A Trusted Blockchain-Based Traceability System for Fruit and Vegetable Agricultural Products

XINTING YANG[1,2,3], MENGQI LI[1,2,3], HUAJING YU[1,2,3], MINGTING WANG[1,2,3], DAMING XU[1,2], AND CHUANHENG SUN[1,2]

[1]National Engineering Research Center for Information Technology in Agriculture, Beijing 100097, China
[2]National Engineering Laboratory for Agri-product Quality Traceability, Beijing 100097, China
[3]College of Information, Shanghai Ocean University, Shanghai 201306, China

Corresponding author: Chuanheng Sun (sunch@nercita.org.cn)

ABSTRACT Traditional traceability system has problems of centralized management, opaque information, untrustworthy data, and easy generation of information islands. To solve the above problems, this paper designs a traceability system based on blockchain technology for storage and query of product information in supply chain of agricultural products. Leveraging the characteristics of decentralization, tamper-proof and traceability of blockchain technology, the transparency and credibility of traceability information increased. A dual storage structure of "database + blockchain" on-chain and off-chain traceability information is constructed to reduce load pressure of the chain and realize efficient information query. Blockchain technology combined with cryptography is proposed to realize the safe sharing of private information in the blockchain network. In addition, we design a reputation-based smart contract to incentivize network nodes to upload traceability data. Furthermore, we provide performance analysis and practical application, the results show that our system improves the query efficiency and the security of private information, guarantees the authenticity and reliability of data in supply chain management, and meets actual application requirements.

INDEX TERMS Blockchain, traceability, on-chain and off-chain, agricultural products.

I. INTRODUCTION

Fruit and vegetable agricultural products have excellent production advantages in China, which is a large agricultural country with superior climate conditions and abundant species resources. According to data from the National Bureau of Statistics of China [1], the total output of fruit and vegetable agricultural products in 2019 was 995.03 million tons, accounting for 54.48% of all agricultural products (1826.55 million tons). Fruit and vegetable agricultural products have the characteristics of green, healthy and high nutritional value [2], which are deeply loved by people. However, the short storage time and the low storage temperature of storage requirements for fruit and vegetable agricultural products, leading to food safety incidents are extremely prone to occur [3].

In recent years, domestic and international safety incidents of fruit and vegetable agricultural products have occurred

frequently. Such as "poisonous ginger" incident in China [4], Hami melon contamination by listeria in United States [5], and the outbreak of E. coli in Germany [6], which have greatly harmed the health of the majority of people. As a result, the state attaches great importance to the traceability of food supply chain, and countries strengthen management of traceability by issuing relevant laws and regulations. The General Food Law promulgated by the European Union in 2002 [7] stipulates that a comprehensive traceability system must be established in the food industry in order to recall targets in a timely and accurate manner and transmit information to consumers. The Food Safety Law implemented by China in 2009 [8], which provides that food producers and operators should establish a food safety traceability system to ensure food traceability. "Traceable" has become a challenge for all food and food-related companies and the traceability system has become an effective means of quality management in the agricultural product supply chain [9]–[11].

The traceability of fruit and vegetable agricultural products involves many subjects. In accordance with the business

The associate editor coordinating the review of this manuscript and approving it for publication was Adnan Abid.

relationship, it can be divided into internal and external entities of the supply chain [12], [13]. The internal entities include production enterprises, processing enterprises, cold chain logistics enterprises, sales enterprises, etc., and the external entities embrace consumers and regulatory agencies, etc. [14]. The entire supply chain has the characteristics of many production points and sales points, long production chains, and wide production areas, which makes supervision and tracing of food safety particularly difficult in practice [15]. In practical applications, data in traditional traceability systems is centralized, and authoritative agencies manage the central database of the traceability system [16], [17]. Since the traceability data of each supply chain node are managed by enterprise, the data are easy to tamper with. Therefore, the reliability of information transmission among different roles in the agricultural supply chain needs to be increased.

Blockchain is a kind of distributed database which is decentralized, tamper-proof, traceability, and maintained by multiple parties [18]. It uses a cryptographic algorithm to form a chain structure composed of data blocks in chronological order. Any party must receive the consent of all other parties in advance according to agreed rules in order to realize information sharing and information supervision among different parties [19]. Moreover, blockchain integrates many technologies, such as Peer to Peer (P2P) networks, cryptographic technologies, smart contract, consensus mechanisms, timestamps, blockchain structure, etc. [20], [21]. Thus, it can achieve the self-verification and management of data without relying on a third party. The use of blockchain technology for the tracing of agricultural products can solve the problems with the current traditional traceability system. Blockchain are mainly divided into three categories: Public chains, Consortium chains and Private chains [22]. Consortium chains refer to the blockchain which several organizations participate in and manage together. In terms of privacy, Consortium chains is intermediate between Public chains and Private chains, with its data only being accessible by members of the alliance. Additionally, Consortium chains transaction efficiency is higher than Public chains. In a traceability system, the main responsibility bodies of the supply chain of agricultural products are related to the cooperative relationship between participants in supply chain. However, these responsibility bodies cannot be fully trusted. In reality, the main responsibility bodies of the supply chain are originally related to each other by horizontal interaction or a vertical transaction relationship. Therefore, this paper chooses the Consortium chain as basic network.

The main purpose of the current paper is to explain how to apply blockchain technology to the traceability of agricultural products. Using the features of distributed storage, hash encryption, and programmable smart contract of blockchain technology, we have designed and implemented a traceability system for fruits and vegetables agricultural products based on a trusted blockchain. We will describe the design process of the system in detail, and clarify the key breakthrough technologies of this system, including the on-chain and off-chain storage structure and the combination of cryptography to achieve privacy data protection. We will build the blockchain environment based on Hyperledger Fabric for performance testing and practical application of the agricultural product traceability system to prove the practicability of the system.

The main contributions of this paper include:

- We elaborated on the main shortcomings of current agricultural product traceability and proposed solutions.
- We apply blockchain technology to the traceability of agricultural products, and propose solutions to the problems of heavy load, slow query speed and privacy data protection on the existing blockchain technology. The detailed design of the on-chain and off-chain storage structure and privacy data protection is a key part of the research.
- We build blockchain environment based on Hyperledger Fabric, and use the C# language to develop and implement traceability system to realize the process of storing and querying agricultural product traceability information. And through the system function test and system actual application case evaluation system.

The remaining paper is organized as follows: Section II provides a literature review on agricultural product traceability; Section III describes the detailed design of the system; Section IV describes the implementation of the system in detail, analyzes the performance of the system, and gives the application results of the system and the comparison of the system and traditional traceability system. The conclusions and suggestions for future work are presented in Section V.

II. RELATED WORK

Traceability is defined as the ability to access any or all information relating to that which is under consideration, throughout its entire life cycle, by means of recorded identifications [22]. For agricultural products, traceability means that when quality problems occur, the raw materials or processing links that have problems can be quickly and effectively checked, product recalls are carried out when necessary, and targeted penalties are implemented to improve the quality and safety of agricultural products.

Traceability has become a challenge for all food and food-related companies, and traceability system has become an effective means of quality management in the agricultural supply chain. In recent years, many scholars have carried out exploratory research in the field of agricultural products traceability. Qian *et al.* [24] combined the 2D barcode and RFID technology to design and implement a Wheat Flour Milling Traceability System (WFMTS) by pasting the QR code label on the wheat package to link to its processing information and pasting the RFID label to the storage box to record the logistics information. The center database is used to manage the information from raw materials to finished products in the flour mill, and realize the whole process

monitoring from source, circulation to sales. However, the information in the traditional traceability system is managed by the enterprises in each link, and the transparency of the information is low, and the information is easy to be tampered with.

Blockchain as an emerging technology that has properties of decentralization, tamper-proof and traceability provides the possibility to solve the problems existing in the current traditional agricultural product traceability system. More and more scholars are beginning to pay attention to the application of blockchain technology in the traceability of agricultural products. In the application of combining blockchain technology with Internet of Things technology, Bumblauskas *et al.* [25] combined Internet of Things technology and blockchain technology to track products from farm to dining table in real time. Taking the egg supply chain of a Midwestern company in the United States as an example, and the implementation of blockchain technology in the supply chain system from farm to consumer was summarized in detail. Feng [26] built a real-time traceable food supply chain traceability system based on HACCP, Blockchain and IoT technologies, and introduced a new concept BigchainDB to solve the problem of blockchain scalability. Liao and Xu [27] established a blockchain traceability system based on intelligent agriculture and wireless sensor networks for tea quality and safety management, combined with food risk assessment and safety traceability technology based on hazard factors to efficiently control products quality and safety. From the multi-chain structure level of blockchain. Zhao *et al.* [13] designed a big data version fresh food traceability platform based on the account blockchain (ABC) and transaction blockchain (TBC) dual-chain architecture, analyzed user needs from the perspective of information ecology, and proposed a risk compensation plan that traces participating entities. Liu *et al.* [28] designed an anti-counterfeiting traceability system (TSPPB) that uses dual blockchain and IPFS systems. TSPPB utilized two sets of blockchains, including public chain and private chain, and the TCDBB technology is used to solve the problem of product label copy and spam. At the level of improved architecture and mechanism. Li *et al.* [29] proposed the application of blockchain technology to the database layer and communication layer of the blockchain food safety traceability system through analysis of the technical architecture level, and demonstrated the design through the case of ham sausage effectiveness of the program. Dwivedi *et al.* [30] designed a pharmaceutical supply chain management system (PSCM) by combining blockchain technology with traditional drug supply chain, and proposed a mechanism to distribute all encryption keys to all participants using smart contract technology. In the design of blockchain storage model, many scholars used on-chain and off-chain data storage to reduce pressure on on-chain storage. Lin *et al.* [31] developed and implemented a food safety traceability system based on blockchain and EPC Information Service (EPCIS), and proposed an on-chain and off-chain data storage structure to solve pressure problem of

blockchain data storage. Khaled *et al.* [32] proposed a method of performing business transactions, where the Ethereum blockchain and smart contract were used to track and trace soybeans throughout the agricultural supply chain process, coupled with the InterPlanetary File System (IPFS) for storing traceable data to reduce the amount of data stored on the chain. Dong *et al.* [33] designed a reliable traceability prototype system for the whole food supply chain based on blockchain technology, and proposed a data storage mode of ''on-chain + cloud database''. Thus ensuring the operating cost and efficiency of the blockchain system. Although a large number of scholars have constructed a blockchain-based traceability system, most of them have not considered the issues of efficient information storage and privacy data security.

III. DESIGN OF TRACEABILITY SYSTEM
A. SYSTEM FRAMEWORK
This paper divides the traceability of agricultural products into the links of production, processing, logistics, and sales. The production link involves planting, transplanting, watering, fertilizing and picking operations of fruits and vegetables agricultural products, and records key information such as seedling information, planting process information, environmental information, and product transaction information. The processing link includes classifying, weighing, packaging, pasting two-dimensional code and other operations for the picked fruits and vegetables, and recording the product information, processing process, processing environment, product transaction and other key information. The transportation link refers to the transportation of (such as the Internet of Things) during the process of production, processing, transportation, and sales. Using a traceability system, detailed information about agricultural products can be displayed to consumers, and the trust of consumers regarding the safety of agricultural products can thereby be enhanced. When quality and safety accidents occur with agricultural products, law enforcement agencies can trace back to the problem link and determine where the main responsibility for the accident lies. Blockchain traceability refers to the use of blockchain technology in traceability systems; such traceability is achieved using blockchain characteristics of decentralization, non-tampering, and traceability to ensure the authenticity and transparency of traceability information in agricultural products traceability systems, and achieves effective and reliable traceability. The blockchain-based fruit and vegetable agricultural products traceability system uses the data storage scheme to manage the growth information, processing information, logistics information and sales information of fruits and vegetables agricultural products, so as to monitor the whole process of agricultural products production, processing, transportation and sales. The structure of agricultural products blockchain traceability system was mainly divided into storage layer, service layer, interface layer and application layer, as shown in Figure 1.
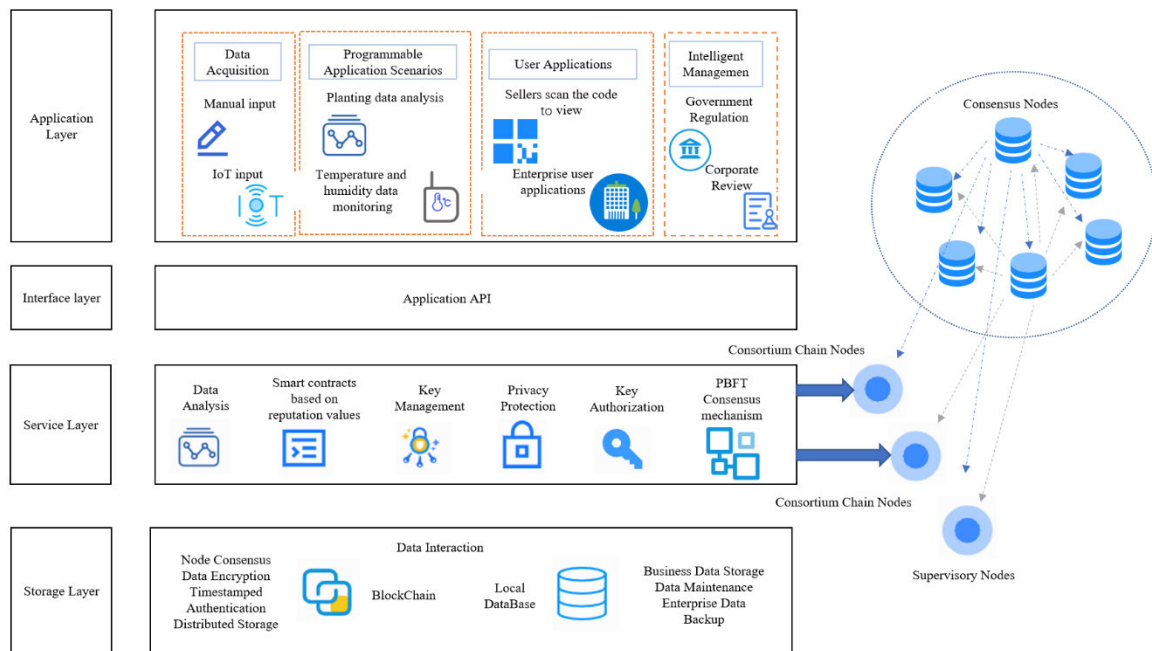
FIGURE 1. Blockchain-based traceability system architecture.

Among them, the storage layer includes MySQL, the local database of the system, and the CouchDB database that comes with the blockchain system. The local database stores the public information of each link. The blockchain system stores the encrypted ciphertext of the private information and the hash value of the public information to meet the needs of fast data query and small storage space on the blockchain, which ensures the security of private information. At the same time, the authenticity comparison is provided when checking whether the traceability information has been tampered with. The service layer includes data analysis, reputation-based smart contract, key management, key authorization, PBFT consensus mechanism, etc. The interface layer is composed of smart contracts, which mainly implement the data upload blockchain system and data query functions. The data was automatically executed when the label is printed, and the query is automatically responded to when the terminal makes a request. The application layer provides business functions corresponding to different users of the system platform, such as uploading data from enterprises in various links, querying traceability information by consumers, and supervision by government departments.

B. ON-CHAIN AND OFF-CHAIN DATA STORAGE TECHNOLOGY

The existing storage mode of blockchain traceability system involves directly writing traceability information of each node of agricultural products into blockchain. With increasing numbers of nodes, an increasing amount of transaction data is obtained, and the storage load pressure of blockchain consequently increases [34]. Due to the unique chain-type structure of blockchain, the query efficiency is very low;
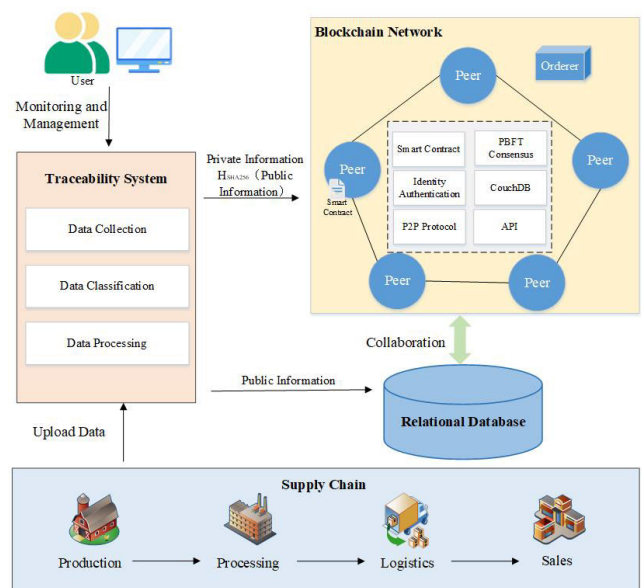

FIGURE 2. On-chain and off-chain data collaboration storage.

members of the same blockchain network access all the data on the chain ledger. To overcome these shortcomings, this paper improved the storage mode of a blockchain traceability system for agricultural products and designed a method involving the double storage of traceability information under the chain of ''database + blockchain''. As shown in Figure 2, after traceability data uploaded to the system, the system classifies the data. The product public information is stored in the local database. The encrypted ciphertext and the hash value of public information is uploaded to blockchain. Considering the issue of storage space, the SHA256 algorithm with higher
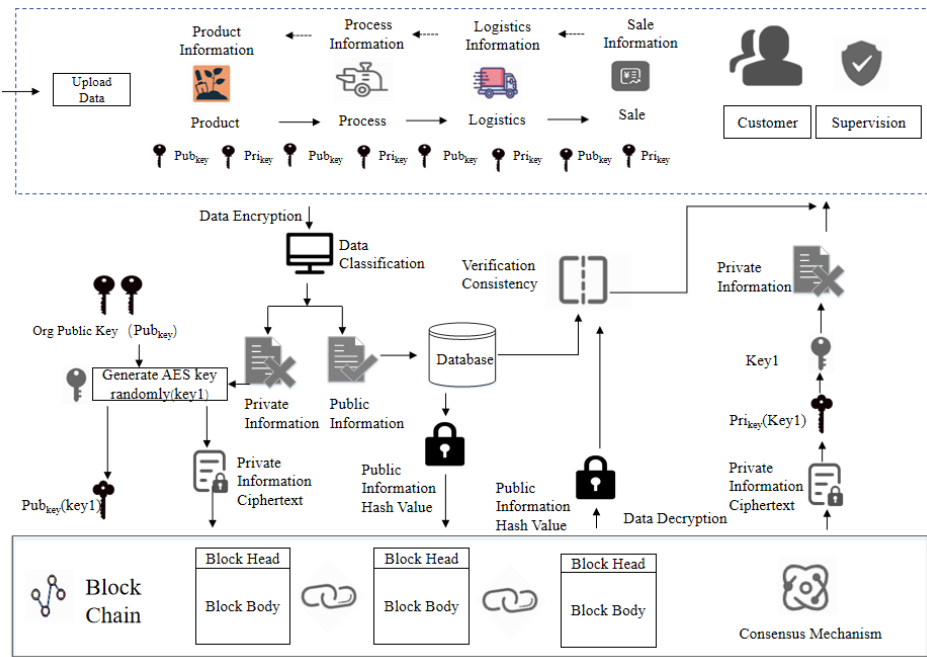
FIGURE 3. Traceability information privacy protection data flow diagram.

security is used in the encryption of public information. For the input of any length string, the SHA256 algorithm will generate a 64-bit hexadecimal value. The block structure of the traceability information data structure stored on the blockchain includes block head and block body. The block head mainly includes current block number, the hash value of previous block, timestamp, and other information. The block body mainly contains transaction-related information. The storage format of the traceability information is shown in Table 1. "Key" is the corresponding ID in the "Value" parameter, which acts as an index and a unique identification field. The parameter "Value" is the value written to the blockchain, including Type, ID, PrivateData and InfoHash. The parameter "Type" is the name of the structure body that is defined by the "Value" parameter. The parameter "ID" is the unique identification field of the source message record, which corresponds to the unique identification field of the source traceability information stored in the local database. The parameter "PrivateData" is the ciphertext of private information encrypted by CBC algorithm. The parameter "InfoHash" is the value of source traceability information after this information has been hashed.

C. TRACEABILITY INFORMATION PRIVACY PROTECTION PROCESS

The data involved in the entire supply chain is not only product traceability information, but also contains private data that only relevant companies can view, such as transaction information. For competing enterprises, data privacy is an important issue. This paper design a traceability information privacy protection data flow that private information is encrypted by deploying smart contract and uploaded to the

TABLE 1. Data structure of the blockchain used in the system.

Key	ID

Value	{
	"Type": "Info",
	"ID": "36",
	"PrivateData":"e515789cae824dad1699f74687a87bf158c eb04b89fdc8b01f7609d6c49ca66adbcf8a4b9bd2c34aea6 4c3",
	"InfoHash":"429ab56c73040aaf65247e44279d073abb131 10654aa99798d5835931065b98e"
	}

blockchain together with the hash value of public information. As shown in Figure 3, private information such as transaction data is encrypted by the Cipher Block Chaining (CBC) mode of the AES encryption algorithm. The required Key1 is randomly selected by the smart contract generate and upload encrypted ciphertext to the blockchain. In order to ensure the security of the Key1, this paper used the Elliptic Curves Cryptography (ECC) to encrypt the Key1. The encrypted Public Key authorized the viewing node. The Public Key of the authorized viewing node and the Encrypted Key1 form a key-value pair, stored in the world state of the smart contract and written to the blockchain. When the relevant enterprise nodes view the private data on the blockchain, the current node private key is used to decrypt the Encrypted Key1 on the blockchain to obtain the original Key1, and the Key1 is used to decrypt the private information and view the private information.

D. SMART CONTRACT FOR SYSTEM

Smart contract are essentially time-driven, stately computer programs deployed on shared distributed database [35]. It can

TABLE 2. Smart contract interface.

Contract business logic	Interface definition	Interface description
Upload traceability data	PutTracedata	Upload hash value of traceability data to blockchain
Query traceability data	QueryTracedata	Query hash value of traceability data from the blockchain
Initialize reputation value	InitReputation	Initialize reputation value when node joins alliance
Allocate Reputation value	GetReputation	Grant reputation value to node
Query reputation value	QueryReputation	Query reputation value of node

be automatically executed when trigger conditions are met, and node behavior can be transmitted and verified in an informationized manner. Smart contract are called Chaincode in Hyperledger Fabric, which greatly reduces the degree of manual participation and ensures the decentralization of blockchain and the tamper-proof of data. Alliance members in the Consortium chains negotiate to participate in book-keeping, and define incentive methods based on business needs. The agricultural products traceability system based on blockchain designed in this paper records traceability data of fruit and vegetable products from production, processing, transportation, and sales. In order to encourage alliance members to upload traceability data, this paper designs a reputation-based smart contract. After the node uploads the traceability data that meets the requirements, the contract logic will be triggered to increase the reputation value of the node. Table 2 presents the interface of the smart contract.

Algorithm 1 Upload Information to Blockchain

Input: ID, Private Information, Hash Value of Public Information, Public Key

1 *ID* is the unique identification field of the source message record

2 **if** *Private Information*!=NULL **then**

3   Randomly generate Key1.

4   PrivateData=CBC (*Private Information*, Key1).

5   EncryptedKey = ECC (Key1, *Public Key*).

6   InfoHash=*Hash Value of Public Information*.

7   Add *ID*, PrivateData, EncryptedKey, InfoHash in blockchain.

8 **end**

9 **else**

10   InfoHash=*Hash Value of Public Information*.

11   Add *ID*,InfoHash in blockchain.

12 **end**

Algorithm 1 elaborates the process of upload information to blockchain. The system categorizes the information and uploads it to the smart contract. After the smart contract judges the information, the corresponding operation is executed on the chain to realize the secure sharing of private information in the blockchain network.

Algorithm 2 illustrates the process of granting reputation value. When alliance member nodes upload traceability data that meets requirements, the smart contract awards the node reputation value in line with the consortium network incentive mechanism, and incentivizes network nodes to upload traceability data to ensure the integrity of the traceability chain and the sharing of information between upstream and downstream links.

Algorithm 2 Grant Reputation Value

Input: Peer, traceability data

1 *Peer* is the member of organization of the Hyperledger Fabric.

2 Initialize reputation value when peer enters the consortium chain.

3 **if** *Peer* upload *traceability data* **then**

4   **if** All nodes have reached a consensus after verification **then**

5   Trigger the smart contract issuing the reputation value.

6   **end**

7   **else**

8   Preview an error after returning the contract to its previous state.

9   **end**

10 end

E. TRACEABILITY ANTI-COUNTERFEITING PROCESS

The flow chart of fruit and vegetable agricultural products blockchain traceability system is shown in Figure 4. The traceability information is collected by Internet of Things device or manually entered. Users upload the traceability information of production, processing, logistics and sales to the system. After classification by system, the traceability information is divided into private information and public information. The private information is uploaded to blockchain after CBC encryption, and the public information is stored in the local database. The SHA256 algorithm is used to hash the public information. The hash value obtained is stored in the blockchain system, and the block number is returned. The block number is updated to the public information record corresponding to the database. If the agricultural products information needs to be modified, the hash value of the public information needs to be rewritten into the blockchain to update its block number. Consumers can obtain public information and block number from the database by scanning the QR code, hash the public information obtained, and compare the consistency with the hash value stored on the blockchain through the block number to determine whether the product traceability information has been tampered with.

IV. IMPLEMENTATION OF THE TRACEABILITY SYSTEM
A. DEVELOPMENT ENVIRONMENT
The blockchain-based traceability system for fruit and vegetable agricultural products mainly divided into two parts,

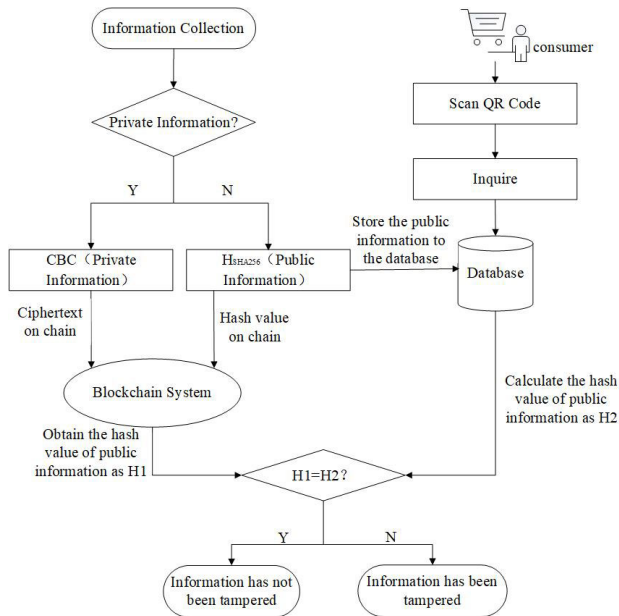**FIGURE 4.** Anti-counterfeiting flowchart of system traceability.

FIGURE 5. Blockchain network environment construction.

one is the construction of consortium chain and the other is the development of business system. Based on the Linux system environment, the blockchain system builds a Hyperledger Fabric distributed network environment based on multiple Docker containers, using CouchDB as database. The shell script is mainly used to build the network. The smart contract is implemented in Go language, and the related dependent NodeSDK development, implement Restful interface for resource call. The application system is developed in .Net/C# language, adopted the MVC (Model-View-Controller) architecture, the Bootstrap framework and a novel JavaScript framework. The blockchain system Hyperledger Fabric runs under the Linux environment and uses the Ubuntu operating system with Inter Xeon Gold 6130 processor, 16GB memory, 100GB hard disk, and 100Mb/s bandwidth. The blockchain network is deployed in a Docker container, as well as the installation, testing, and instantiation of smart contracts need to be performed in the Docker environment. As shown in Figure 5, the blockchain system in this paper adopts the deployment mode of single machine multi-node. The production enterprises, processing enterprises, logistics enterprises, sales enterprises and regulatory authorities in the supply chain are added to the blockchain as five organizations, named org1-org5 respectively. Each organization contains a peer node, corresponding to a CA certification, used to track identity and digital certificate management. The entire network contains an orderer node, which is used to sort data and generate blocks.

B. CONSENSUS MECHANISM

Consensus mechanism is a vital part of the blockchain, which ensures that the participating nodes in the blockchain network store consistent information and the latest blocks are
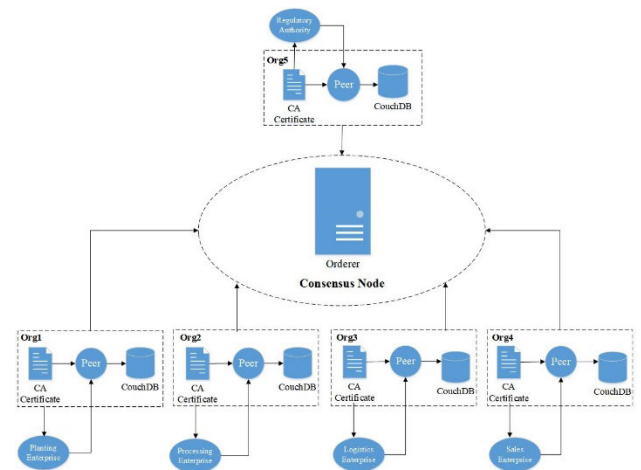
accurately added to the blockchain. The current mainstream consensus mechanisms include Proof of Work (POW), Proof of Stake (POS), Delegated Proof of Stake (DPOS), practical Byzantine fault tolerance (PBFT), etc. [36]. The core idea of POW is to ensure data consistency and consensus security by introducing the computing power competition of distributed nodes, which can solve the problem of sybil attacks caused by the free entry and exit of nodes. In order to avoid the power consumption caused by the high dependence on the computing power of the nodes, the researchers proposed a proof of stake mechanism POS that does not rely on computing power and a delegated proof of stake mechanism DPOS. PBFT consensus mechanism allow distributed system to reach a consensus when there are a few malicious nodes. It uses cryptographic algorithms such as signatures, signature verification, and hashing to ensure tamper-proof modification, anti- counterfeiting, and non-repudiation during message transmission. And optimized the BFT algorithm, reducing its algorithm complexity from exponential level to polynomial level. PBFT consensus mechanism is not suitable for large-scale Public chain scenarios owing to consensus cost, and it is more suitable for Consortium chains or Private chains with fewer nodes. According to the characteristics of agricultural product traceability, this paper chooses Consortium chain as the basic network, and the consensus mechanism chooses the PBFT mechanism apply to Consortium chain.

C. MODULE DISPLAY

The system operation page includes eight modules which are my farm, base management, production operations, crop traceability, value-added services, system settings, big data analysis, and blockchain management modules were shown in Figure 6. Figure 6(a) shows the resume creation page. Users can set the traceability information displayed to consumers according to the traceability requirements, and the hash value of the information will be stored in the blockchain. Figure 6(b) is the blockchain management page. Users can
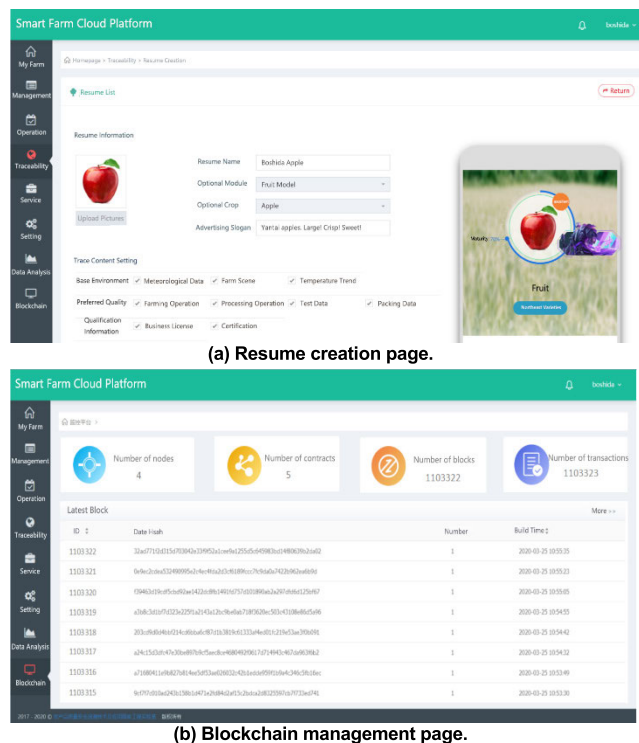
(a) Resume creation page.

(b) Blockchain management page.

FIGURE 6. Blockchain-based traceability system operation page:
(a) Resume creation page. (b) Blockchain management page.

view the relevant information of the blockchain in real time, such as the number of nodes, the number of contracts, the number of blocks, and the number of transactions.

D. SYSTEM PERFORMANCE ANALYSIS

This paper has carried on the comprehensive test to system performance, by changing send rate to test system throughput and network latency. An open source blockchain performance evaluation tool Hyperledger Caliper is used, which allowed users to perform performance tests on the blockchain network through predefined use cases and obtain a set of performance test results. The currently supported performance indicators include transaction success rate, transaction throughput, transaction latency, resource consumption, etc. The performance of system is mainly reflected in two aspects: transaction latency and transaction throughput under different send rate. Transaction latency refers to the response time required for a single user to send a request, including query latency and write latency. Transaction throughput refers to the number of successfully sent data per second, also falls into two categories: query throughput and write throughput. This paper tested transaction latency and transaction throughput of the system. The test results of read request are shown in Figure 7. It can be found from Figure 7(a) that when the send rate of the read request is less than 250tps, the send rate of the read request is linearly related to the read throughput. When the send rate exceeds 250tps, the read throughput of system reaches saturation. The system read latency is tested by increasing the send rate from 0tps to 400tps in a total time

of 60 s, each increment of 50tps. The transaction latency test result of the read request is shown in Figure 7(b). The results show that the send rate has little effect on the read latency of the system, and the average response time of the system is stable at 0.02s. The test results of the input request are shown in Figure 8. It can be found from Figure 8(a) that when the send rate of the input request is less than 125tps, the send rate of the input request is linearly related to the input throughput. When the send rate exceeds 125tps, the input throughput of the system reaches saturation. The system input latency is tested by increasing the sending rate from 0tps to 200tps in a total time of 60 s, each increment of 50tps. It can be shown from Figure 8(b) that there is no obvious correlation between the send rate and the input latency of the system, and the average response time of the system has always been kept at a low input latency of about 0.12s. In summary, the fruit and vegetable agricultural products traceability system based on blockchain technology proposed in this paper is a low-latency, high-throughput system that satisfies actual production needs.

E. APPLICATION OF THE TRACEABILITY SYSTEM

The system has been successfully applied to an apple company in Yantai City, Shandong Province, China. Through on-the-spot investigation on the apple supply chain of enterprise, the apple traceability system collection method was designed from the planting and warehousing, processing, transportation and sales links, and the "database + blockchain" proposed on the chain was used. The dual storage design of traceability information, and the query method of the external database index, have realized the efficient storage and query of the traceability information of the apple blockchain. Figure 9 shows the product label and product information query method in practical applications. Figure 9(a) shows the label information of apple. Users can scan the QR code on the package and send a query request to the background server to obtain the relevant traceability information of the product. Figure 9(b) and Figure 9(c) are the schematic diagrams of consumers inputting traceability source code on the web to query product information and using mobile phone to scan QR code to query product traceability information and data storage certificate information. After the system apply in the company, compared with the traditional traceability system used before, the cost of equipment and system software has increased by 7.3% and 24.9% respectively. The system applications requires to rent multiple server equipment. The cost of developing and maintaining the system has increased to a certain extent, and the training fee for workers to learn to use software has increased slightly. In addition, the use of IoT devices to automatically upload data to the system reduces the waste of human resources and reduces labor costs by 5.3%. According to financial statistics in 2019 and 2020, the total cost of the product increased by 18.2%, and the sales revenue increased by 34.6%. Although many factors influencing the increase in sales revenue, the application of the blockchain-based traceability system guarantees the authenticity and
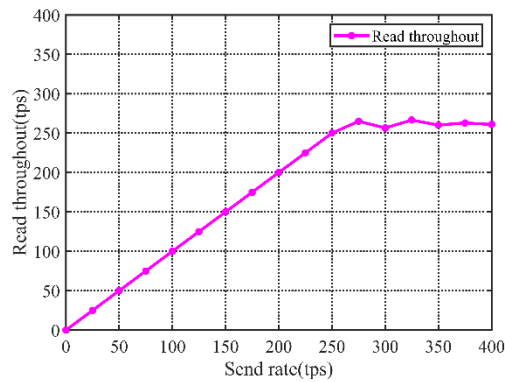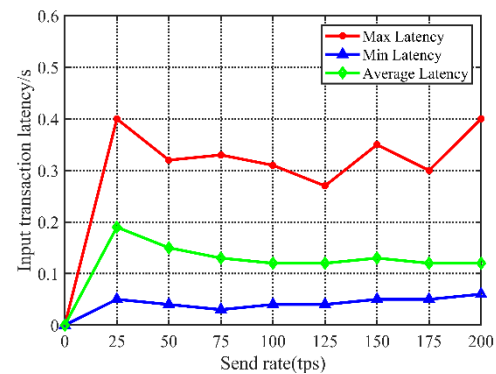
(a) Effect of the send rate on blockchain network read throughput.
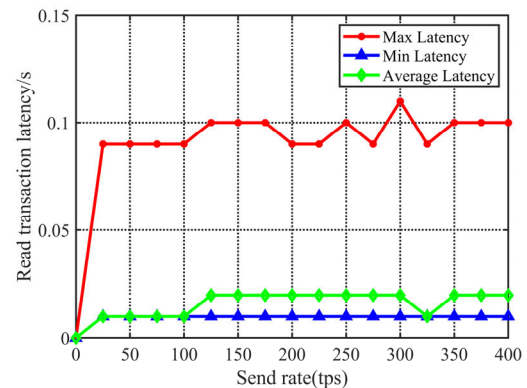
(b) Effect of the send rate on blockchain network read transaction latency.

FIGURE 7. System test results of the read request: (a) Effect of the send rate on blockchain network read throughput. (b) Effect of the send rate on blockchain network read transaction latency.
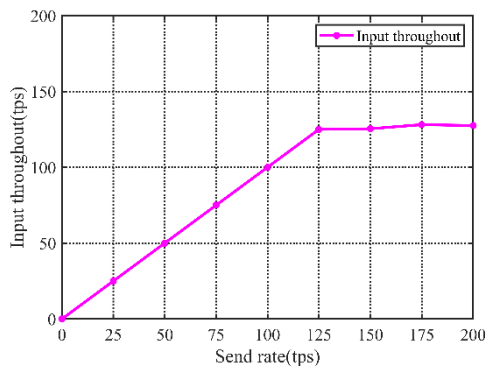
(a) Effect of the send rate on blockchain network input throughput.

(b) Effect of the send rate on blockchain network input transaction latency.

FIGURE 8. System test results of the input request: (a) Effect of the send rate on blockchain network input throughput. (b) Effect of the send rate on blockchain network input transaction latency.

TABLE 3. Comparison of traditional traceability system and blockchain-based traceability system.

Index	Traditional Traceability System	Blockchain-based Traceability System
Storage Mode	Centralization	Multicentralization
Data Sharing Scope	All participants in the supply chain	Authorized Participants
Data Transparency	Low	High
Government Supervision	Low	High
Data Credibility	Low	High
Query Rate	Fast	Medium

F. SYSTEM COMPARISON

Due to complicated links involved in the supply chain process, Table 3 compares to six aspects of the traditional apple traceability system with the blockchain-based apple traceability system in terms of storage mode, data sharing scope, data transparency, government supervision, data credibility and query rate. The traditional apple traceability system adopts centralized management. Product manufacturers,

processing manufacturers, logistics parties, sales companies, and terminal consumers of government regulatory departments are isolated from each other. They are isolated islands of information, with low transparency of data and low government supervision. Product information is easy to be tampered, and the credibility of the information is low. The blockchain-based apple traceability system adopts all links of companies and government regulatory departments as nodes to join the consortium chain. It has the characteristics of multi-centralization, does not rely on an organization or individual, and realize information transparency, ensure the integrity and accuracy of the information, and strengthen government supervision. At the same time, real-time tracking is performed to ensure the verifiability and reliability of product quality, and to solve the "trust problem" in apple supply chain management. The non-calculable modification of the data using the blockchain ensures that the traceable data cannot be tampered with, assures the credibility of the data, and has ideal application functions such as tracing the main body responsibility, tracking product flow, and sharing regulatory information, which effectively protects consumption rights. In order to solve the problem of low query rate of the blockchain, this paper proposed an on-chain and off-chain

credibility of data, which is an significant reason for winning the trust of consumers.

FIGURE 9. Product label and product information query method: (a) The tag of apple. (b) Query results of traceability code input on the web. (c) Mobile phone scan query results.

storage structure, which can alleviate the storage pressure brought to the blockchain system due to the continuous increase of data under the condition of ensuring that the data cannot be tampered, so that the query rate significantly improved.

V. CONCLUSION

In this paper, we designed and implemented the traceability system of fruits and vegetables agricultural products based on the non-tampering and traceable characteristics of blockchain, and discussed the storage and query design of the system. To overcome the problems of high data load pressure and poor private security of the blockchain traceability system as the data grows, an on-chain and off-chain data storage method using "database + blockchain" is proposed. The public information displayed to consumers is stored in the supply chain to the local database, whose hash value by SHA256 algorithm was upload to the blockchain system. The private information encrypted by the CBC encryption algorithm is stored into the blockchain for sharing with relevant companies. The storage method proposed in this paper combines the actual situation, taking into account the need for encryption of corporate private information as well as the need for public supervision of supply chain public information, and reduce the pressure of data load on the chain. By storing the block number of the public information on the database, the association between the blockchain and the database is realized. The consumer obtains the public information from the database by scanning the QR code, and the system verifies the information according to the corresponding block number stored in the database to determine whether the product information has been tampered with. With the development of blockchain, in order to meet actual business needs, multi-chain is the future development direction. For future research, we will further explore the cross-chain technology between multiple chains and a new type of consensus mechanism suitable for traceability.

REFERENCES

[1] NBSC National Bureau of Statistics of China. (2019). *National Data*. [Online]. Available: https://data.stats.gov.cn/

[2] G. Francois, V. Fabrice, and M. Didier, "Traceability of fruits and vegetables," *Phytochemistry*, vol. 173, May 2020, Art. no. 112291, doi: 10.1016/j.phytochem.2020.112291.

[3] J. Hu, X. Zhang, L. M. Moga, and M. Neculita, "Modeling and implementation of the vegetable supply chain traceability system," *Food Control*, vol. 30, no. 1, pp. 341–353, Mar. 2013, doi: 10.1016/j.foodcont.2012.06.037.

[4] W. Li, S. M. Pires, Z. Liu, X. Ma, J. Liang, Y. Jiang, J. Chen, J. Liang, S. Wang, L. Wang, Y. Wang, C. Meng, X. Huo, Z. Lan, S. Lai, C. Liu, H. Han, J. Liu, P. Fu, and Y. Guo, "Surveillance of foodborne disease outbreaks in China, 2003–2017," *Food Control*, vol. 118, Dec. 2020, Art. no. 107359, doi: 10.1016/j.foodcont.2020.107359.

[5] A. N. Desai, A. Anyoha, L. C. Madoff, and B. Lassmann, "Changing epidemiology of listeria monocytogenes outbreaks, sporadic cases, and recalls globally: A review of ProMED reports from 1996 to 2018," *Int. J. Infectious Diseases*, vol. 84, pp. 48–53, Jul. 2019, doi: 10.1016/j.ijid.2019.04.021.

[6] P. Luber, "The case of the European escherichia coli outbreak from sprouts," in *Global Safety of Fresh Produce*. Amsterdam, The Netherlands: Elsevier, 2014, pp. 356–366.

[7] *Regulation 178/2002 of the European Parliament and of the Council of 28 January 2002 Laying Down the General Principles and Requirements of Food Law, Establishing the European Food Safety Authority and Laying Down Procedures in Matters of Food Safety*, Eur. Commission, Brussels, Belgium, 2002.

[8] *Food Safety Law of the People's Republic of China, Order No. 21 of the President of the People's Republic of China C.F.R.*, Standing Committee NPC, Beijing, China, 2009.

[9] M. M. Aung and Y. S. Chang, "Traceability in a food supply chain: Safety and quality perspectives," *Food Control*, vol. 39, pp. 172–184, May 2014, doi: 10.1016/j.foodcont.2013.11.007.

[10] X. Yang, J. Qian, C. Sun, and Z. Ji, "Key technologies for establishment agricultural products and food quality safety traceability systems," *Trans. Chin. Soc. Agricult. Machinery*, vol. 45, no. 11, pp. 212–222, 2014, doi: 10.6041./j.issn.1000-1298.2014.11.033.

[11] Y. Zhang, W. Wang, L. Yan, B. Glamuzina, and X. Zhang, "Development and evaluation of an intelligent traceability system for waterless live fish transportation," *Food Control*, vol. 95, pp. 283–297, Jan. 2019, doi: 10.1016/j.foodcont.2018.08.018.

[12] F. Casino, V. Kanakaris, T. K. Dasaklis, S. Moschuris, and N. P. Rachaniotis, "Modeling food supply chain traceability based on blockchain technology," *IFAC-PapersOnLine*, vol. 52, no. 13, pp. 2728–2733, 2019, doi: 10.1016/j.ifacol.2019.11.620.

[13] L. Zhao, X. Bi, and A. Zhao, "Frame reconstruction of mobile traceability information system for fresh foods based on blockchain," *Food Sci.*, vol. 41, no. 3, pp. 314–321, 2020, doi: 10.7506/spkx1002-6630-20181119-217.

[14] K. Demestichas, N. Peppes, T. Alexakis, and E. Adamopoulou, "Blockchain in agriculture traceability systems: A review," *Appl. Sci.*, vol. 10, no. 12, p. 4113, Jun. 2020, doi: 10.3390/app10124113.

[15] X. Yang, M. Wang, D. Xu, N. Luo, and C. Sun, "Data storage and query method of agricultural products traceability information based on blockchain," *Trans. Chin. Soc. Agricult. Eng.*, vol. 35, no. 22, pp. 323–330, 2019, doi: 10.11975/j.issn.1002-6819.2019.22.038.

[16] H. Yu, B. Chen, D. Xu, X. Yang, and C. Sun, "Modeling of rice supply chain traceability information protection based on block chain," *Trans. Chin. Soc. Agricult. Machinery*, vol. 51, no. 8, pp. 328–335, 2020, doi: 10.6041./j.issn.1000-1298.2020.08.036.

[17] P. Zhu, J. Hu, Y. Zhang, and X. Li, "A blockchain based solution for medication anti-counterfeiting and traceability," *IEEE Access*, vol. 8, pp. 184256–184272, 2020, doi: 10.1109/ACCESS.2020.3029196.

[18] Y. Lu, "Blockchain and the related issues: A review of current research topics," *J. Manage. Anal.*, vol. 5, no. 4, pp. 231–255, Oct. 2018, doi: 10.1080/23270012.2018.1516523.

[19] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.

[20] Y. Lu, "The blockchain: State-of-the-art and research challenges," *J. Ind. Inf. Integr.*, vol. 15, pp. 80–90, Sep. 2019, doi: 10.1016/j.jii.2019.04.002.

[21] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congress)*, Jun. 2017, pp. 557–564.

[22] X. Li, F. Lv, F. Xiang, Z. Sun, and Z. Sun, "Research on key technologies of logistics information traceability model based on consortium chain," *IEEE Access*, vol. 8, pp. 69754–69762, 2020, doi: 10.1109/ACCESS.2020.2986220.

[23] P. Olsen and M. Borit, "How to define traceability," *Trends Food Sci. Technol.*, vol. 29, no. 2, pp. 142–150, Feb. 2013, doi: 10.1016/j.tifs.2012.10.003.

[24] J.-P. Qian, X.-T. Yang, X.-M. Wu, L. Zhao, B.-L. Fan, and B. Xing, "A traceability system incorporating 2D barcode and RFID technology for wheat flour mills," *Comput. Electron. Agricult.*, vol. 89, pp. 76–85, Nov. 2012, doi: 10.1016/j.compag.2012.08.004.

[25] D. Bumblauskas, A. Mann, B. Dugan, and J. Rittmer, "A blockchain use case in food distribution: Do you know where your food has been?" *Int. J. Inf. Manage.*, vol. 52, Jun. 2020, Art. no. 102008, doi: 10.1016/j.ijinfomgt.2019.09.004.

[26] T. Feng, "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of Things," in *Proc. Int. Conf. Service Syst. Service Manage.*, Dalian, China, 2017, pp. 1–6.

[27] Y. Liao and K. Xu, "Traceability system of agricultural product based on block-chain and application in tea quality safety management," *J. Phys., Conf. Ser.*, vol. 1288, p. 12062, Aug. 2019, doi: 10.1088/1742-6596/1288/1/012062.

[28] J. Liu, T. Yang, and W. Wang, "Traceability system using public and private blockchain," *J. Cyber Secur.*, vol. 3, no. 3, pp. 17–29, 2018, doi: 10.19363/j.cnki.cn10-1380/tn.2018.05.03.

[29] M. Li, D. Wang, X. Zeng, Q. Bai, and Y. Sun, "Food safety tracing technology based on block chain," *Food Sci.*, vol. 40, no. 3, pp. 279–285, 2019, doi: 10.7506/spkx1002-6630-20171026-299.

[30] S. K. Dwivedi, R. Amin, and S. Vollala, "Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism," *J. Inf. Secur. Appl.*, vol. 54, Oct. 2020, Art. no. 102554, doi: 10.1016/j.jisa.2020.102554.

[31] Q. Lin, H. Wang, X. Pei, and J. Wang, "Food safety traceability system based on blockchain and EPCIS," *IEEE Access*, vol. 7, pp. 20698–20707, 2019, doi: 10.1109/ACCESS.2019.2897792.

[32] K. Salah, N. Nizamuddin, R. Jayaraman, and M. Omar, "Blockchain-based soybean traceability in agricultural supply chain," *IEEE Access*, vol. 7, pp. 73295–73305, 2019, doi: 10.1109/ACCESS.2019.2918000.

[33] Y. Dong, X. Zhang, J. Xu, X. Wang, J. Kong, and P. Sun, "Blockchain-based traceability model for grains and oils whole supply chain," *Food Sci.*, vol. 41, no. 9, pp. 30–36, 2019, doi: 10.7506/spkx1002-6630-20190418-227.

[34] J. F. Galvez, J. C. Mejuto, and J. Simal-Gandara, "Future challenges on the use of blockchain for food traceability analysis," *TrAC Trends Anal. Chem.*, vol. 107, pp. 222–232, Oct. 2018, doi: 10.1016/j.trac.2018.08.011.

[35] A. Vacca, A. Di Sorbo, C. A. Visaggio, and G. Canfora, "A systematic literature review of blockchain and smart contract development: Techniques, tools, and open challenges," *J. Syst. Softw.*, vol. 174, Apr. 2021, Art. no. 110891, doi: 10.1016/j.jss.2020.110891.

[36] Y. Yuan, X. Ni, S. Zeng, and F. Wang, "Blockchain consensus algorithms: The state of the art and future trends," *Acta Automatica Sinica*, vol. 44, no. 11, pp. 2011–2022, 2018, doi: 10.16383/j.aas.2018.c180268.

XINTING YANG received the B.S. degree from Qingdao Agricultural University, Qingdao, China, in 1997, the M.S. degree from Zhejiang University, in 2000, and the Ph.D. degree from the Research Center for Eco-Environmental Sciences, Chinese Academy of Sciences, China, in 2008. In July 2000, he worked with the Beijing Agricultural Information Technology Research Center and successively served as a Research Intern, an Assistant Researcher, an Associate Researcher, and a Researcher, where he has been the Deputy Director, since 2012. His research interests include blockchain, agricultural traceability, and machine learning.

MENGQI LI received the B.S. degree in network engineering from Anhui Sanlian University, Anhui, China, in 2018. She is currently pursuing the M.S. degree with Shanghai Ocean University. Her research interests include blockchain, cryptography, and agricultural traceability.

HUAJING YU received the B.S. degree in software engineering from the Jiangsu University of Science and Technology, Jiangsu, China, in 2019. He is currently pursuing the M.S. degree with Shanghai Ocean University. His research interests include blockchain and smart contract.

DAMING XU received the B.S. and M.S. degrees from the Taiyuan Institute of Technology, Shanxi, China, in 2013, and the M.S. degree from the Taiyuan University of Technology, in 2016. In July 2016, he worked with the Beijing Agricultural Information Technology Research Center, where he successively served as an Engineer. His research interests include blockchain and agricultural traceability.

MINGTING WANG received the B.S. degree in electronic information science and technology from Fuyang Normal University, Anhui, China, in 2017, and the M.S. degree from Shanghai Ocean University, Shanghai, China, in 2020. Her current research interests include blockchain and consensus mechanism.

CHUANHENG SUN received the B.S. degree from Qingdao Agricultural University, Qingdao, China, in 2002, the M.S. degree from Zhejiang University, in 2005, and the Ph.D. degree from China Agricultural University, Beijing, China, in 2012. In July 2005, he worked with the Beijing Agricultural Information Technology Research Center, where he successively served as a Research Intern, an Assistant Researcher, an Associate Researcher, and a Researcher. His research interests include blockchain, agricultural product identification, and agricultural traceability.

• • •