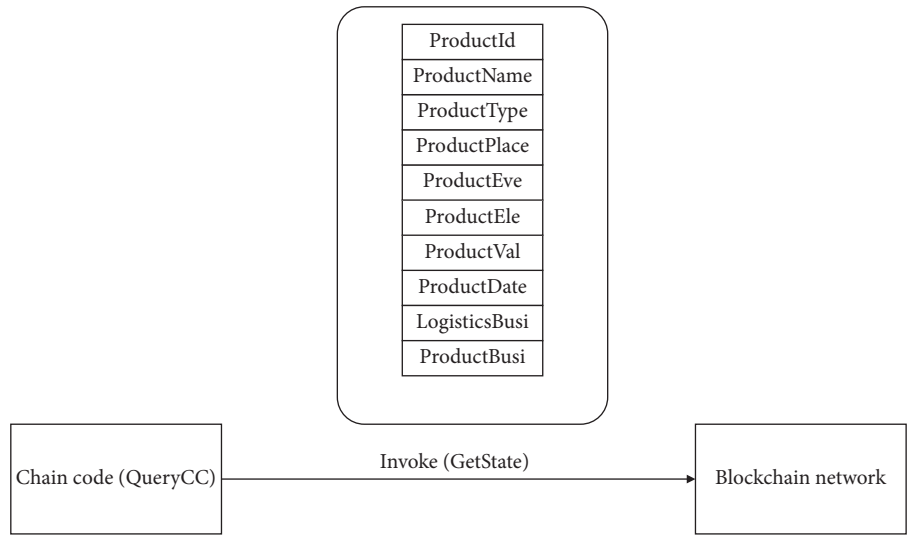

Figure 5: Traceability model of agricultural products.

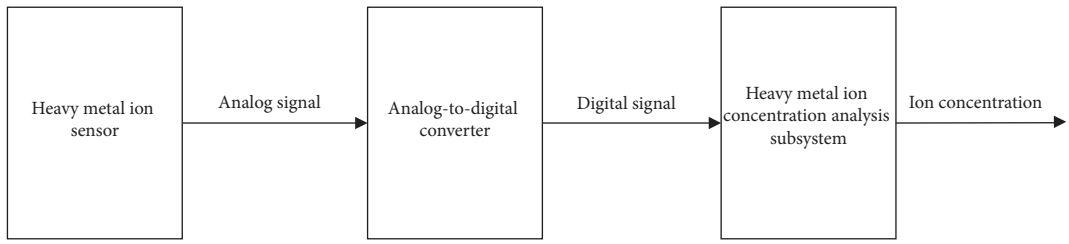

Figure 6: Soil heavy metal inspection system.

Table 2: List of unit test files.

Test content	Test results
product.go	Pass
process.go	Pass
logistics.go	Pass
sale.go	Pass
source.go	Pass

uploading and query function modules are normal. Specific verification data are shown in Table 3.

4.3. System Performance Test. The system performance test, also called the stress test or load test, mainly tests whether the system can normally work under a certain load. The performance test of the agricultural product traceability system studied in this paper mainly starts with two indicators: user concurrency and response time, through LoaderRunner software to simulate online users and through LoaderRunner software controller module for multiuser simulation.

In the controller interface, you can choose to set the number of users manually and then increase the test index in a gradual way to test the limit of the system. The traceability system of agricultural products studied in this paper adopts the working state of 100 people, 400 people, and 1000 people, and its test results are shown in Tables 4–6.

We also compared the performance of agricultural products traceability system in Heilongjiang Province. Under the same experimental environment, the results are as follows.

To show the superiority of performance more clearly, the blockchain system is compared with the traditional multiple traceability systems, and its average response time is plotted with the number of users. The results are as shown in Figure 7.

```
 package main
import(
   “fmt”
   “eccoding/json”
   “github.com/hyper ledger/fabric/core/chaincode/shim”
   pb “github.com/hyperledger/fabric/protos/peer”
   )
func TestUploadProductInfo(t *testing.T){//The test function name must begin with test and must accept a * testing.T type parameter
   got: = uploadProductinfo(“orange”, “orange01”, “fruit”, “sichuan”, “xxx”, “xxx”)//Program output result
   want: = shim.Success(nil)//Expected result
   if !reflect.DeepEqual(want, got){
      t.Error(“excepted:%v, got:%v”, want, got)//Test failure output error prompt
      }
}
```

Algorithm 1: The product _ test Function.

Table 3: System function test table.

Test	Test content	Test results
Functional test project	Does the container in the blockchain network operate normally	Normal
	Is the interface of each link in the agricultural product supply chain displayed normally	Yes
Functional interface test	Inquire whether the traceability information interface is displayed normally	Yes
	Is page jump normal	Yes
	Whether the required entry is validated	Yes
Form validation test	Prompt for input errors	Yes
	Prompt for success or error of submission	Yes
Browser compatibility test	Is the display of different mobile phones normal	Normal

Table 4: Performance test of agricultural product traceability system based on blockchain.

Number of users	Average response time (ms)	Peak traffic response time	Test conclusion
100	0.925	1.145	Pass
400	1.318	1.923	Pass
1000	2.466	2.786	Pass

Table 5: Performance test of Heilongjiang agricultural products traceability system.

Number of users	Average response time (ms)	Peak traffic response time	Test conclusion
100	2.012	2.203	Pass
400	3.318	3.567	Pass
1000	4.466	4.498	Pass

Table 6: Performance test of the traditionally developed traceability system.

Number of users	Average response time (ms)	Peak traffic response time	Test conclusion
100	3.523	3.125	Pass
400	6.451	6.874	Pass
1000	7.355	7.845	Pass

As can be seen from Figure 7, the designed data sharing traceability system based on blockchain has a better response time, which means that our performance can meet the general requirements of the traceability system and is better.

4.4. Comparison of Specific Functional Tests of Block Systems. ART: average response time per request; TPS: the number of concurrent requests that can be responded to per second.

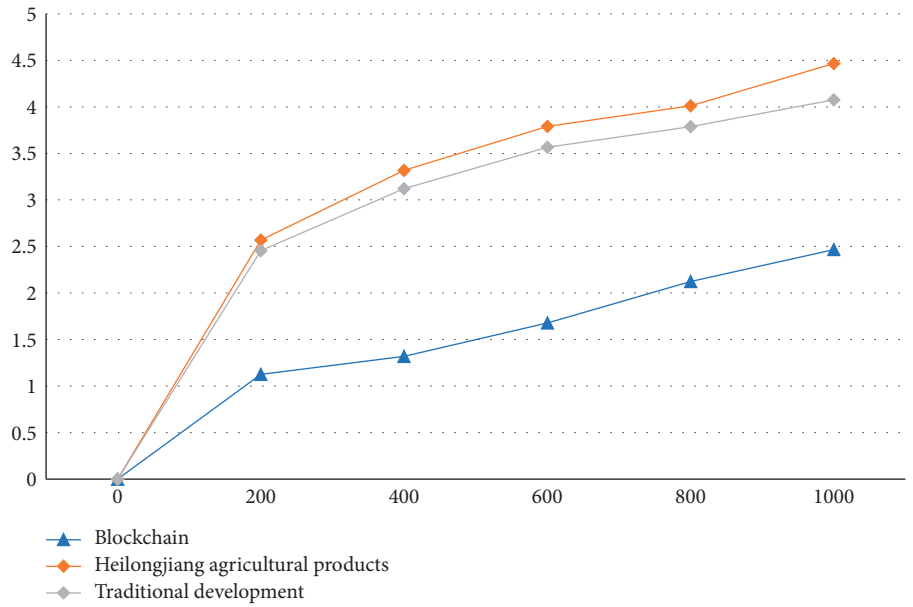

Figure 7: Performance diagram of various traceability systems.

Table 7: System query test results.

System	Number of query requests	1000	1500	2000	2500	3000	3500	4000
Blockchain	Mean response time (MS)	22	35	52	97	125	215	278
	Success rate (%)	100	100	100	100	100	100	100
Heilongjiang agricultural products	Mean response time (MS)	25	40	70	125	189	264	387
	Success rate (%)	100	99.7	99.6	99.5	99.4	98.4	99.3
Traditional development	Mean response time (MS)	32	54	87	165	221	312	452
	Success rate (%)	100	99.4	99.3	99.2	99.2	99.1	99

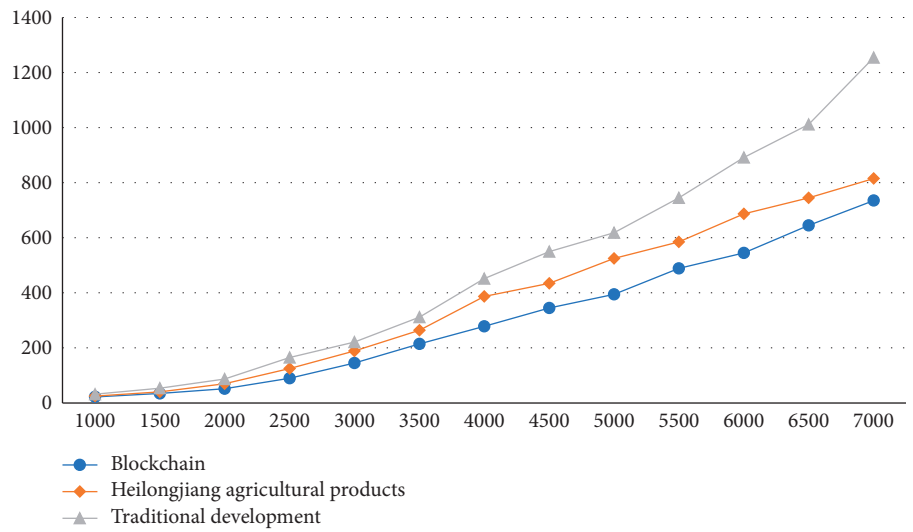

Figure 8: ART-concurrent information query request curve.

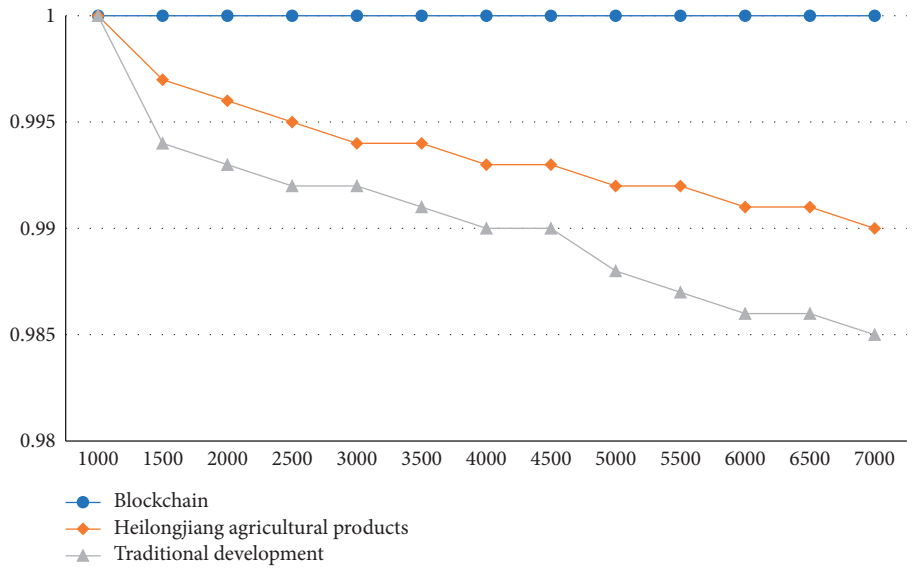

Figure 9: ART-concurrent information query request success rate.

Table 8: Business transaction processing function test.

System	Transaction volume	30	60	90	120	150	180	210
Blockchain	Mean response time (MS)	74	156	227	345	489	654	801
	Success rate (%)	100	100	100	100	100	100	100
Heilongjiang agricultural products	Mean response time (MS)	85	174	310	415	612	1021	1250
	Success rate (%)	100	99.5	99.4	99.4	99.3	99.2	99.1
Traditional development	Mean response time (MS)	112	225	398	521	787	1254	1545
	Success rate (%)	99.6	99.4	99.3	99.2	99.1	89.9	89.7

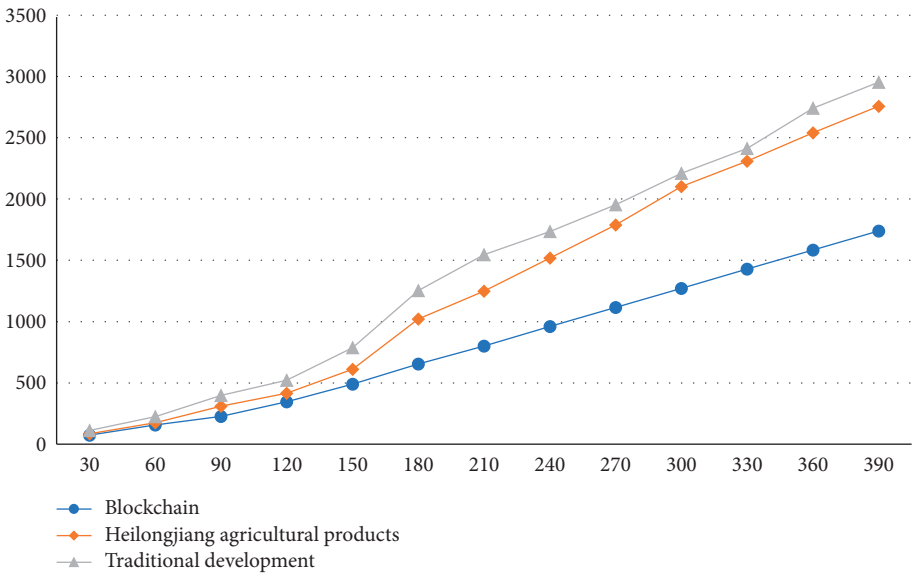

Figure 10: ART-concurrent completion transaction volume curve.

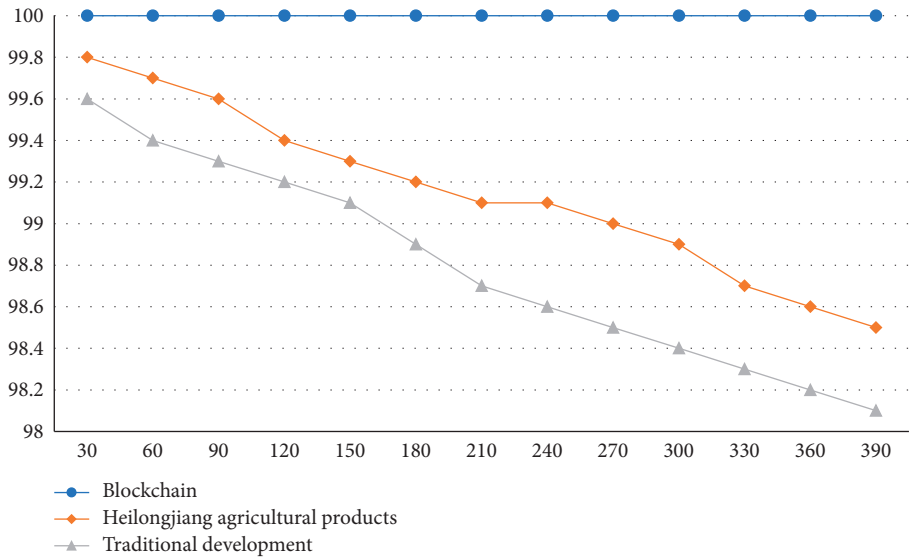

Figure 11: ART-success rate of concurrent business transaction.

Through the influence of ART and TPS indexes on the load performance of blockchain system because it is a simulation system, considering many factors, such as cost, time, and experimental conditions, according to the experimental test process, the system is reduced in equal proportion, which is convenient for the experiment.

4.4.1. Query Function Test. Grouped according to the number of query requests, there are seven groups for 1000, 1500, 2000, 2500, 3000, 3500, and 4000. The data are as shown in Table 7.

From the query time and success rate of concurrent information in Figures 8 and 9, the system based on the blockchain can have a very low average response time and the highest query success rate. In the other two methods, the average response time increases obviously with the increase in concurrency, but the success rate is getting lower and lower.

4.4.2. Business Transaction Processing Functional Testing. There are seven groups, 30, 60, 90, 120, 150, 180, and 200, which are grouped according to the transaction volume of concurrent requirements. The data are as shown in Table 8.

From the response time and success rate of completing business transactions in Figures 10 and 11, the system based on the blockchain can have a very low average response time and the highest query success rate. In the other two methods, the average response time increases obviously with the increase of concurrency, but the success rate is getting lower and lower.

5. Conclusion

In this paper, aiming at the shortcomings of the traditional agricultural product traceability system, such as low security, untrustworthiness, and difficulty in information collection, a data-sharing traceability system based on blockchain technology is proposed. The traceability system uses a license chain with high throughput to store traceability information and realizes the function of locating the responsible person. To reduce the security overhead of the license chain, the verification information of the license chain is stored in the public chain with great computing power to ensure security, and its legitimacy is verified by Merkle verification. The security of the public chain is fully guaranteed. Future work considers different intelligent optimization algorithms [23, 24] in blockchain to further optimize the system and improve its performance.

Data Availability

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

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study was sponsored in part by the Innovation and Entrepreneurship Demonstration Team of Yingcai Program of Chongqing, China (Grant no. CQYC201903167), Science and Technology Research Project of Chongqing Education Commission (Grant no. KJQN202001342), Technical Innovation and Application Development Special Project of Chongqing (Grant no. cstc2020jscx-sbqwX0015), Tower Foundation Project of Chongqing University of Arts and Sciences (Grant no. Y2020RG11), Social Undertakings and People's Livelihood Guarantee Project of Yongchuan District (Grant no. Ycstc, 2020cc1201).

References

[1] H. Lei, "Empirical analysis of the influence of tax on the agricultural products processing industry development under the constraint of financial index," *Boletin Tecnico/Technical Bulletin*, vol. 55, no. 15, pp. 570–578, 2017.

[2] A. R. Rajput, Q. Li, and M. T. Ahvanooey, "A blockchain-based secret-data sharing framework for personal health records in emergency condition," *Healthcare*, vol. 9, no. 2, pp. 206–215, 2021.

[3] V. Jaiman and V. Urovi, "A consent model for blockchain-based distributed data sharing platforms," *IEEE Access*, vol. 8, pp. 143734–143745, 2020.

[4] T. Li, J. Zhang, Y. Lin, S. Zhang, and J. Ma, "Blockchain-based fine-grained data sharing for multiple groups in Internet of Things," *Security and Communication Networks*, vol. 2021, Article ID 6689448, 13 pages, 2021.

[5] Z. Su, Y. Wang, Q. Xu, and N. Zhang, "LVBS: lightweight vehicular blockchain for secure data sharing in disaster rescue," *IEEE Transactions on Dependable and Secure Computing*, no. 99, p. 1, 2020.

[6] C.-L. Chen, Y.-Y. Deng, W. Weng, M. Zhou, and H. Sun, "A blockchain-based intelligent anti-switch package in tracing logistics system," *The Journal of Supercomputing*, vol. 77, no. 7, pp. 7791–7832, 2021.

[7] H. Huang, X. Chen, and J. Wang, "Blockchain-based multiple groups data sharing with anonymity and traceability[J]," *Science China Information Sciences*, vol. 63, no. 3, pp. 1–13, 2020.

[8] B. Zhang, C. W. Chao, Y. Tsybovsky et al., "A platform incorporating trimeric antigens into self-assembling nanoparticles reveals SARS-CoV-2-spike nanoparticles to elicit substantially higher neutralizing responses than spike alone," *Scientific Reports*, vol. 10, no. 1, Article ID 18149, 2020.

[9] R. Zou, X. Lv, and J. Zhao, "SPChain: blockchain-based medical data sharing and privacy-preserving eHealth system," *Information Processing & Management*, vol. 58, no. 4, Article ID 102604, 2021.

[10] 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 2017 IEEE International Congress on Big Data (BigData Congress)*, pp. 557–564, Honolulu, HI, USA, June 2017.

[11] R. Saxena, D. Arora, V. Nagar, and S. Mahapatra, "Bitcoin: a digital cryptocurrency," in *Blockchain Technology: Applications and Challenges*, S. K. Panda, A. K. Jena, S. K. Swain, and S. C. Satapathy, Eds., vol. 203, , pp. 13–28, Intelligent Systems Reference Library, 2021.

[12] C. S. Shih and K. W. Yang, "Design and implementation of distributed traceability system for smart factories based on blockchain technology," in *Proceedings of the Conference on Research in Adaptive and Convergent Systems*, pp. 181–188, Chongqing, China, September 2019.

[13] O. I. Konashevych, "Data insertion in blockchain for legal purposes. How to sign contracts using blockchain," *Elektronnoe Modelirovanie*, vol. 41, no. 5, pp. 103–120, 2019.

[14] R. Shanthakumari and S. Malliga, "Dual layer security of data using LSB inversion image steganography with elliptic curve cryptography encryption algorithm," *Multimedia Tools and Applications*, vol. 79, no. 4, pp. 3975–3991, 2020.

[15] Y. Zhang, W. Yang, Q. Xue, J. Huang, and W. Che, "Broadband dual-polarized differential-fed filtering antenna array for 5G millimeter-wave applications," *IEEE Transactions on Antennas and Propagation*, no. 99, p. 1, 2021.

[16] T. G. Volkova, "Reasons and features of implementing blockchain technology in the pension system of the Russian federation," *Bulletin of Udmurt University. Series Economics and Law*, vol. 30, no. 3, pp. 333–339, 2020.

[17] P. Zhu, J. Hu, X. Li, and Q. Zhu, "Using blockchain technology to enhance the traceability of original achievements," *IEEE Transactions on Engineering Management*, no. 99, pp. 1–15, 2021.

[18] L. Tian and Y. Sun, "Research summary of blockchain fragmentation propagation mechanism based on Merkel tree," *Journal of Physics: Conference Series*, vol. 1914, no. 1, Article ID 012010, 2021.

[19] P. Podduturi, P. Ahmadi, K. Islam, and T. Maco, "RFID implementation in supply chain management using P2P network overlays," in *Proceedings of the 2019 Wireless Telecommunications Symposium (WTS)*, New York, NY, April 2019.

[20] P. Wang, P. Liu, and F. Chiclana, "Multi-stage consistency optimization algorithm for decision making with incomplete probabilistic linguistic preference relation," *Information Sciences*, vol. 556, pp. 361–388, 2020.

[21] A. L. Nitka, W. M. DeVita, and P. M. McGinley, "Evaluating a chemical source-tracing suite for septic system nitrate in household wells," *Water Research*, vol. 148, pp. 438–445, 2019.

[22] X. Liu, Z. Cai, H. Fan, and M. Yu, "Experimental studies on the rtEthernet-based centralized fault management system for smart grids," *Electric Power Systems Research*, vol. 181, pp. 106163.1–11, 2020.

[23] G. Chen and S. Li, "Research on location fusion of spatial geological disaster based on fuzzy SVM," *Computer Communications*, vol. 153, pp. 538–544, 2020.

[24] G. Chen, L. Wang, M. Alam, and M. Elhoseny, "Intelligent group prediction algorithm of GPS trajectory based on vehicle communication," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 3987–3996, 2020.