Hindawi
Security and Communication Networks
Volume 2021, Article ID 3298514, 12 pages
https://doi.org/10.1155/2021/3298514

Research Article

A Research on Traceability Technology of Agricultural Products Supply Chain Based on Blockchain and IPFS

Lejun Zhang,[1,2] **Weimin Zeng**,[1] **Zilong Jin**,[3] **Yansen Su**,[4] **and Huiling Chen**[5]

[1]*College of Information Engineering, Yangzhou University, Yangzhou 225127, China*
[2]*Cyberspace Institute Advanced Technology, Guangzhou University, Guangzhou 510006, China*
[3]*School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing 21004, China*
[4]*Key Laboratory of Intelligent Computing and Signal Processing of Ministry of Education, School of Computer Science and Technology, Anhui University, Hefei 230601, China*
[5]*Department of Computer Science and Artificial Intelligence, Wenzhou University, Wenzhou 325035, China*

Correspondence should be addressed to Lejun Zhang; zhanglejun@yzu.edu.cn

Received 10 August 2021; Revised 22 October 2021; Accepted 27 October 2021; Published 12 November 2021

Academic Editor: Xiu-Bo Chen

Blockchain technology, the fundamental technology of Bitcoin, is featured with high transparency, decentralization, traceability, tamperproof nature, and anonymousness. In this thesis, a case study of the traceability of agricultural products is to explain a traceability solution of agricultural products supply chain based on blockchain and IPFS. The latter one is used to store large quantities of transactions data; and the former one is used for the safety of data storage and circulation. And consumers can know the quality of agricultural products in the shortest time through the evaluation function. As shown in the experiment, the solution is more efficient and secure compared with existing supply chain traceability methods, meeting the traceability requirements of security, transparency, and reliability. Furthermore, the traceability, safety, and performance of the scheme are also analyzed here.

1. Introduction

The consumption market in China is facing a brand new era of traceability, and product traceability has become a hot issue concerned by the society. Food security has become an escalating concern in the society. Even though national traceability standards for major products have been formulated by the government, incidents of counterfeit and inferior products often occur in the market. Thus, a series of food security problems have triggered the consumer trust crisis, which is also a major challenge to the efforts made in the progress of the national development of a credible society [1]. The food traceability system can identify the source of food and detail the whole process from food production to dining tables. In case of any food security and quality problem, it can quickly locate the key link of the problem and identify the subject of responsibility to contain the problem from worsening, which provides an effective way to solve the food security problems.

The analysis of the current food information storage platforms and supply chains reveals that the current food traceability system is deficient with the following defects: It highly relies on centralized databases, exposing a hidden hazard of information tampering to many key links, such as storage, presentation, and maintenance of data[2]; The phenomenon of "information silo" undermines the current supply chains, as the internal systems of the entities possess most of the information. While the lateral interconnection between the systems is insufficient which makes it difficult to realize the linkage regulation, in the whole circulation process from food production to consumer consumption, the extent and efficiency of automation are insufficiently low in the links of food processing, warehousing, logistics, etc. With broad application of 5 G technology, the demand for data storage is surging sharply, and the market is facing

overwhelming pressure with larger scales of data storage requirements. The emergence of IPFS is right on time. The *Notice of the General Office of the National Radio and Television Administration on Issuing: A Series of White Papers on the Application of Blockchain Technology* has repeatedly mentioned the distributed storage of IPFS and blockchain, affirming the application value and technical advantages of IPFS. The blockchain technology can magnify the function of IPFS, while IPFS can overcome the data storage constraints of blockchain. The combination of the two technologies is the trend of food traceability development in the future. In this thesis, grain traceability, as an example, is introduced to demonstrate the real-time monitoring of the supply chain, in which case effective tracing of grains and traceability of business transactions of agricultural products in the supply chain are realized by virtue of smart contracts deployed in the blockchain, in a bid to carry out real-time monitoring of the supply chain and improve transparency, and we call it Bc-IPFS.

The main contributions can be summarized as follows:

(i) Combine blockchain technology and IPFS technology. The details of transactions are stored in IPFS and the hash is stored in the blockchain, which cannot only ensure data security and effectively overcome the shortcoming of constrained data storage capacity of blockchain.

(ii) Discuss the sequence of interaction and relations between major participants, the solution, and the key points resolved.

(iii) Propose the transaction assessment function and make the consumer information and purchased products private.

(iv) Deploy smart contracts based on Hyperledger to realize traceability of the food supply chain and verify the feasibility by the throughput capacity test and delay test.

2. Relevant Work

With the development of the blockchain technology, the unique decentralization, traceability, and tamperproof nature of blockchain have been promoting the transition from traditional traceability to blockchain traceability [3]. More and more scholars start to study blockchain-based food supply chain traceability. Yu and Huang [4] put forth the traceability solution for broiler chickens by combining the blockchain technology and RFID technology. With the solution, smart devices can be used to scan the traceable QR code on the chicken claw ring to retrieve the corresponding data and information, where the chicken claw ring is designed into an "inverted tooth" shape to prevent its secondary use. Tian et al. [5] developed an agricultural food supply chain traceability system, covering the whole process of data acquisition and information management of all links of the entire supply chain. The RFID technology is adopted to realize data acquisition, data circulation, and data sharing, and the blockchain technology is adopted to ensure data reliability. However, the RFID technology is deficient in high costs, such as the equipment costs of RFID transmitters, readers, and antennas. Besides, the availability of RFID frequency bands is varied in different countries. RFID is prone to inciting privacy leakage and other problems, and RFID can be easily impacted in an environment containing metal and moisture; thus RFID cannot be broadly utilized in large scale. Afterwards, Tian [6] proposed the food supply chain traceability based on hazard analysis and key control points (HACCP) by adoption of blockchain and Internet of things. Highly similar to the application scenario of [5], it adopts RFID for data acquisition, blockchain technology for ensuring data security, HACCP for monitoring and tracing of supply chains, and BigchainDB for storage and management of food supply chains data. However, on the one hand, BigchainDB is still exposed to the deficiency of RFID, and, on the other hand, it is not ideal for file storage, but for the structural data. Yang et al. [7] used Hyperledger as the traceability chain to store information in the local database, which is useful in solving the problem of blockchain deficiency in massive data storage. However, it is disadvantageous in high cost, slow data transition rate, low security, etc., in comparison with data storage by IPFS. Further, it does not provide the consumer with feedback function, so retailers cannot get access to product security and other aspects in the first time. Xie et al. [8] utilized the IoT technology to carry out ETH-based tracing of agricultural products, ensuring that data will not be maliciously tampered or damaged. However, on the data storage layer, data storage is blockchain-based; thus the network overheads will become increasingly greater with the increase of data volume. Hao et al. [9] researched the traceability storage solution based on the blockchain technology, which stores the crop growth information in IPFS and provides analysis of crop growth data by virtue of the auxiliary database. Although the solution overcomes the data storage constraint of blockchain, the focus of the system is on the acquisition of crop growth information, and thus the solution is not favorable to the information tracing subsequent to crop processing. Besides, the traceability of agricultural product supply chains includes the crop growth information and also the data and information subsequent to crop processing; thus traceability becomes a zero-distance shortcut from farmlands to dining tables. Salah et al. [10] researched the business transaction implementation method relying on ETH-based smart contract, in order to realize the traceability and transparency of soybean supply chain. However, due to the lack of consumer feedback function, retailers cannot gain access to safety problems in the first time after food is sold to consumers, and ETH involves data exploiting processes which consume time and resources.

With the development of blockchain 2.0, smart contract has been widely applied, and this thesis discusses the realization of traceability function automation and the introduction of the consumer feedback function based on the smart contract deployed on the blockchain. It is intended that, in case of any agricultural product security problem, entities in the supply chains may respond in the first time.

3. A Agricultural Product Supply Chain Traceability Solution Based on Bc-IPFS

In terms of the traceability of agricultural product supply chains, there are high requirements for the backup of transaction data. The IPFS storage technology is to separate a file into many pieces scattered on different locations of the network, which provides more powerful backup capacity compared with cloud storage. The blockchain technology can ensure the integrity of the data stored in IPFS, which is ideal for the traceability of agricultural product supply chains. Thus, in this section, we use the Hyperledger to trace and implement the transactions in the agricultural product supply chains by deployment of smart contracts of chaincode and store transaction information in IPFS to effectively reduce the reliance on the centralized database. Store the hash in the blockchain to take advantage of the features of blockchain to provide secure and reliable transaction records for the management of supply chains and thus ensure the information authenticity and reliability of the agricultural product acquired by the consumers.

3.1. Schematic Design. The unique feature of the solution is that it adopts the blockchain as the foundation layer, allows transactions between mutually untrusted users through smart contract, and adopts the IPFS technology to resolve the data storage constraint of blockchain. Within a certain period after the closure of a transaction, the consumer may use the ring signature algorithm to carry out anonymous assessment on the retailer. Relevant regulatory authorities or product suppliers may determine the quality security problems of a certain batch of products in the first time through consumer feedback. The batch information of the product purchased by the consumer can be used to identify the specific product batch, and the smart contract can be used to trace the root cause.

In this thesis, we propose the deployment of smart contract on Hyperledger, which can automatically send the preset data resources (including the triggering condition event) according to the contract information agreed in the smart contract when the triggering condition is met. Once the smart contract is deployed, it cannot be changed but can be upgraded to launch new functions or fix bugs [11]. The Fabric smart contract is independent of the underlying ledger, and it is not required to relocate the ledger data to the new smart contract when the smart contract is upgraded, which truly realizes the separation between logic and data. The smart contract of Fabric is referred to as chaincode, including system chaincode and user chaincode [12]. System chaincode is used to realize system-level functions and the processing logics of Fabric nodes, including system configuration, endorsement, and verification [13, 14]. User chaincode operates in an isolated chaincode container and is responsible for the user's application function, providing status processing logics based on the distributed blockchain ledger. It is programed by application developers as a support to upper-level services. Smart contract receives transactions and triggers events in the form of function call, so that a participating entity can constantly monitor the events being sent in blockchain without too many expenses [15].

Figure 1 shows the traceability of agricultural products. The Hyperledger smart contract is adopted to record information, and all participants involved in the supply chain are added to the processes, which are used to trace the agricultural products from the place of origin to the end consumers in a digital manner. The supervisory and regulatory bodies or relevant government departments deploy the main smart contract which provides an interface to the entities in the supply chain for function call and transaction implementation. IPFS hash files are stored in blockchain, which can be processed within the specified time period if the product conforms to the buyer's requirements. Supervisory and regulatory bodies almost deal with the entire supply chain. For instance, the agricultural bureau may carry out supervision, recording and management of farmer information, seed information, product information, etc., to ensure information authenticity. The quality supervision bureau must carry out supervision, management, and recording of processing plant information, retailer information, and product quality information and ensure security and quality of agricultural products. In order to improve the storage capacity, the information of all products and the data of all transactions and events are stored in IPFS, and the blockchain is only used to store the hash value of the data. IPFS is designed for distributed storage, which can be combined with Hyperledger to improve its throughput. The formula symbol description is shown in Table 1. Each transaction (TX_{tr}) bears the product identifier (ID_{pro}), product data hash (H_{pro}), identifier (ID_{own}) of the product owner and its signature (Sig_{own}), and public key (PK_{own})

$$\begin{cases} TX_{tr} = \left[ID_{\text{pro}} || H_{\text{pro}} || ID_{\text{own}} || Sig_{\text{own}} || Pk_{\text{own}}\right], \\ H_{\text{pro}} = \left[P_{\text{typ}} || P_{\text{quan}} || P_{\text{pri}} || P_{\text{ori}}\right]. \end{cases} \tag{1}$$

TX_{tr} is stored in IPFS and hash is stored in blockchain. The product hash (H_{pro}) includes the product type (P_{typ}), quantity (P_{quan}), price (P_{pri}), and place of origin (P_{ori}). When a product is confirmed to have been delivered from the seller to the buyer in a transaction, $Tx_{tr} = [ID_{pro}||H_{pro}||ID_{buy}||Sig_{buy}||PK_{buy}||Sig_{sell}||Pk_{sell}]$, where ID_{buy}, Sig_{buy}, and PK_{buy} represent the identifier, signature, and public key of the owner, respectively;

$$TXtr = \left[ID_{\text{pro}} || H_{\text{pro}} || ID_{\text{buy}} || \text{Sig}_{\text{buy}} || Pk_{\text{buy}} || \text{Sig}_{\text{sell}} || Pk_{\text{sell}}\right]. \tag{2}$$

ID_{buy}, Sig_{sell} , and PK_{sell} represent the identifier, signature, and public key of the seller, that is, the signature (Sig_{own}) and public key (PK_{own}) of the product owner in (1). The identity is required to be transformed in the process of product transaction, the owner of a transaction will be the seller in a subsequent transaction, and the buyer will become the owner of the product when the transaction is complete. After the consumer buys the product from the retailer, the seller creates the transaction order m_R

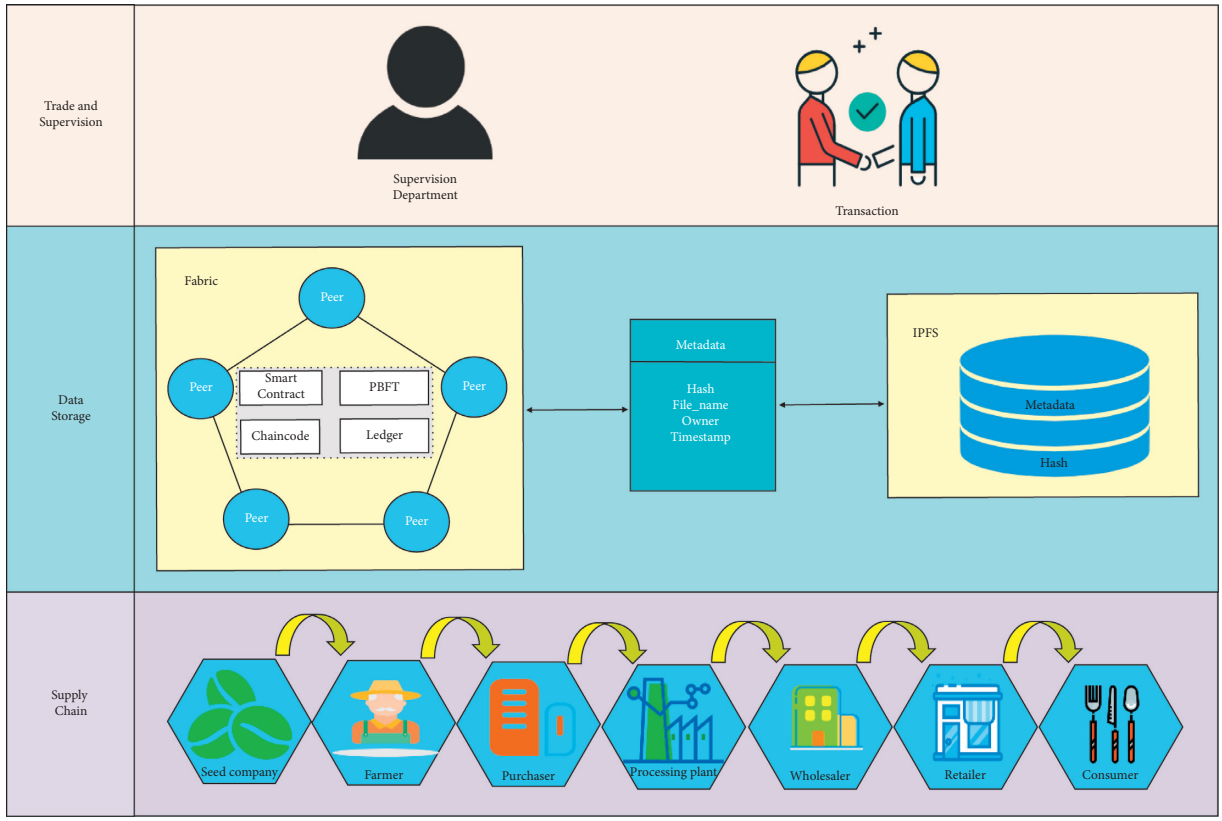

Figure 1: Agricultural product supply chain traceability solution based on Bc-IPFS.

Table 1: Symbol meaning.

Symbol	Meaning
ID	Identifier
H	Hash
Sig	User signature
PK	Public key
SK	Private key
m_R	Transaction order
$\|\|$	Connection symbol
ς	Ring signature
$Info$	Assessment information
$Value_{trust}$	Trust value
$Total_{trans}$	Total number of transactions

$$m_R = \Phi\left(m_t, \varsigma\left(SK_{\text{sell}}, m_t\right)\right). \tag{3}$$

Only after obtaining the completed order m_R, can the consumer release a comment on the product. Firstly, the consumer verifies the transaction signature $\varsigma(SK_{\text{buy}}, m_t)$ of the retailer

$$\Phi\left(mt, PK_{\text{sell}}, \varsigma\left(SK_{\text{sell}}, mt\right)\right) = 1. \tag{4}$$

Then, he/she verifies the seller's signature based on the seller's public key. Secondly, the consumer creates the ring signature ς based on the assessment information $\text{Info} = [ID_{\text{pro}}||H_{\text{pro}}||P_{\text{sco}}||P_{\text{txt}}]$ and sends the $(\text{Info}, \varsigma, m_R)$ to the blockchain. The blockchain verifies m_R and ς, and, upon successful verification, Info will be stored in IPFS, and H_{Info} will be stored in the blockchain network. In addition, the trust value

$$\text{Value}_{\text{trust}} = \frac{\sum\left(\alpha \cdot \text{score}_{\text{ser}} + \beta \cdot \text{score}_{\text{qual}}\right)}{\text{Total}_{\text{trans}}}, \quad \text{Total}_{\text{trans}} \geq n, \tag{5}$$

can be calculated through consumers' evaluation of goods ($score_{ser}$), including service score and product quality score for retailers ($score_{qual}$), where the coefficient is $\alpha + \beta = 1 \vee \alpha, \beta \in (0, 1)$ and n refers to the number of transactions; even if individual consumers conduct malicious evaluation, the behavior will still have slight impact on the overall evaluation score, effectively reducing the negative effect of malicious evaluation on retailers [16, 17]. The total number of transactions must have at least n successful orders before the trust value is recognized, which can effectively protect new businesses from malicious comments at the initial stage. At the same time, only the first score of each natural month is valid for each user, thus avoiding malicious comments [18].

3.1.1. Data Storage/Query. Any data created from a transaction between both parties will be stored. As shown in Figure 2, first, the data will be sent by the http-post method, and when the predefined block size is achieved, the data will be partitioned, packed, and stored in IPFS, and the address of the IPFS storage block will be acquired. Then, the address will be stored in the Fabric blockchain, and the Fabric

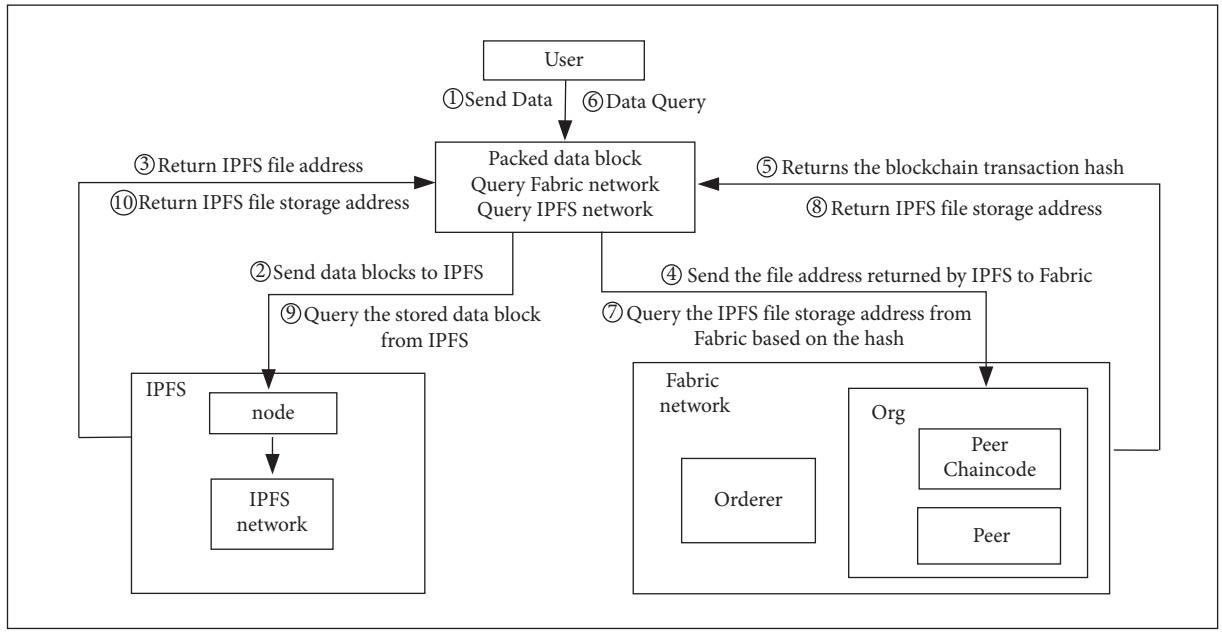

Figure 2: Functional design of data storage and query.

chaincode will be called to store the information in the peer node ledger for preservation. Upon data query, the http-get method will be adopted for data request, Fabric chain will be initiated to check whether the chaincode includes the IPFS address, and the transaction data will be retrieved from IPFS according to the hash address of the corresponding data block file on IPFS.

IPFS stores the data blocks of all source data, and the storage of data blocks is not subject to any sequence, but each data block is specifically correlated to the corresponding hash address, and the mapping relations between hash addresses and detail information is stored in the Fabric blockchain.

Nowadays, many problems of cloud storage resulted from improper server management and maintenance provided by decentralized cloud service providers or excessively centralized distribution of cloud service providers. If a file is stored in the cloud hard disks provided by the cloud service provider, and if the hard disks are put together in a centralized manner, even if the file is provided with the corresponding backup file, the hard disk in which the backup file is located may be stored in the hard disk in which the original file is located. As a result, the servers malfunction in case of power outage or other failures happens, and it cannot be accessed externally; the only way to the problem is to wait for recovery of the servers. But IPFS is not limited, as IPFS is a new type of Internet technology comparative to the HTTP protocol, solving the data storage and distribution problems, and it is designed to create permanent and decentralized storage and file-sharing methods through peer-to-peer network (PPN), with the concept of separating a file into many pieces scattered on different locations of the network, which can be acquired simultaneously from multiple servers upon downloading of the file. Even if certain servers are malfunctioning, it will not create adverse influence on the access of external users to the entire network, nor on the users' data acquisition. In addition, even if certain node data is completely lost due to improper operation, there are many backups on the entire network. The advantages of IPFS are ideal to tackle the shortcomings of traditional centralized cloud storage, e.g., vulnerability to data leakage, vulnerability to hardware damage, and poor repair capacity.

In order to achieve large-scale distributed storage, there are three problems that need to be handled: (1) How to increase storage capacity, that is, to attract more users to provide storage resources, (2) how to improve retrieval efficiency and achieve rapid service response, and (3) how to guarantee that data storage and circulation are safe. In response to that, the researchers introduced blockchain technology as the incentive layer for distributed storage and obtained a series of research results. The most representative solution is a distributed storage system based on IPFS.

The storage party can prove its effective storage capacity through the proof of storage mechanism (Proof of Storage) to obtain tokens (the first problem) [19, 20]. Retrieval service parties can provide data retrieval services, and efficient retrieval can obtain more tokens (the second problem). The data security can be solved by encryption technology, and the blockchain can provide evidence of data access.

3.1.2. Relationship between Entity Sequences. As shown in Figure 3, the relationship between entities shows some key properties and functions of smart contract. The relationship between entities and smart contract is shown in Figure 3. Each participating entity in the supply chain participates by invoking the functions in the smart contract. Therefore, the metadata and relationships are of great importance to the realization of the smart contract [21]. The regulatory authority creates a master smart contract to be invoked by

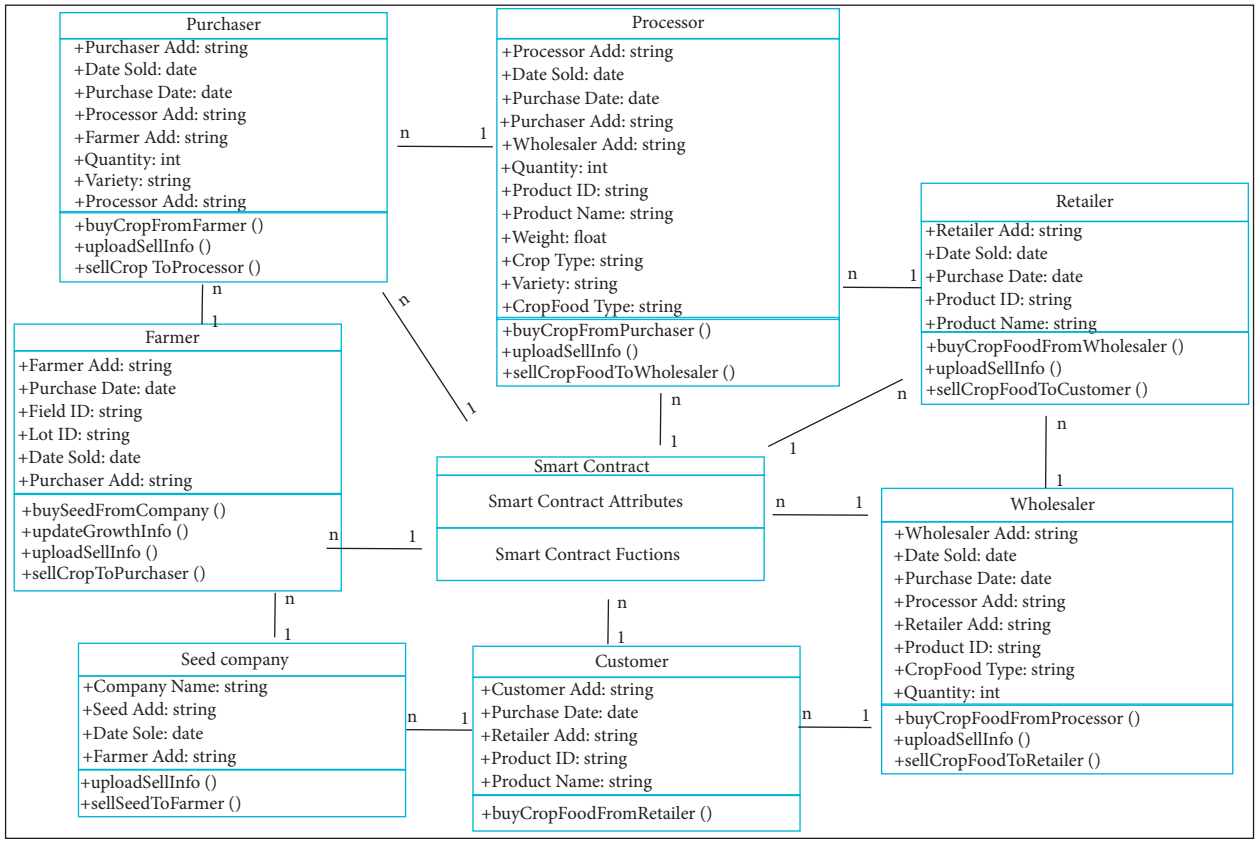

Figure 3: Entity relationship chart.

other entities. If certain changes happen to the relationship between the buyer and the seller, the corresponding contract will be executed. Once the parties have agreed on the details of the agreement, the transaction can proceed.

3.1.3. Algorithm. As mentioned above, the relevant supervision departments deploy the master smart contract, and each entity can invoke the trade through the interface. In the initialization state, each transaction entity needs to be registered; otherwise the transaction cannot be carried out. Later, the process of user registration, transaction, and product evaluation will be described in detail. Table 2 shows the interpretation of the variables in the algorithm.

3.2. User Registration. Algorithm 1: when users register their identities, the input parameters include ID_{user}, V_{IDuser}, *User_address*, and Pk_{user}. The algorithm is used for user registration, and the necessary user information is stored in the blockchain. Unregistered users cannot participate in the transaction. After the user registration verification is passed, the regulatory agencies call the smart contract interface node_register() to store user information in the blockchain.

3.3. Goods Registration. Algorithm 2: firstly, the goods owner registers the products so that the buyer can view the information of the goods he/she needs to buy and input the information of the goods to save, which plays a vital role in traceability. The goods owner enters ID_{pro}, *Pro_Lot*, P_{typ}, P_{quan}, V_{IDpro}, ID_{own}, and PK_{own}.

3.3.1. Commodity Transaction. Algorithm 3 is jointly implemented by the buyer and the seller. Both parties negotiate P_{pri}, P_{quan}, and P_{qual} requirements of the goods. After reaching an agreement, the buyer pays for the goods *Pay_pri*. At the same time, the seller submits the deposit *Fine*, which is one half of the commodity transaction price λ, $\lambda \in (0, 1)$. The value of λ is decided by both parties, i.e.,

$$\text{Fine} = \lambda \cdot \text{Pay\_pri}, \quad \lambda \in (0, 1), \tag{6}$$

$$\text{Pay\_pri} = P_{\text{pri}} \times P_{\text{quan}} \& \text{Fine} = \lambda \cdot \text{Pay\_pri}. \tag{7}$$

When formula (7) is satisfied, the smart contract triggers the function Sell_agree(). After the buyer confirms the receipt of the goods and the loan, the smart contract triggers Pay_agree() to pay the loan and deposit to the seller. If the buyer does not confirm the loan and there is no dispute, the transaction is considered to be successful within seven days, and the payment and deposit are also paid to the seller. When the transaction is done successfully, the smart contract calls Trans_Record() to record *address_buyer* and *address_seller*, as well as the information of the traded goods. If the buyer has disputes on the goods and does not agree to pay or the buyer has disputes over the goods within seven days, the Dispute_event() will be triggered and should be

Table 2: Contract function description.

Function	Description
node_register()	Only the supervisory authority can call users whose registration has been successfully verified
node_record()	Only the supervisory authority can call it to record the object that this batch of goods belongs to at the time
release_pro()	This is used to release the information of the batch of goods
Trans_Record()	This is used to record transactions
Dispute_event()	Arbitrators or third-party agencies handle transaction disputes
Signature()	This is used for evaluation signature
Storage()	This is used to store records
Credit()	This is used to update reputation value

Input: ID_{user}, V_{IDuser}, *User_address*, PK_{user}
Output: Registration result
(1) Users send ID_{user}, V_{IDuser}, *User_address* and PK_{user} to regulatory agencies
(2) Regulatory agencies verify users' identity information
(3) **if** the verification is successful **then**
(4) Regulatory agencies call node_register (*User_address*, PK_{user})//Only the regulatory agencies can call, register the user with successful verification, and send the relationship of *User_address* and PK_{user} into address_pk.
(5) Update address_pk
(6) return "successfully registration"
(7) **else**
(8) **return** "registration failed. Please submit the real information to register again."
(9) **end if**

Algorithm 1: User registration algorithm.

Input: ID_{pro}, *Pro_Lot*, P_{typ}, P_{quan}, V_{IDpro}, ID_{own}, PK_{own},
Output: Registration result
(1) Goods owner upload ID_{pro}, *Pro_Lot*, P_{typ}, V_{IDpro}, ID_{own} onto the IPFS
(2) Goods owner sends H_{pro}, V_{IDpro}, PK_{own} to regulatory authorities
(3) Regulatory agencies verify the owner of the goods
(4) **if** the verification is successful **then**
(5) Regulatory agencies call node_record (ID_{pro}, ID_{own}, *Pro_Lot*, *Time*)//It can only be called by regulatory agencies to record the owner of the commodity batch at that time
(6) **return** "successful registration" **then**
(7) Goods owner invokes release_pro (ID_{pro}, *Pro_Lot*, P_{typ}, P_{quan})//The goods are successfully registered by the owner, Later, the information of this batch of goods can be released for buyers to choose.
(8) **else**
(9) **return** "failed verification, please submit the information again"
(10) **end if**

Algorithm 2: Goods registration algorithm.

handled by an arbitrator or a third-party organization. The place where the commodity is sold should be recorded for a single completed transaction, so that the commodity circulation record can be checked. In other words, both the buyer's and the seller's user address should be recorded in the transaction records, and these two addresses refer to the addresses registered in Algorithm 1.

3.4. Consumer Evaluation. In Algorithm 4, consumers can score the product and service quality of this transaction after an order completed and then upload such evaluation to IPFS.

4. Theory and Experiment Analysis

In this section, we analyze the traceability, security, and performance of the plan and make qualitative analysis by comparing this thesis with other papers at last.

4.1. Traceability Analysis. In this thesis, the solution of grain traceability of information is stored in IPFS files based on Hyperledger through chaincode (smart contract), in which transaction data is uploaded to IPFS to effectively solve the potential dangers such as high cost, waste of broadband, short text storage time, dependence on backbone network,

Input: ID_{buyer}, ID_{seller}, *address_buyer, address_seller,* P_{pri}, P_{quan}, P_{quab} *Fine*
Output: Transaction result
(1) The seller applies smart contract function: negotiate (ID_{buyer}, ID_{seller}, P_{pri}, P_{quan}, P_{qual})//Both parties can negotiate the commodity price, quantity and quality through this function.
(2) **if** $Pay\_pri = P_{pri} \times P_{quan} || Fine = \lambda \cdot Pay\_pri$ **then**
(3) Contract status becomes Sell_agree
(4) **if** Confirm receipt or time stamp > deadline **then**
(5) Apply smart contract function: Trans_Record (*payment, address_buyer, address_seller*)
(6) **else**
(7) Trigger the contract event: Dispute_event (ID_{buyer}, ID_{seller}, P_{pri}, P_{quan}, P_{quab}, *Fine*)
(8) **end if**
(9) **else**
(10) Contract status becomes Sell_disagree
(11) **return** ("transaction failed")
(12) **end if**

Algorithm 3: Commodity trading algorithm.

Input: ID_{seller}, m_R,$\varsigma(SK_{\text{buy}}, m_t)$, PK_{sell},ς, *Info*
Output: Evaluation agency verification results
(1) The seller applies evaluation contract function: comment (m_R, $\varsigma(SK_{\text{buy}}, m_t)$, PK_{sell})
(2) **if** $\Phi(m_t, PK_{\text{sell}}, \varsigma(SK_{\text{sell}}, m_t)) = 1$ **then**
(3) Apply signature function: signature (Info, ς, m_R)
(4) **If** block verification passed **then**
(5) Trigger contract storage function: storage (*Info,* H_{Info})
(6) Trigger contract credit update function: credit (ID_{seller}, $Value_{trust}$)
(7) **else**
(8) **return** ("verification failed")
(9) **end if**
(10) **else**
(11) **return** ("No review permission")
(12) **end if**

Algorithm 4: Consumer evaluation algorithm.

DDOS, XSS, and CSRF attack[22–25]. Meanwhile, combined with blockchain technology, it makes hash stored in blockchain to solve the limited data storage in blockchain efficiently and keep data stored safe and not tampered [26–28]. The information of each transaction involves the previous owner's information before and after the transaction. The unique identifier and batch number of the grain are added to each subsequent transaction to form a complete traceability chain. When consumers give negative evaluation to the quality and safety of commodity, the regulatory authorities and retailers can trace the source quickly according to the relevant product batches in the evaluation, determine the production batches of the products, and locate the product batches for inspection in time. Consumers can also screen and select suitable purchase objects based on the retailer's reputation value and product evaluation [29].

As shown in Figure 4, the access query records for the uploaded file are displayed. Each record contains the hash value, owner name, visitor, and time stamp of the accessed file.

4.2. Security Analysis

Unforgeability: distributed storage of data is allowed in IPFS, and the data will not be tampered and forged. The data stored in IPFS network cannot be altered without changing the data identifier. In IPFS, the identifier is an encrypted data hash [30]. It means that if the identifier of data is stored in the underlying distributed general ledger, noncritical data can be stored in IPFS. This can cut down consumption of operation in distributed ledger. Compared with centralized storage, if a hacker intercepts the request from hash and tries to send a malicious phishing site, the user can, with the help of data received through running hash function, compare the hash value of the data received with the one requested and reject the received data if not matched.

Consumer privacy: consumers make an evaluation through ring signature after obtaining m_R. The ring signature is anonymous, so attackers are not sure which ring member generates the signature. The probability is lower than $1/n$ even if the private key of ring member is acquired.

```
"File1":{"accessor":"33k5b3zd3CbhRnV8Qh7bYK9c4QGkp1VBcbXFSLsyce1aGT",
"filehash":"31Ra4FtkfZqD5EhpSeERAj4vy3LSkihKtLAH98SYRw9nRu",
"owner":"pikachu",
"time":"2021-10-13 14:18:34"},

"File2":{"accessor":"33WwsymTS93LbMWAbJYfE9LQnqwuRsN63E5iVpRN6PyMZA",
"filehash":"25qowBS4a8gjqMLm7FYhM6pRogy2T7TZc6gpxmpyqWPGqf",
"owner":"pikachu",
"time":"2021-10-13 14:21:12"},

"File3":{"accessor":"33Y3Vv4cVS4hTiyqyxfx3eX9BLQtR4NFojoC4Ct5MLjpd7",
"filehash":"21Ew3urZVj37WrPaiVdmnuJNsZgiMMYCLbFwSAPwQEhLAD",
"owner":"pikachu",
"time":"2021-10-13 14:27:37"},

"File4":{"accessor":"2xtBLHejVEeBBUCYFknxSvMnAarkNRqkFsZeybZtDsgrAA",
"filehash":"2z3hc1bDddRb1bMSDprzsZG25Zrq8JTJU7MxWH1L7WLVdr",
"owner":"pikachu",
"time":"2021-10-13 14:35:42"},

"File5":{"accessor":"27F3PRTbRAe7aX1BMQqdMB4uiYAACvaizFDKwmMtyVw4Jh",
"filehash":"272uTJpWcuZ4LxvonDKnwFPPpLcaB6MjqpAg6WuTYYAmBz",
"owner":"pikachu",
"time":"2021-10-13 14:43:26"},
```


Figure 4: On-chain metadata for accessing files.

Transparency: both the consumer evaluation and the credit value of retailers are open to the public. Other consumers can screen these contents during commodity purchase. Meanwhile, the credit value can only be shown by setting a certain amount of turnover, effectively lowering the negative effect due to malicious evaluation from malicious consumers.

4.3. Experimental Results and Analysis. The test is done under the circumstance of Ubuntu 20.04 LTS on a computer equipped with Intel(R) Core(TM) i7-10750H CPU @ 2.60 GHz, running memory of 64 G, 1T mechanical hard disk, and 500 GB solid state hard disk. Ubuntu is built in mechanical hard disk. Generate a local IPFS node and obtain its public ID, create an IPFS network, and embed it in the Fabric blockchain, Hyperledger Caliper, an open source blockchain performance evaluation tool, is used to test transaction throughput and delay, and the test results are shown in Figures 5 and 6.

As shown in Figure 5, the query transaction and the R/W transaction show a bottleneck at the throughput of 25 tps and 22 tps, respectively. In case of low transaction rate, the submitted transaction must wait. Furthermore, transactions are continuously sent through the client, and it will show low delay of subsequent transactions received in each block timeout period, as shown in Figure 6. When the transaction rate is 10 tps, the query delay drops to about 0.75 tps, and if the transaction rate exceeds the maximum throughput, the accumulated transactions will show higher delay. Therefore, the delay continues to increase after the transaction rate exceeds 20 tps. The performance is related to network delay, consensus delay, chaincode execution time, block

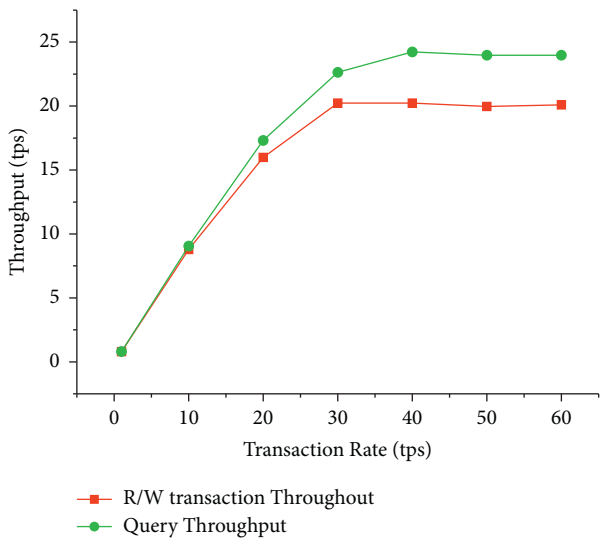

Figure 5: Transaction throughput.

verification delay, and other factors, but the system's throughput always has linear relation to the number of channels [31].

Since adding blockchain to IPFS will result in additional consumption of computing resources and time, thus this solution measures the performance variations of file reading when blockchain is adopted and when blockchain is not adopted. Thus, five files with the sizes of 0.5 T to 2.5 T are selected and uploaded to Ubuntu 20.04 LTS, data reading is conducted with the computers in the same network (Windows 10 , Intel(R) Core(TM) i7-4720HQ CPU @ 2.60 GHz, 12 GB RAM, and 500 GB Hard Disk), and the test results are shown in Figure 7. In the circumstance where

Figure 6: Transaction delay.

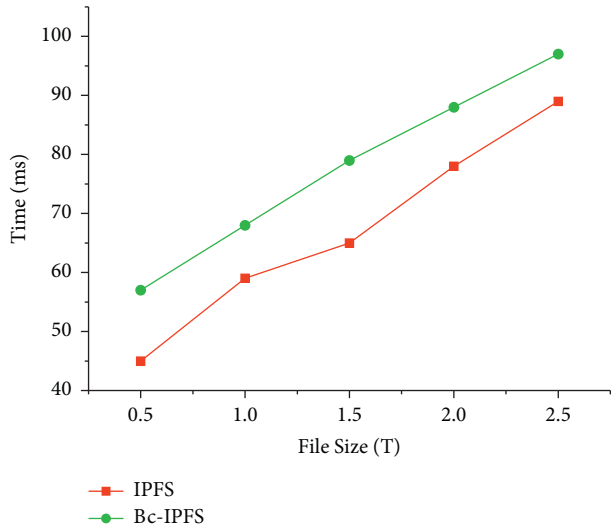

Figure 7: Compare the file read performance difference between IPFS and Bc-IPFS.

blockchain is adopted, the file reading is slightly lower than that of ordinary IPFS, as a blockchain transaction relies on the completion of IPFS processes, and the transaction time may also be adversely influenced by the local network speed and computer operation capacity. However, regardless of the sizes of the files added to IPFS, the sizes of the metadata stored on the blockchain do not show any signs of evident changes, as shown in Figure 8.

4.4. Scheme Comparison. First of all, Hyperledger is a private blockchain technology, distinctive from the blockchain technology such as ETH and Bitcoin, and the members of a blockchain network are known to each other, and the membership is available to the public, allowing new members to join in and carry out transactions on the network [32]. Hyperledger is a type of blockchain managed by

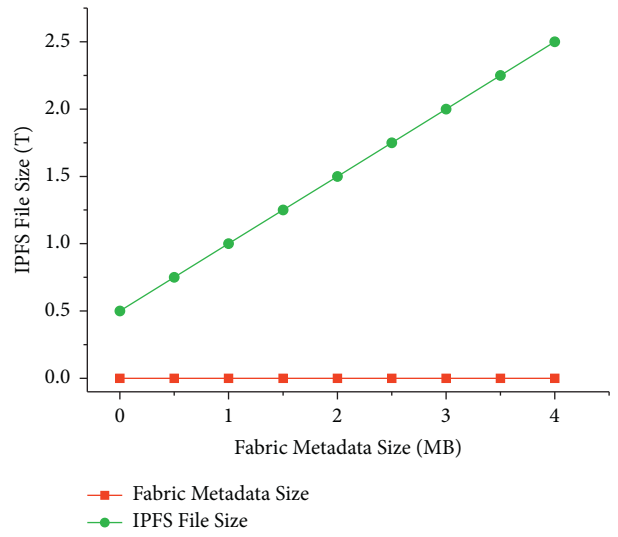

Figure 8: Comparing the size of files on Bc-IPFS and the size of file metadata on blockchain ledger.

multiple organizations or institutions, and its data can only be read, written, and maintained by those organizations or institutions. It effectively tackles the problem of "information silo" between different entities, which is ideal to the security traceability systems of agricultural products. The specific reasons of why Hyperledger Fabric is more adaptable to the solution proposed in this thesis, compared with ETH, are as follows:

(1) *Expandability*. One of the main characteristics distinguishing Hyperledger Fabric from other blockchain technologies such as ETH is its modularity, which provides an architectural structure of modularity and expandability applicable in various environments, making it more adaptable to the functional expansion of IPFS [33].

(2) *Consensus Mechanism*. The current ETH adopts the Proof of Work (POW) consensus mechanism, which is inefficient in accounting and vulnerable to 51% hash rate attack, and it consumes a great deal of computer resources. The Hyperledger adopts the Byzantine Fault Tolerance (PBFT) consensus mechanism, which provides an accounting efficiency at the sec level and low power consumption; thus it is ideal for the development of the traceability industry [34].

(3) *Confidentiality*. Since ETH is a public network irrelevant to the concept of authority and is completely transparent, thus all transactions recorded on the blockchain network can be available to and accessible by each counterparty, but Hyperledger is a blockchain platform with access authority and high levels of security; thus all transactions are only available to the ones with access authority.

(4) *Interactivity*. Hyperledger Fabric provides SDKs for interaction, so it can interact with IPFS and can effectively search the blockchain and provide data for review through the functions provided by SDKs.

Table 3: Plan comparison.

Characteristic	[5]	[7]	[10]	[35]	This work
Traceability	Yes	Yes	Yes	Yes	Yes
Supervisory	No	Yes	No	Yes	Yes
Scalability	No	Yes	Yes	Yes	Yes
Evaluation	No	No	No	No	Yes
Gas	—	No	Yes	Yes	No
On-chain data	High	Low	Low	High	Low

Then, we compare the traceability plan designed here with other plans, and the results are shown in Table 3 [7]. The data is still stored centrally, although traceability is based on blockchain. In contrast, this plan has higher decentralization. In addition, in this plan, a supervision organization is set up to supervise the members of the supply chain and products, ensure the integrity and accuracy of information, and strengthen the supervision of the organization [10]. Obviously, relevant entities in the supply chain are not supervised efficiently. At the same time, the consumer evaluation function designed in this plan plays a strong role in retailers' self-monitoring, and, through retailers' credit value function, consumers are able to quickly screen the purchase objects so that it can effectively reduce the negative effects due to malicious evaluation behavior. K. Salah [35] solves the problem studied by Ethereum smart contract. This method needs to cost the Gas fee. Once the Gas is used up, the contract will not be executed and the used fee will not be refunded. However, Hyperledger is not involved in mining process, which can save resources and time, and has modularity and expansibility.

5. Conclusion

The Bc-IPFS-based solution proposed in this thesis tackles the problem of "information silo" between entities by the alliance blockchain Hyperledger and realizes the automation of traceability through the smart contract deployed on Hyperledger Fabric, so as to improve efficiency. The IPFS technology is adopted to ensure data security and overcome the data storage constraint of blockchain for overwhelming data, the ring signature algorithm is adopted to privatize consumer information and encourage consumers to timely feedback product problems, and performance evaluation is conducted by virtue of throughput capacity and delay, in addition to security analysis of the solution. The solution is developed with comprehensive considerations to traceability, transaction, and retailer reputation, and the established reputation function can be used to maintain the reputation of the entities in the supply chains of agricultural products and the quality rating of the products. This thesis describes the plan design, overall structure, entity relationship diagram, interaction, and details related to implementation algorithm and shows how to apply the plan to track grain supply chain. The plan designed can provide and meet reliable decentralized traceability demands for any crop in agricultural supply chain.

Up to now, the system based on blockchain is still challenged by its practical implementation. In the future, we plan to integrate protection of enterprise and consumer privacy in agricultural food trade. Similarly, the retailer's credit value comes from consumers' evaluation, which may be biased or falsified. As a result, we plan to design a supervision mechanism for comment information to help improve such accuracy.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was sponsored by the National Natural Science Foundation of China under grant no. 62172353. Future Network Scientific Research Fund (project no. FNSRFP-2021-YB-48), Science and Technology Program of Yangzhou City (no. YZU202003). Natural Science Foundation of the Jiangsu Higher Education Institutions (grant no. 17KJB5 20044), and Six Talent Peaks Project in Jiangsu Province (no. XYDXX-108).

References

[1] X. Yuan, "Research on the credit and law enforcement mechanism of food safety in my country," *Food Safety Guide*, pp. 32-33, 2016.

[2] L. Zhang, M. Peng, W. Wang, Y. Su, S. Cui, and S. Kim, "Secure and efficient data storage and sharing scheme based on double blockchain," *CMC-Computers Materials & Continua*, vol. 66, pp. 499–515, 2021.

[3] M. Crosby, "Blockchain technology: beyond bitcoin," *Applied Innovation*, vol. 2, p. 71, 2016.

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

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

[6] F. Tian, "A supply chain traceability system for food safety based on HACCP blockchain & Internet of Things," in *Proceedings of the 2017 International Conference on Service*

Systems and Service Management, pp. 1–6, Dalian, China, Jun. 2017.

[7] X. Yang, M. Li, H. Yu, M. Wang, D. Xu, and C. Sun, "A trusted blockchain-based traceability system for fruit and vegetable Agricultural products," *IEEE Access*, vol. 9, pp. 36282–36293, 2021.

[8] C. Xie, Y. Sun, and H. Luo, "Secured data storage scheme based on block chain for agricultural products tracking," in *Proceedings of the 2017 3rd International Conference on Big Data Computing and Communications*, pp. 45–50, Chengdu, China, August 2017.

[9] J. T. Hao, Y. Sun, and H. Luo, "A safe and efficient storage scheme based on blockchain and IPFS for agricultural products tracking," *Journal of Computers*, vol. 29, no. 6, pp. 158–167, 2018.

[10] 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.

[11] E. Nyaletey, R. M. Parizi, Q. Zhang, and K.-K. R. Choo, "BlockIPFS - blockchain-enabled interplanetary file system for forensic and trusted data traceability," in *Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain)*, pp. 18–25, Atlanta, GA, USA, July 2019.

[12] Hyperledger Fabric Documentation: https://hyperledger-fabric.readthedocs.io/zh_CN/latest/whatis.html, March 20 2021.

[13] A. Lohachab, S. Garg, B. H. Kang, and M. B. Amin, "Performance evaluation of Hyperledger Fabric-enabled framework for pervasive peer-to-peer energy trading in smart Cyber-Physical Systems," *Future Generation Computer Systems*, vol. 118, pp. 392–416, 2021.

[14] M. Uddin, "Blockchain Medledger: hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry," *International Journal of Pharmaceutics*, vol. 597, Article ID 120235, 2021.

[15] M. Kumar and S. Chand, "MedHypChain: a patient-centered interoperability hyperledger-based medical healthcare system: regulation in COVID-19 pandemic," *Journal of Network and Computer Applications*, vol. 179, Article ID 102975, 2021.

[16] X. Xue, Z. Chen, S. Wang, Z. Feng, Y. Duan, and Z. Zhou, "Value entropy: a systematic evaluation model of service ecosystem evolution," *IEEE Transactions on Services Computing*, p. 1, 2020.

[17] X. Xue, S. Wang, L. Zhang, Z. Feng, and Y. Guo, "Social learning evolution (SLE): computational experiment-based modeling framework of social manufacturing," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3343–3355, 2019.

[18] S. Su, Z. Tian, S. Liang, S. Li, S. Du, and N. Guizani, "A reputation management scheme for efficient malicious vehicle identification over 5G networks," *IEEE Wireless Communications*, vol. 27, no. 3, pp. 46–52, June 2020.

[19] T. Li, Z. Wang, G. Yang, Y. Cui, Y. Chen, and X. Yu, "Semi-selfish mining based on hidden Markov decision process," *International Journal of Intelligent Systems*, vol. 36, no. 7, pp. 3596–3612, 2021.

[20] T. Li, Z. Wang, Y. Chen, C. Li, Y. Jia, and Y. Yang, "Is semi-selfish mining available without being detected?" *International Journal of Intelligent Systems*, 2021.

[21] L. J. Zhang, Z.-D. Liu, X. Guo, and X. Xiao, "Secure data sharing model based on smart contract with integrated credit evaluation," *Acta Automatica Sinica*, vol. 47, no. 3, pp. 594–608, 2021.

[22] R. Kumar and R. Tripathi, "Towards design and implementation of security and privacy framework for Internet of Medical Things (IoMT) by leveraging blockchain and IPFS technology," *The Journal of Supercomputing*, vol. 77, pp. 1–40, 2021.

[23] Y. Chen, J. Sun, Y. Yang, T. Li, X. Niu, and H. Zhou, "PSSPR: a source location privacy protection scheme based on sector phantom routing in WSNs," *International Journal of Intelligent Systems*, 2021.

[24] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "CorrAUC: a malicious bot-IoT traffic detection method in IoT network using machine-learning techniques," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3242–3254, 2021.

[25] M. Shafiq, Z. Tian, A. Bashir, X. Du, and M. Guizani, "IoT malicious traffic identification using wrapper-based feature selection mechanisms," *Computers & Security*, vol. 94, Article ID 101863, 2020.

[26] R. Kumar, R. Tripathi, N. Marchang, G. Srivastava, T. R. Gadekallu, and N. N. Xiong, "A secured distributed detection system based on IPFS and blockchain for industrial image and video data security," *Journal of Parallel and Distributed Computing*, vol. 152, pp. 128–143, 2021.

[27] M. Shafiq, Z. Tian, A. A. Bashir, A. Jolfaei, and X. Yu, "Data mining and machine learning methods for sustainable smart cities traffic classification: a survey," *Sustainable Cities and Society*, vol. 60, 2020.

[28] M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani, "Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city," *Future Generation Computer Systems*, vol. 107, pp. 433–442, 2020.

[29] J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, and B. Fang, "A survey on access control in the age of internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 4682–4696, June 2020.

[30] E. Politou, E. Alepis, C. Patsakis, F. Casino, and M. Alazab, "Delegated content erasure in ipfs," *Future Generation Computer Systems*, vol. 112, pp. 956–964, 2020.

[31] P. Thakkar, S. Nathan, and B. Viswanathan, "Performance benchmarking and optimizing hyperledger fabric blockchain platform," in *Proceedings of the 2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*, pp. 264–276, Milwaukee, WI, USA, September 2018.

[32] T. Sato and Y. Himura, "Smart-contract based system operations for permissioned blockchain," in *Proceedings of the 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pp. 1–6, Paris, France, February 2018.

[33] Hyperledger Blockchain Performance Metrics: 2021, https://www.hyperledger.org/wp-content/uploads/2018/10/HL_Whitepaper_Metrics_PDF_V1.01.pdf.

[34] L. Zhang, Y. Zou, W. Wang, Z. Jin, Y. Su, and H. Chen, "Resource allocation and trust computing for blockchain-enabled edge computing system," *Computers & Security*, vol. 105, Article ID 102249, 2021.

[35] S. Wang, D. Li, Y. Zhang, and J. Chen, "Smart contract-based product traceability system in the supply chain scenario," *IEEE Access*, vol. 7, pp. 115122–115133, 2019.