Information and Knowledge Management (2022)
Clausius Scientific Press, Canada

DOI: 10.23977/infkm.2022.030101
ISSN 2523-5893 Vol. 3 Num. 1

Agricultural Information Data Sharing Model of Mobile Communication Network Based on Blockchain

Tianxiang Yang[1,a,*], Yiming Lin[2,b]

[1]*School of Business Administration, Jiangxi University of Finance and Economics, Nanchang 330032, Jiangxi, China*
[2]*School of Economics and Management, Xiamen University of Technology, Xiamen 361024, Fujian, China*
[a]*tax_y@qq.com*, [b]*taxydegirl@qq.com*
**Corresponding author*

Keywords: Blockchain Technology, Agricultural Information, Data Sharing Model, Mobile Communication Network

Abstract: Technological progress enables enterprises to make better decisions and cooperation. Data can be obtained from data sources through information technology tools. In this paper, the decentralized agricultural information sharing system is constructed by using block chain technology, which is also suitable for other fields. Users share data through streams in the blockchain. The system collects user data through verification and ensures that users can reasonably control data and protect user privacy. The data in the database is transformed into open data mode, which is shared through the flow in the blockchain so that other users can easily convert the data to their database after receiving the data. This article tested the latency and memory consumption that affect the user experience to evaluate model performance. The delay result of the request to the blockchain data sharing service provider is 682.32 ms. The time for integrity and signature verification is 28.32 ms. Experiments show that the results can respond quickly and the user experience is very good.

1. Introduction

The main characteristics of blockchain technology are distributed, asymmetric encryption and time stamp. The important significance of blockchain is to establish a trusted data storage scheme through mathematical principles, which can establish a set of trusted multi person accounting scheme without an administrator. The basic idea of blockchain is to establish a "public account book" on the mutually beneficial network by "sharing" and "checking" all accounts in the network to ensure that the information is true and will not be tampered with [1]. The main characteristics of blockchain are decentralization, mutual trust, collective maintenance and reliable database.

A series of agricultural tracking information systems inspired by the blockchain technology can be constructed through the decentralized network of members.The key to this system is to build an information recording system that can copy and share data using algorithms that all of us know. The data management of a single member is transparently resolved and decentralized through

blockchain technology. The sauce of the agricultural industry chain began, and the production personnel used the Internet and the Internet of Things to make use of the Internet. The quality of all participants including farmers, food processing companies, distribution companies, and food delivery companies can record relevant information. The network cannot be tampered with. Blockchain can not only guarantee credit, but also reduce costs and increase profits.

Abdullah reviewed the application of blockchain encryption in industry 4.0 this new encryption method can simplify the process of financial transactions and other network security related fields, so it is widely used in industry 4.0, relevant documents show that blockchain technology has broad prospects in Internet finance, manufacturing, public sector, health care and media industries. Abdullah et al. Studied the application of blockchain in different fields to provide more secure services without the need of a third party [2]. Ding proposed a battery data sharing model based on blockchain, which has the functions of anti-counterfeiting, digital signature, traceability, distribution, anti tampering, etc. The model is used to evaluate battery life and registration, and to determine the cause of battery problems. Ding also simulated different parts of the battery industry chain with raspberry pie and used the blockchain platform to run the application [3].

This paper analyzes the existing architecture and limitations of blockchain, and introduces the developing agricultural data information sharing model based on blockchain. This paper evaluates the performance of the model, introduces the factors that have the greatest impact on the user experience, provides a descriptive analysis of the experimental results, and finally emphasizes the impact of blockchain on agricultural informatization, which can better protect the privacy of users in the field of privacy protection data sharing.

2. Blockchain and Its Application in Agriculture

Blockchain is a distributed database, which is an ordered list of connected nodes [4]. The node records relevant information. Blockchain maintains a growing ordered list, which is distributed and cannot be changed. Therefore, the system based on blockchain technology has high reliability and information security [5]. For users who want to exchange information, they first need to verify the information through the node set, and then exchange the information of both sides. Through a series of verification, the change records of information are all in the public database for reference [6].

If a malicious change of information occurs, the verification node can track the properties of the node and prevent the behavior. For such a system, a highly secure and tamper proof database is required [7]. For the exchange of information between customers with unknown identities, a system is also needed to make secure information changes in the absence of trust. Blockchain is very suitable to solve the security problem of changing the data in cloud storage. Blockchain is distributed, so every customer on the Internet has a record of every change data made on the network [8]. The tamperability of blockchain and the ability to execute untrusted transactions enable it to share data securely.

The blockchain network consists of multiple nodes, which are linked orderly. When the nodes containing all information propagate to the network, these nodes form a chain, and can not be tampered, updated or deleted. When the user maliciously changes the node information or the system detects a malicious threat, data validation will be enabled and data traceability will be enhanced [9]. The node consists of a single event, the time range of which is from the time when the request is sent to the time when the node is broadcast to the blockchain. When a violation in the system needs to be investigated, a request is sent and access is obtained to investigate the violation. The public node is responsible for discovering and reporting violations [10]. Blockchain can record information in a distributed way and prevent data from being tampered with. When and only when the node is authorized to broadcast, the processed and authorized nodes are allowed to access the

blockchain network. Other unauthorized nodes cannot broadcast [11].

(1) Encryption Key

Encryption key is a key set established for performing tasks related to system security [12]. For blockchain based systems, create a key, perform user authentication with the key, and request to generate information related to authentication [13]. These keys can determine the security level of the scheme. The encryption keys include:

Membership grant key: to generate and send the key for the user who requests to join the data sharing system, the user must have a private key and a public key for generating transactions. Without the key, the user cannot join the system.

Membership verification key: verify the validity of the user in the system, and allow the user to access the membership key, which is used to generate the user's membership key [14].

Membership key: create a request, and then the request generates a node. If there is no membership key, the request cannot be created.

Transaction private key: digitally sign the request created by the member number.

Transaction key: used to verify who is signing. If the request cannot match the key, the request is invalid.

When a user sends a registration request, he needs to submit his account public key. After confirming the user's ID and assigning a proper attribute set to the user, add the user's account address to the smart host's authorized user set.

$$\widehat{\sigma}_{\iota} = \sigma_{\iota,k_i} = g^{H_0(y\|i\|k_i)} H_1(sk)^{H_0(y\|i\|k_i)} \tag{1}$$

The shared key is calculated according to the account public key submitted by the user, and CTusk is obtained by encrypting SKd and SK with asymmetric encryption algorithm. Embed the CTusk in the transaction TXusk, and broadcast the TXusk to the blockchain. Through the secure channel, its account public key, transaction ID, user attribute set, smart contract address, and smart contract source code are transmitted to users. The user can confirm the smart host deployed on the blockchain.

The encryption algorithm is

$$< X_P, Y_P >=< \prod_{i\in L_P} \widehat{X}_i, \prod_{i\in L_P} \widehat{Y}_i > \tag{2}$$

$$\prod_{i=1}^{x} e(S_i, (L_j M_j^{u(i)})^{T_{ij}}) = \begin{cases} e(C, h_1) e(Ng^{\mu}, R_1), j = 1 \\ e(Ng^{\mu}, R_j), \quad j > 1 \end{cases} \tag{3}$$

The decryption algorithm is

$$K = \frac{C_0}{\widehat{e}(\sigma p, C_1) \cdot \widehat{e}(H_1(sk), C_2)} \tag{4}$$

$$\frac{e(C', sk)}{(\prod_{i\in U} (e(C_i, T) e(D_i, sk_{\beta(i)}))^{\rho_i})} = \frac{e(k,k)^{sl} e(k,k)^{alt}}{\prod_{i\in U} e(k,k)^{ta\gamma_i\rho_i}} = e(k,k)^{sl} \tag{5}$$

Users who want to join the blockchain need to verify their membership. The user identity needs to be verified and acquired through the system to generate a specific key related to the user [15]. In this scheme, a secure and effective identity based authentication and key protocol is adopted, which can complete the authentication under the condition of anonymity. There are two ways to set a new user as a system member [16]:

The first is based on a unique encryption technology. In the authentication phase, the system setup, key exchange, authentication and key end of the month should be completed. The system

settings are the parameters needed to generate and calculate the system public key, which are obtained according to the user identity and random number [17]. Key exchange is to extract the calculation set from the system setup program, with special emphasis on the exchange of random variables between users and publishers [18]. Authentication and key protocol describes the creation of a shared symmetric key for users and developers [19]. Users and developers calculate the shared key to encrypt and decrypt the information related to account registration and verification, so that users become system members [20].

The second is to provide users with account registration and verification based on shared information. The developer sends an encrypted form with user details related to the pre-set regulations and Yan verification certificate [21]. Validation demonstrates the effective response of the encryption method that defines the user registration details. The user decrypts the file with the shared key, and then encrypts it [22]. The completed form is combined with the limited test value and sent to the developer. The developer creates a membership issuance key according to the user's identity, sends the key to the user, and makes the user a member of the group. User request authentication provides information security for developers to generate key correctness. After the developer confirms that the key is correct, the parameters related to the ID and the correct level are jointly sent to the user [23]. The user creates a transaction key pair through parameters.

Membership certification is very important to set the user's permission to participate in data access. The verification mechanism based on the blockchain data sharing scheme is implemented between users and verifiers [24]. The user sends a request to the verifier to confirm the membership of the group. The verifier sends a query through the random number generated by the membership issuance key. The user calculates according to the query and random number, and sends a response to the verifier, and signs the message using the member authentication key [25]. In addition to the response, the user can also send a random number to confirm the identity of the verifier. The verifier compares the signature and calculation with the value stored in the memory associated with the shared verification key. The verifier sends the hash value and random number of the member certificate to the user [26]. The user confirms the identity of the verifier and sends the transaction public key of the verifier to the verifier. When the verifier receives the message, the public key of the transaction is stored in a private database. The authorizer calculates the membership secret key based on the membership authentication key and sends it to the user [27].

Proof of authority is part of a block chain protocol mechanism based on inherently defective algorithms and high performance. The authority proof algorithm is based on K trusted node sets. Each trusted node has its own ID. For all subscription agreements executed by unacknowledged nodes, authorized nodes will perform agreement verification. The authority proof algorithm relies on the cheating model and supports fair authority allocation to create areas between nodes to be trustworthy. This method suggests that your evaluation mechanism can be used to honestly assign nodes based on reputation scores. The page level of all addresses will be redefined according to the page level connected to other addresses. First, the first score of all addresses will be assigned n, and then updated with a mathematically defined score.

$$PR(A) = (1-d) + d(\frac{PR(B_1)}{C(B_1)} + ... + \frac{PR(B_n)}{C(B_n)}) \tag{6}$$

PR (a) is the page rank of a, PR (BN) is the page rank of B of a, C (BN) is the number of out bound links of address BN, and D is the locking coefficient. $0 \leq d \leq 1$. Public relations (BN) connected to the a address will not affect the ranking of the a page. The page rank of address BN will assign a weight value to the external link C (BN) of address B. Therefore, the more A-b external connections C, the lower the level of page A. In addition, the address level BN for multi-page addresses will be added. After adding a link to address a, the ranking of the address a

page will always improve. In general, the weighted series of all addresses are multiplied by the damping coefficient. Consider a time frame of one week, with a target interval of 600 seconds. This provides sufficient time for transaction inspection and inspection. Consider the solution price of the customer base to calculate the difficulty based on the customer reputation score.

(3) Unprocessed Request Pool

The unprocessed request pool is a block data pool created by the user that contains the user creation request. The user creates and provides data, or accesses data in the storage device. A consensus node is an entity that obtains data from the pool for processing [28]. There are no links to nodes that are not in the pool. They have a time stamp in the swimming pool. In order to define the order in which these blocks are extracted and processed, you need to use a suitable algorithm. The unprocessed request pool and the blockchain network are two independent entities with no links at all. The only feature between them is the consensus node [29].

Although much attention to blockchain technology is focused on the money and financial markets, many observers, including senior officials of the world bank and the food and Agriculture Organization of the United Nations, predict that the non monetary application of blockchain will have a more profound impact. The blockchain in the field of agricultural food has many ways to change the industry [30]:

Smart contract: blockchain technology can automatically perform smart contracts. Agricultural products are usually sold under forward contracts, which means that farmers and buyers agree to buy / sell goods at a predetermined price at a specific time in the future. This has led to many problems, such as the income inequality of farmers, the sensitivity of price fluctuation and the unperformed contracts. If smart contracts are applied to the agricultural product market, these problems can be solved and stronger relations between producers and consumers can be promoted [31, 32].

Monitoring and verification: blockchain is a distributed bookkeeping method that cannot be tampered with; it cannot be changed in any way without the consent of all participants. Blockchain provides an ideal mechanism to track farm environmental sensor data and other information such as pesticide and fertilizer use. This information is often used for sustainability certification [33]. Farmers can be sure that their information is confidential relative to people outside the blockchain, and users and consumers can be sure that the information they get about the impact of food on the environment and the growing information is reliable and accurate [34].

Supply chain traceability: blockchain can be used to accurately track food from farm to table throughout the supply chain [35]. With permanent and complete distributed accounting, low cost, high accuracy and trust, the agricultural food supply chain will be changed in many ways [36]. First, it will allow government officials to trace the source of disease products and other harmful products within seconds to improve food safety. In the food crisis, the function of tracing the origin of finished products is very important, which can save money and time. Secondly, by allowing consumers access to information about the product's journey in the system, including information about the source of the product and how it is planted, transported and packaged, public trust will be enhanced [37].

One of the most promising applications of blockchain is its ability to track goods in the whole supply chain from production, transportation, manufacturing to wholesale and then to retail [38, 39]. Blockchain's tamper proof and distributed accounting is an ideal tool to maintain a comprehensive record of information changes throughout the supply chain.

Tracking tuna from sustainable sources to enhance the capacity of smallholder fishers using sustainable fishing methods. The source of fish is an important issue in the fishing market. If the fishing method cannot be confirmed, fishermen will not be able to obtain market premium from the fish they can purchase sustainably. This has encouraged large-scale fishing activities, leading to

local unemployment and overuse of natural fisheries. Work with fishers to collect data on catches. After fishing, fishermen only need to send a message to register the fish, which will automatically create a digital asset on the blockchain, which is permanently bound with a unique identification number on the fish. Then, information about the location data and sustainability attributes is sent to NGOs for verification. These institutions then create digital certificates and classify them on the blockchain. Fish, certificates and digital assets are then transferred to the Buyer / supplier and then to the processor. After processing, a near field communication chip is connected to each tuna can to help track the transport and retail parts of its journey. At each stage of the supply chain, specific digital assets are transferred on the blockchain together with the tangible assets of fish. In retail stores, consumers using smartphones can scan cans and get farmers' names, capture fair trade information such as places and ways [40]. Using blockchain technology can greatly improve the traceability and transparency of the supply chain. This technology is applicable to almost any supply chain that needs trust.

The goal of the agricultural tracking platform is to record production supply chain information and ensure that all processes are completed under the supervision of a third party. The characteristics of integrated block technology can fully meet the needs of agricultural tracking platforms. The purpose of building an agricultural tracking platform based on blockchain technology is to record all relevant information in the blockchain structure.It means that another company cooperates with an institution. So you must define the usual structural representation in the data. The Bitcoin block chain stores transaction details and it is difficult to integrate all the information, and there may be many repetitions [41]. Therefore, the agricultural tracking system has designed two related structures, namely basic food information and source records.

3. Design of Agricultural Resources System

The technology required for the agricultural tracking system has many similarities with the blockchain technology [42]. However, the agricultural tracking system has its inherent characteristics, and it cannot be completely learned from the traditional component network design. This section will explain the design of the agricultural tracking system, The system design is shown in Figure 1 and Figure 2. The platform mainly includes the three roles of registry, node, data node and client described in the following sections.

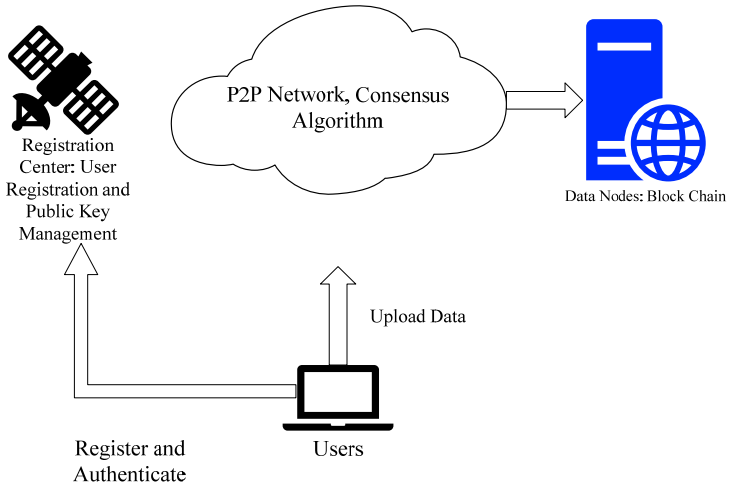

Figure 1: Structure of agricultural information sharing system

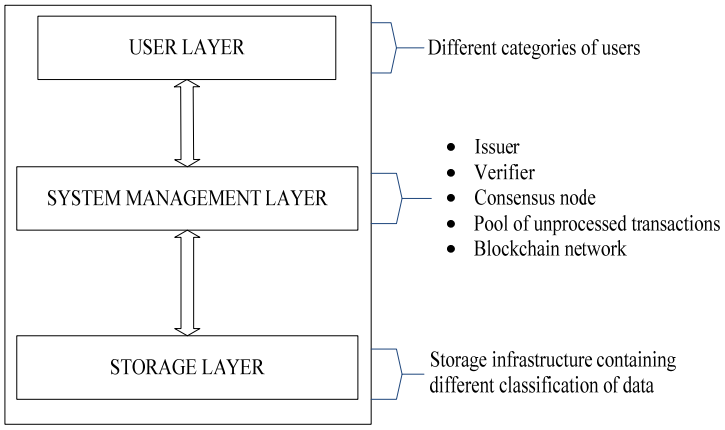

Figure 2: Layers of agricultural information sharing system

Unlike the Bitcoin network anonymity, the agricultural tracking system should clearly indicate the data provider and the person responsible for the accuracy and timeliness of the data, and include the identity confirmation process responsible for the type of registration. The registration form does not process agricultural tracking data, but is only responsible for user registration. The users here mainly refer to users who need to submit data to the platform, including agricultural companies, test organizations, transportation companies, storage companies, and sales companies.

When uploading data to the platform, users must use a private key to sign each data, not for tracking information. In this registry, each user has a corresponding public key, so anyone can confirm the actual ID of the database during this process. This certification process has two meanings. For protons, you can view the data source. When uploading data, it is effective not to allow others to upload wrong data.

The monotone span procedure is defined as follows:

$$\Gamma(x_1, x_2, ..., x_n) = 1 \Leftrightarrow \exists \vec{v} \in F^{l \times t} : M = [1,0,0,...,0] \tag{7}$$

(1) Data node

The data node is a major part of the system. They establish a distribution network between different locations and communicate with each other through the network. Each database runs in server mode, with responsibilities:

Please accept the user's upload request and confirm the validity of the data, and then send the valid data to other nodes.Users can request and upload data in all data nodes. After receiving the request, the node must first verify the correctness of the data form, and then require the validity of the digital signature on the registry. After verification, the data will be saved in the local data buffer, and the broadcast will be replaced by other data nodes [43].

Organization block data receives user uploads and broadcasts from other nodes, and stores undecoded data buffers at each node. When a certain amount of data is accumulated, the node configures the data from the block in a predetermined form and uses the block as the next candidate block in the chain.

Whenever a node prepares a candidate, Send and receive block data broadcast,it will replace the node with another node [44]. At the same time, you are ready to accept the broadcast replaced by another node. All nodes are parallel, so other candidate areas may be generated.

Algorithms that implement decentralized agreements. Because there are many candidate areas, it is necessary to determine the next area by agreement algorithm. You can use different algorithms according to the situation. After reaching an agreement, each node accepts this result and records the new block in the local block chain, and deletes the data from the block chain cache, and then executes the protocol algorithm.

(2) Customers

As mentioned earlier, in order to digitally sign, you need to register and maintain a personal height. Second, requesting node data, consumer users who get results can get quotas, or end users can get quotas. Generally no registration is required, but the end user is an important part of the system.

4. Network Reliability Test

We developed and deployed an agricultural information data sharing software on a machine. A machine is a node that collects customer data through proper testing and sorting. Then use different computers for performance testing. Users can choose to share information with third parties and create personal data in the agricultural information data sharing system at the first node of the blockchain. The software process can be used for general data storage and retrieval, obtaining addresses, and entering the closed network of the blockchain. Public key encryption is the basic technology of the system. All nodes connected together will generate a public key and private key pair.

By extending the "handshake" process when two blockchain nodes are connected, the system limits blockchain access to the list of allowed users. Firstly, a multi chain is created for the first node in the blockchain in the agricultural information data sharing system. By default, this node is an administrator and can further grant administrator status to other nodes. The permissions of other nodes will be set by this node, but when setting the chain parameters, the permissions of all nodes can be set to true,

You can also set other permissions for other nodes while granting connection permissions. Node B is given the rights to connect, send, receive, send, create, mine, activate and manage, while node C is given all the rights except administrator and activation. This means that node B in the blockchain can act as an administrator, while node C cannot. Seven other nodes were created to evaluate system performance.

The first node is agricultural information data sharing system, which basically collects user data when uploading agricultural information. Useful information about the collected user profiles is shared between enterprise federations under predefined contractual terms.

The data collected at node a is added to the flow as a project. The files added to the stream are then published and distributed to all nodes. All files that exist in the stream can be viewed. Only nodes with receive permission can view content in the stream.

All other nodes on the network can easily convert the streaming media files you receive to their own repository and save them. Each node of the blockchain can access the original data. The data will be encrypted and then stored in the chain to solve this confidential problem. Three block chains combining symmetric and asymmetric encryption are used.

Public key stream: Participants can use this function to publish their public keys with an asymmetric public key encryption system.

Engineering process: It will be used to display a large amount of data, and each data will be encrypted with a symmetric encryption system.

Access stream: Provide data access. For each participant who needs to view the data, an encrypted process is used to decrypt it, which contains the password of the data. Combine multiple and non-sub-chains to create a data sharing and management model that focuses on security and personal information protection.

Blockchain is the guarantee of data security. If an attacker acts as a bad node in the blockchain network, the block to be linked is forged. The competition between honest chain and attacker chain can be described by the random walk of binary tree. The probability of success of the forgery block

attack is calculated as an equation.

$$P_Z = 1 - \sum_{k=0}^{Z} \frac{\lambda^k e^{-\lambda}}{k!} * (1 - (\frac{q}{p})^{z-k}), \lambda = Z\frac{q}{p} \tag{8}$$

p is the probability that the honest node generates the next block, q is the probability that the attacker generates the next block, and PZ is the probability that the attacker catches up with the main chain from the following z blocks.

There may be an attacker maliciously exploiting the loophole of this contract. Therefore, any wrong system can prevent any attacker. If an attacker collides with other nodes to generate a fake link structure, or the page ordering mechanism can generate the page rank of two nodes with the same value. Perform the following tasks to prevent the similarity between the two nodes:

$$PR(A) = \sum_{j=1}^{N} H_p(A) PR(A) \tag{9}$$

Therefore, rewards at each address can be used as incentives or disincentives, and the calculation formula is:

$$R = \frac{PR(A)}{\sum_{j=1}^{N} PR} \tag{10}$$

5. Analysis of Experimental Results

5.1 System Delay Test, Memory Consumption Test, Signature Verification Time Test

The system adopts the user centered mode, uses the blockchain network to process agricultural data, and ensures the ownership and integrity of each data. Operations on data records are highly interoperable and compatible with the current system. By implementing access control policies, users can process their personal data without worrying about privacy. At the same time, every request and update from agricultural suppliers are recorded and locked on the blockchain network, so that changes to agricultural information can be made accountable.

Evaluating system performance is critical to the scalability and efficiency of data integrity demonstration generation and data validation processes. We tested different numbers of concurrent records, ranging from 2 to 20000. Figure 3 and Figure 4 show the average time cost, respectively.

From these two figures, we can see that the system can process large data sets with low latency, which shows the scalability and efficiency of data processing. An algorithm is implemented by batch processing the data. This is an important advantage when data records are collected at a high frequency. Figures 3 and 4 show the test results of the system delay.

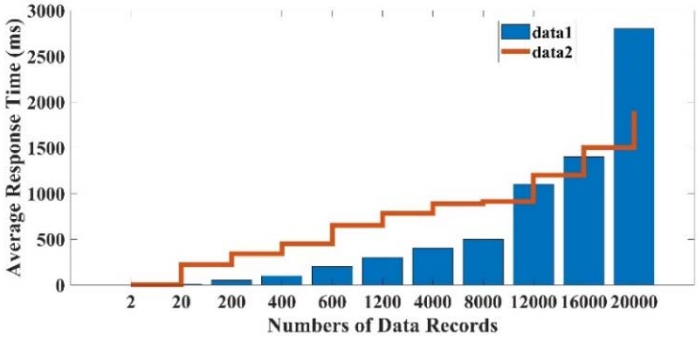

Figure 3: Average Time for Integrity Proof Generation.

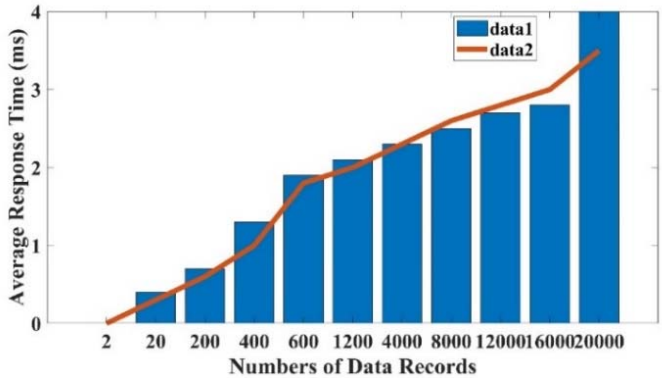

Figure 4: Average Time for Integrity Proof Validation.

The delay in the system is evaluated by analyzing the time it takes to deliver the packet after sending the request. This includes all the steps required to process requests from all entities in the agricultural information sharing system. The delay of this system is shown in Figure 3 and Figure 4. An important performance of latency is that with the increase of cloud service provider requests, latency increases significantly. This is due to the tradeoff between implementing security on low latency. Tuple size, data processing and anonymity help to increase delay. Through careful analogy of data use and data accumulation, we can draw a conclusion that this system has greater advantages than the existing system.

The delay results of the request to the blockchain data sharing service provider are shown in Table 1.

Table 1: Request delay from blockchain data sharing service provider.

Number of Users	Latency(ms)
4	682.32
9	328.23
14	782.93
19	239.48
29	987.23
29	973.20
39	834.72
99	2133.54

The time for integrity and signature verification is shown in Table 2.

Table 2: Time to perform integrity and signature verification

# of Events	# of Graphs for Hashing	Execution Time (ms)
232	289	28.32
1823	6523	324.34
3894	12903	841.33
4832	19323	1493.42
7432	24023	1932.23
8321	30234	2294.13

The memory consumption test is shown in Table 3.

Table 3: Testing Memory Consumption

Memory usage		
Initial	Later daemon started	Total daemon
812	792	20
923	911	12
943	923	20
932	902	30
953	923	30

The time test results for integrity and signature verification are shown in Figure 5.

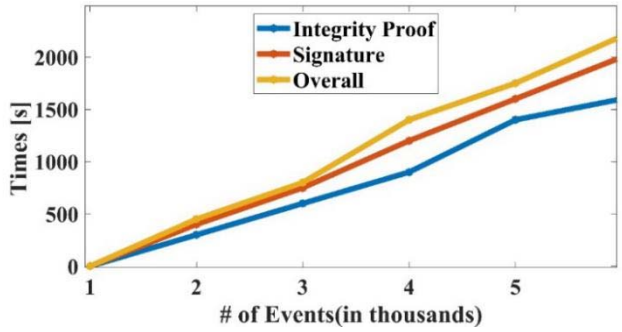

Figure 5: Time to perform integrity and signature verification

Figure 6 shows the execution time of the four operations.

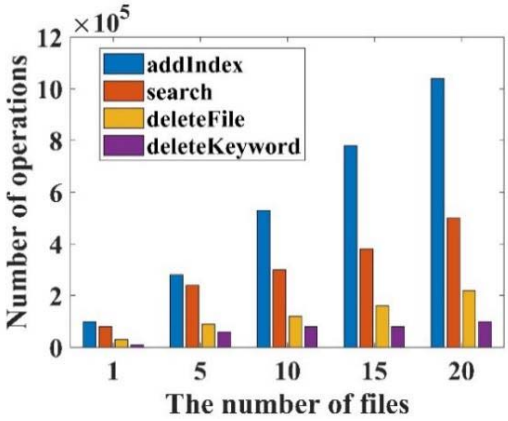

Figure 6: Smart contract operation costs under different number of files

We build an encrypted keyword index for five different keywords and get Figure 6. As shown in Figure 6, the cost of these four operations increases with the number of files.

The main advantages of using blockchain in agricultural information sharing are prevention of denial and transparency. Preventing denial can be achieved through the constant storage of the blockchain and its basic technology, the public key infrastructure. In our model, all access to data can be proven through the blockchain. To ensure reliability, confirm the signature before storing the data on the blockchain, and then add the gateway server's signature to all data on the blockchain. In addition, our model will also deal with some blockchain issues, such as cancellation of consent, confidentiality of data, storage restrictions, etc. Private blockchains are used to solve performance, energy consumption and scalability issues. It can be used to solve the problems of performance, scalability and energy consumption.

5.2 Availability Considerations

In this model, only metadata is stored in the blockchain. In order to ensure the availability of encrypted actual data, cloud storage that stores encrypted actual data is provided. Users can use metadata to search the data on the blockchain and query the data through the gateway server. As mentioned above, through an authentication mechanism based on public key infrastructure, actual users can access the data.

5.3 Privacy Considerations

By supporting fine-grained access control to its data through access control lists, the privacy of data owners can be protected. Data owners can revoke access to their data by updating the access list and maintaining data ownership, as long as no one performs auditable data access. In our model, we assume that the server is semi trusted. Use the public key of the data owner to encrypt the encrypted real data stored in the cloud storage. Only the data owner can create the re encryption key and set the access control policy. The gateway server can know all the re encryption keys and can try to re encrypt the encrypted confidential data. However, because the corresponding private key is protected, the gateway server cannot display the real confidential data.

5.4 Safety Considerations

This section introduces a proposed mode of malicious access and regeneration attacks, and how a proposed mode responds to such attacks.

Malicious access: Malicious users will read and write confidential data without sincerity. This mode can use the gateway server to prevent malicious readers from violating it. After confirming the relevant authenticity, the gateway server loads the ten thousand component data into the blockchain. Similarly, before recording the read transaction, the gateway server will also transmit the related transaction to confirm whether the transaction is suitable for a valid reader, and send it by the authorized reader in the matching access list. The server will use this re-encryption key to re-encrypt the data only to the accepted readers. Using these mechanisms on the gateway server can protect malicious leaders and authors.

6. Conclusions

At present, due to force majeure, traditional cloud storage may lead to the unavailability of user data. Attribute based encryption and searchable encryption are important technologies to solve data privacy and fine-grained access control problems. However, the traditional property-based encryption solution always needs a trusted private key generator. The private key generated by private key generator for users is not flexible enough, which may lead to key abuse, user data disclosure, etc. The traditional searchable encryption scheme requires the cloud server to perform the search honestly, but in practice, the cloud server may return incorrect results, or even no results, in order to save resources.Distributed storage method can solve the single point of failure in traditional cloud storage system. At the same time, compared with centralized storage, it also has a series of advantages such as low price and high throughput. In this paper, we study data storage and sharing in decentralized storage system, and propose a framework, which combines decentralized storage system, Ethereum blockchain and attribute based encryption technology. In this framework, a trusted private key generator is not required. The data owner can distribute your key to users, and according to the specified access strategy, encrypt and subdivide the access control of the data. At

the same time, based on the intelligent protocol of Ethereum block change, the keyword search function is implemented in the password text of the decentralized storage system, which solves the problem that the cloud server does not return or returns the wrong result in the existing cloud storage. And provide experimental case studies. Through experimental simulation experiments, the experimental data is analyzed to prove the rationality and achievable possibility of the system.

As the demand for data sharing continues to grow rapidly, data sharing and collaboration based on blockchain will become available rapidly in the near future. In this chapter, we review the use of blockchain technology to achieve secure and confidential data sharing and collaboration. We studied issues related to blockchain and privacy. Then, we study the privacy and security issues that affect the blockchain, and then we study how to solve these problems. The delay result of the request to the blockchain data sharing service provider is 682.32ms. The time for integrity and signature verification is 28.32 ms.

This paper discusses why it is important to share data in blockchain and how to share data in blockchain. We discuss the key management in blockchain and how to ensure the security and confidentiality of data, so as to share the data in blockchain safely and privately. This paper reviews the latest technical literature related to key management in blockchain and explains the different technologies currently used to achieve secure data sharing in blockchain. We also review the latest technical literature on secure and confidential data sharing in blockchain, and briefly outline the future of data sharing in blockchain, so that data owners can better control their usage data.

References

[1] Singh, P., and Agrawal, R. 2018. "A Customer Centric Best Connected Channel Model for Heterogeneous and Iot Networks," Journal of Organizational and End User Computing (30:4), pp. 32-50.

[2] Abdullah R S , Faizal M A . Block Chain: Cryptographic Method in Fourth Industrial Revolution. International Journal of Computer Network & Information Security, 2018, 10(11):9-17.

[3] Ding P . A Battery Health Data Sharing Model via Blockchain. Open Access Library Journal, 2018, 05(11):1-12.

[4] Bradbury D . Blockchain's big deal [financial IT]. Engineering & Technology, 2016, 11(10):44-44.

[5] Linnhoff-Popien C , Widmann A . Blockchain – Zum Geleit. Digitale Welt, 2018, 2(1):26-28.

[6] Stommel S . Blockchain-Ökosysteme. Datenschutz Und Datensicherheit Dud, 2017, 41(1):7-12.

[7] Esposito C , Santis A D , Tortora G , et al. Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?. IEEE Cloud Computing, 2018, 5(1):31-37.

[8] Pieters G C , Koch C . Blockchain Technology Disrupting Traditional Records Systems. Economic review (Federal Reserve Bank of Dallas), 2017, 6(2):1-3.

[9] Treleaven P , Brown R G , Yang D . Blockchain Technology in Finance. Computer, 2017, 50(9):14-17.

[10] Ellehauge J . Blockchain in Geospatial Applications. Gim international, 2017, 31(5):43-45.

[11] Siems R . Blockchain for Science Erste internationale Fachtagung in Berlin, 5. bis 6. November 2018. Abi Technik, 2019, 39(2):153-160.

[12] Saracevic, Muzafer, Saša Adamović, Nemanja Macek, Mohamed Elhoseny, and Shahenda Sarhan. "Cryptographic Keys Exchange Model for Smart City Applications." IET Intelligent Transport Systems, In Press, 2020.

[13] Lorne F T, Daram S, Frantz R, et al. Blockchain Economics and Marketing. Journal of Computer & Communications, 2018, 06(12):107-117.

[14] Namasudra, S., and Roy, P. 2018. "Ppbac: Popularity Based Access Control Model for Cloud Computing," Journal of Organizational and End User Computing (30:4), pp. 14-31.

[15] Nadine Rückeshäuser, Brenig C, Günter Müller. Blockchains als Grundlage digitaler Geschäftsmodelle. Datenschutz Und Datensicherheit Dud, 2017, 41(8):492-496.

[16] Bahga A, Madisetti V K. Blockchain Platform for Industrial Internet of Things. Journal of Software Engineering and Applications, 2016, 09(10):533-546.

[17] Michael Eldred. Blockchain Thinking and Euphoric Hubris (vol 35, pg 39, 2016). IEEE Technology & Society Magazine, 2016, 35(2):27-27.

[18] Thakur S, Kulkarni V. Blockchain and Its Applications – A Detailed Survey. International Journal of Computer Applications, 2017, 180(3):29-35.

[19] Liu, Y., Yang, C., Sun, Q., & Chen, Y. (2020). (k, n) scalable secret image sharing with multiple decoding options. Journal of Intelligent and Fuzzy Systems, 38(1), 219-228.

[20] Choksi B , Sawant A , Subhasree S . Blockchain-based Smart P2P Lending using Neural Networks. International Journal of Computer Applications, 2018, 180(35):51-55.
[21] Xue T F , Fu Q C , Wang C , et al. A Medical Data Sharing Model via Blockchain. Zidonghua Xuebao/Acta Automatica Sinica, 2017, 43(9):1555-1562.
[22] Saracevic, Muzafer, Saša Adamović, Nemanja Macek, Mohamed Elhoseny, and Shahenda Sarhan. "Cryptographic Keys Exchange Model for Smart City Applications." IET Intelligent Transport Systems, In Press, 2020.
[23] Mukkamala R R , Vatrapu R , Ray P K , et al. Blockchain for Social Business: Principles and Applications. IEEE Engineering Management Review, 2018, PP(99):1-1.
[24] Seth S Leopold, Raphal Porcher. Editorial: Sparse-data Bias-What the Savvy Reader Needs to Know. Clinical Orthopaedics and Related Research, 2018, 476(4):657-659.
[25] Zou J , Ye B , Qu L , et al. A Proof-of-Trust Consensus Protocol for Enhancing Accountability in Crowdsourcing Services. IEEE Transactions on Services Computing, 2018, PP(99):1-1.
[26] Haubeck C , Bornholdt H , Lamersdorf W , et al. Step-based evolution support among networked production automation systems. At Automatisierungstechnik, 2018, 66(10):849-858.
[27] J. Zhang. Walks trajectory tracking of shared information based on consortium blockchain. Revista de la Facultad de Ingenieria, 2016, 31(12):8-17.
[28] Kim T K , Kan J M . Sharing the attribute information based on blockchain. Journal of Engineering and Applied Sciences, 2018, 13(3):771-775.
[29] Esposito C , Santis A D , Tortora G , et al. Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?. IEEE Cloud Computing, 2018, 5(1):31-37.
[30] Yishu, L.(2020)"Promoting Competitiveness of Green Brand of Agricultural Products based on Agricultural Industry Cluster", Revista De La Facultad De Agronomia De La Universidad Del Zulia, 37(2),pp. 769-778
[31] Dinh T T A, Liu R, Zhang M, et al. Untangling Blockchain: A Data Processing View of Blockchain Systems. IEEE Transactions on Knowledge & Data Engineering, 2017, pp. (99):1-1.
[32] Fabisiak, L. 2018. "Web Service Usability Analysis Based on User Preferences," Journal of Organizational and End User Computing (30:4), pp. 1-13.
[33] Gammon K. Experimenting with blockchain: Can one technology boost both data integrity and patients' pocketbooks? Nature Medicine, 2018, 24(4):378-381.
[34] Wang, B.; Zhang, X.H.; Dong, X.C.(2018). Novel Secure Communication Based on Chaos Synchronization, IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences, E101A, 1132-1135.
[35] Zongsheng Huang, Jiajia Nie & Sang-Bing Tsai. 2017. Dynamic Collection Strategy and Coordination of a Remanufacturing Closed-Loop Supply Chain under Uncertainty. Sustainability, 9, 683.
[36] Singh M, Kim S. Intelligent Vehicle-Trust Point: Reward based Intelligent Vehicle Communication using Blockchain. Optical Engineering, 2017, 33(1):701-709.
[37] Liu, Z., Feng, J., Liu, B.(2019) Pricing and service level decisions under a sharing product and consumers' variety-seeking behavior, Sustainability (Switzerland),11(24).
[38] Adoma F. Big Data, Machine Learning and the BlockChain Technology: An Overview. International Journal of Computer Applications, 2018, 180(28):1-4.
[39] Liu, B., Li, T. & Tsai, S.B. 2017. Low carbon strategy analysis of competing supply chains with different power structures. Sustainability, 2017, 9, 835.
[40] S Wan, L Qi, X Xu, C Tong, Z Gu. Deep Learning Models for Real-time Human Activity Recognition with Smartphones, Mobile Networks and Applications, 1-13, 2019.
[41] M.Elhoseny, Multi-object Detection and Tracking (MODT) MachineLearning Model for Real-Time Video Surveillance Systems, Circuits, Systems, and Signal Processing, First Online: 20 August 2019. 39, pages611–630.
[42] Y. Jiang, H. Song, R. Wang, M. Gu, J. Sun and L. Sha, (2017). "Data-Centered Runtime Verification of Wireless Medical Cyber-Physical System," in IEEE Transactions on Industrial Informatics, 13(4), pp. 1900-1909.
[43] Wu, Y., Rong, B., Salehian, K., & Gagnon, G. (2012). Cloud transmission: A new spectrum-reuse friendly digital terrestrial broadcasting transmission system. IEEE Transactions on Broadcasting, 58(3), 329-337.
[44] Lv Z, Kumar N. Software defined solutions for sensors in 6G/IoE. Computer Communications. 2020. Mar 1;153:42-47.