A blockchain-based rice supply chain system

Yang Xue[2,1], *Xun* Liang[2,1,*], and *Dongyan* Zhao[1]

[1]Institute of Computer Science and Technology, Peking University, Beijing 100871, China
[2]School of Information, Renmin University of China, Beijing 100872, China

Abstract. With the continuous development of blockchain technology, "blockchain+" has gradually evolved into a new form of social and economic development. Blockchain technology can be applied to the rice supply chain management field. Consider integrating the encryption algorithm, timestamp technology, consensus algorithm, and sidechain technology of blockchain with the rice supply chain, analliance chainbetween companies upstream and downstream of the supply chain, including producers, suppliers, and vendors can be built to create a safe and efficient supply chain information management. This information system uses the unique encryption technology of the blockchain and its unforgeable features of irreversibility and decentralization to help the supply chain break the current bottleneck, solve the problem of information security in the rice supply chain and realize the practical traceability of rice. At the same time, the involvement of the blockchain will also open up new opportunities for supply chain finance and bring about fundamental changes in supply chain management.

1 Introduction

As the infrastructure and implementation of bitcoin, blockchain appeared in early 2009 with the birth of the first block of bitcoin, genesis block. Since the price of bitcoin soared in 2013, bitcoin and blockchain have entered the public's view for the first time through the media's attention. In essence, blockchain is a decentralized distributed accounting system. Its core advantages are decentralization and distrust. It has the characteristics of open consensus, unforgeability and traceability. On this basis, it makes it possible to decentralize market transactions. At the same time, it provides a good solution for the problems of high cost, low security and low security in the centralized system. In 2016, the establishment of China's blockchain research alliance also further promoted the research and development of blockchain. McKinsey pointed out in the research report that blockchain is the key technology that has the most potential to become the fifth wave of disruptive revolution after steam engine, power, information and Internet.

China's "Internet plus" concept is the first concept of "Internet+" proposed in 2015's twelve session of the three session of the National People's Congress. Both will have a huge impact on the development of the world economy. "Internet +" is the result and symbol of the deep integration of China's industry and informatization, and the "block chain +" is

* Corresponding author: liangxun@pku.edu.cn

another socio economic issue on the basis of it. New forms of exhibition. Blockchain technology originated from digital currency, but now it comes out of the background of digital currency, and has a wide range of application scenarios in economic and financial, social system and other aspects. Many scholars are also constantly exploring the changes it will bring in the market economy and its development and application in various industries. Melanie Swan put forward the concept of blockchain finance, believing that blockchain may become the third stage of database development. After the integration of blockchain technology and finance, it can realize the transaction and control of digital assets, and bring a major breakthrough in the development of the financial field. Yuan Yong and Wang Feiyue pointed out that blockchain has a wide range of application prospects in data storage, data authentication, financial transactions, asset management, election voting and other aspects, and evolved three modes of public chain, alliance chain and private chain according to different application scenarios [1].

In the traditional supply chain information management, there is a serious problem of information inequality before the upstream and downstream, which makes the upstream and downstream information of the supply chain can not be connected in time, suppliers can not know the needs of users in time, and the whole system has the defects of high cost and low efficiency. Through the blockchain technology, we can build a blockchain between the upstream and downstream of the supply chain, including manufacturers, suppliers, sellers and other enterprises and consumers [2], and build a distributed and shared information management [3]. This enables enterprises on the platform to share their own data information, greatly reducing the asymmetry of data and information, and at the same time of data exchange, the blockchain can also protect the privacy of all parties. After the blockchain technology is integrated into the supply chain and the isolated data island between upstream and downstream is opened, the enterprises can exchange information in time, the internal coordination of the industry can be greatly improved, and the efficiency of the whole supply chain will also be significantly improved, thus forming a new theory and method of information storage, transmission, processing and retrieval.

2 Implementation of information management security of rice supply chain based on blockchain technology

2.1 Cryptography principle of information management in rice supply chain based on blockchain

A variety of encryption algorithms are used in the blockchain system, including secure hash algorithm, Merkel tree algorithm, conic curve digital signature algorithm, etc. These algorithms have good unforgeability by virtue of good random source. Among them, in the rice supply chain information management, the encryption principle is derived from the asymmetric encryption algorithm, which is different from the traditional symmetric encryption algorithm in which both parties need to transfer the key. In addition, the existence of Merkel tree greatly reduces the algorithm complexity of transactions. For blocks with n transactions, the algorithm complexity of confirming a transaction is only log2n, which provides conditions for the existence of lightweight nodes without storing the whole blockchain, making it possible to conduct transactions and information query on the supply chain on mobile terminals such as mobile phones.

2.2 Design of time stamp server for rice supply chain information management based on blockchain

Timestamp server is an important innovation in blockchain technology. In the information management of rice supply chain, "timestamp server" carries out hash processing for each transaction block in the supply chain, that is, the input is transformed into the output of fixed length through hash algorithm, and the hash value is broadcast after the timestamp is stamped in the block head of the data area. Among them, each time stamp will include the time stamp of the previous block into its random hash value. Therefore, we can think that each timestamp enhances the previous timestamp, thus forming an unforgeable chain composed of supply chain transaction blocks. Once the data of a block is modified, the hash value of the previous block of the block will not match it. Therefore, it is necessary to continue to modify the hash value of the previous transaction block. This iteration can be traced back to the head of the linked list, i.e. Chuangshi block. Since the Chuangshi block cannot be modified, once a transaction block on the supply chain is confirmed by the blockchain and exists in the blockchain In the longest chain, it can not be tampered with and forged.

In the traditional rice supply chain, due to the lack of information sharing and transparency, once there is a problem in the supply chain, it is difficult to accurately investigate the responsibility of the corresponding enterprises, and it is also difficult to provide evidence for illegal activities, which can not achieve the supervision and review on the supply chain. In addition, due to the information blocking in the supply chain, it is difficult to communicate between enterprises, which provides an opportunity for fraud and data theft, which makes the security of information in the supply chain difficult to be guaranteed. The application of blockchain technology in the information management of rice supply chain provides a way for information sharing in the blockchain, which makes the trust between upstream and downstream enterprises quickly established. The unforgeable nature of the data guaranteed by the timestamp server ensures the authenticity of the data on the blockchain, which makes it possible for enterprises to supervise each other, and the audit work in the supply chain is easy to carry out, which can improve the operation efficiency of the supply chain. The transparency and openness of the data in the supply chain ensures that the data is difficult to cheat in the process of transmission. At the same time, the special encryption measures of the blockchain make the data on the supply chain difficult to crack, which further provides security for the data, and ensures the security of the data in the supply chain in the circulation process.

3 Design of rice supply chain information management consensus mechanism based on blockchain

3.1 Rice supply chain selection based on blockchain

According to the degree of decentralization, blockchain can be divided into public chain, alliance chain and private chain. In the public chain, there is no user authorization mechanism and any centralized nodes. All nodes are peer-to-peer and can read and write on the blockchain. The blockchain adopted by bitcoin is a typical public chain. The speed of the alliance is second only to that of the public chain. The alliance chain is only open to some specific organizations, and the generation of blocks is determined by some nodes. Therefore, not all nodes can read and write to the blockchain. When building a blockchain between different institutions, alliance chain is usually chosen. The weakest degree of decentralization is the private chain open to a single institution. Private chain has weak

decentralization and extremely fast processing speed, which can be widely used in enterprises. Therefore, in the design of rice supply chain information management, alliance chain is selected to build the platform.

3.2 Design of consensus algorithm for information management of rice supply chain based on blockchain

In the initial bitcoin blockchain system, the consensus algorithm is proof of work (POW), which is used to deal with denial of service attacks and other service abuse countermeasures. It requires the client to carry out a certain amount of calculation, allowing nodes to compete with each other through computing power. In bitcoin network, workload proof is the main work to be done in "mining". In this process, miners solve the puzzle of workload proof through continuous double SHA-256 calculation based on their own computing power. Nodes are independent of each other, and each node allocates resources according to the proportion of computing power, so as to achieve the goal of "mining" The purpose of the heart. In addition, workload proof also increases the cost of attacking the system. In order to successfully attack the blockchain, you often need to calculate yourself to reach 51% of the total computing power. However, the profit obtained by the attacker through the attack is not worth the attacker to pay such a large cost. Therefore, the workload proof also ensures the security of the blockchain to a great extent. But there are still some problems in POW algorithm. For example, it requires nodes to do a lot of calculation, which leads to large energy consumption. Moreover, in bitcoin system, the generation time of new block is about 10 minutes, which is not suitable for most transactions in other scenarios. Therefore, based on the proof of workload, proof of Stack (POS) has been proposed and become a new consensus mechanism instead of competitive hash operation in pow. In POW mechanism, nodes with strong computing power get higher trust, while in POS mechanism, nodes with more tokens and older coins have more rights and interests, and get more trust The higher. In addition, the commonly used consensus algorithms are delegated proof of stack (dPOS) and practical Byzantine fault tolerance (pBFT). Dpos mechanism refers to that the trustee of the system is selected by equity first. Only these trustees have the right to book in the blockchain. When the transaction occurs, the trustee is responsible for bookkeeping on the blockchain in turn. Pbft algorithm is an algorithm that allows a small number of nodes to reach a consensus in the case of errors. When a transaction occurs, each node can vote for the transaction. If the voting ratio is higher than a certain proportion, the block can be connected to the blockchain. This algorithm completes the consensus process in the blockchain through the minority obeying majority mechanism. In practical applications, different blockchains often choose their own consensus algorithm according to their own degree of decentralization and application scenarios. For example, companies can build private chains within themselves. In this case, due to the hierarchical structure within the enterprise, they can usually choose to compromise the degree of decentralization rather than choose In order to achieve the purpose of high efficiency and low cost, other algorithms with fast operation speed and less energy consumption are adopted.

PBFT algorithm is a mature algorithm commonly used in alliance chain. In rice supply chain information management, we use the improved Byzantine fault tolerance (dBFT). This method first selects consensus nodes in the supply chain network according to the proportion of equity held by each enterprise in the supply chain, and then reaches a consensus through voting. Among them, only the consensus node has the right to account in the blockchain. This consensus method has good fault tolerance and is suitable for the alliance chain system built in the supply chain. In the information management of rice supply chain, the core enterprises in the supply chain have large shares, which can be used

as consensus nodes in the whole alliance chain. When a new transaction occurs, the consensus node can generate blocks, that is, bookkeeping in the blockchain. The newly generated block needs to vote in all consensus nodes. When the number of votes passed exceeds a certain proportion, the block can be used As the correct block, which can be connected to the existing blockchain. In the alliance chain of rice supply chain system, not all transaction information is open to the outside world. Except for the core enterprises with high degree of trust in the supply chain, only the participants involved in the block have the right to read the transaction information. This consensus algorithm not only ensures the ability of sharing data in the supply chain, but also protects the privacy of the participants in the supply chain.

In the practical application of rice supply chain, because the source of rice may come from many different places of origin, and in the process of goods from the producer to the final purchase by customers, the transaction information is usually very scattered, which also leads to the commodity problems in a certain link, consumers are difficult to trace the goods The specific source information, in addition, even if there is no problem with the goods, it is difficult for consumers to get feedback information in time after the goods are out of the warehouse, thus providing an opportunity for fake and inferior products.

In the practical application of rice supply chain, because the source of rice may come from many different places of origin, and in the process of goods from the producer to the final purchase by customers, the transaction information is usually very scattered, which also leads to the commodity problems in a certain link, consumers are difficult to trace the goods The specific source information, in addition, even if there is no problem with the goods, it is difficult for consumers to get feedback information in time after the goods are out of the warehouse.

4 Realization of Information Management Side Chain of Rice Supply Chain Based on Blockchain

Side chain technology (i.e. wedge type side chain technology) refers to the technology to realize the safe transfer of assets between multiple blockchains. Therefore, even if the main chain and the main chain are not damaged, it means that the value of the main chain can not be broken between the main chain and the main chain. There are two ways to realize the value transfer between the main chain and the side chain, which are two-way wedging and joint wedging. Two way wedging is a mechanism of transferring assets between main chain and side chain with a fixed exchange rate through simplified payment verification proof (SPV). Joint wedging refers to an asset transfer mechanism between the main chain and the side chain, which locks or unlocks assets through multiple signature addresses controlled by multiple notaries and the control rights of multiple parties. The emergence of side chain provides more possibilities for blockchain technology, even if the side chain technology (i.e. wedge type side chain technology) refers to the technology to realize the safe transfer of assets between multiple blockchains. The side chain refers to another block chain parallel to the main chain. At the same time, the side chain can realize the two-way transfer of value with the main chain, but the side chain and the main chain are isolated. Therefore, even if the encryption in the side chain is cracked, the main chain will not be damaged. There are two ways to realize the value transfer between the main chain and the side chain, which are two-way wedging and joint wedging. Two way wedging is a mechanism of transferring assets between main chain and side chain with a fixed exchange rate through SPV. Joint wedging refers to an asset transfer mechanism between the main chain and the side chain, which locks or unlocks assets through multiple signature addresses controlled by multiple notaries and the control rights of multiple parties. The emergence of side chain provides more possibilities for blockchain technology, which not only enables the traditional

blockchain to support more asset types such as stocks and bonds, but also provides more convenient technical support for the emergence and mass use of smart contracts. Considering the asset transfer between the side chain and the main chain and the isolation between the side chain and the main chain, the side chain can be constructed by joint wedging in the rice supply chain system to help the main chain to expand and test run new functions and new businesses, and build an intelligent contract system on the side chain, so as to achieve the goal of the production, suppliers, sellers and consumers in the purchase, development and trial operation of new functions and new business Payment, transportation, financing, tax and other aspects of the circulation of multi-party Intelligent Implementation and monitoring. Fig. 1 lists some smart contracts in rice supply chain information management from three aspects of supply chain acquisition, distribution and sales.

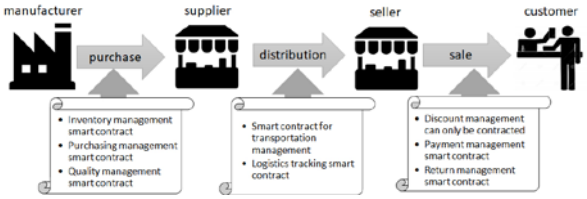

Fig. 1. Supply chain smart contract based on blockchain.

5 Application Examples

Taking a brand rice in Heilongjiang Province as an example, this paper constructs the information management of Rice Industry Supply Chain Based on blockchain. After the rice is purchased by the general supplier from various rice manufacturers, the rice is transported to the distribution enterprises in Beijing, Tianjin, Shanghai, Jiangsu and Zhejiang, Guangdong and other regions by rail transportation or land sea combined transportation, and finally delivered to consumers through local retailers.

In this brand rice supply chain system, some enterprises with large shares in the upstream and downstream, that is, the core enterprises in the supply chain, can be set as consensus nodes in the blockchain. These consensus nodes have the right to account in the blockchain. When other nodes in the blockchain want to become consensus nodes, the existing consensus nodes need to vote. After the voting is passed, the newly added nodes have the same permissions as the original consensus nodes. When a rice transaction is completed, these large enterprises have the right to record the transaction information in the block, and other consensus nodes can vote for confirmation of the transaction information by means of digital signature. Because the encryption technology of blockchain ensures the unforgeability of digital signature, the security of enterprise voting information is ensured. When the block is voted by the consensus node, it will be connected to the end of the existing blockchain and time stamped. The transaction here can refer to the transaction of rice in every circulation link in the supply chain. In the existing situation, some goods provide consumers with the service of scanning two-dimensional code or bar code to understand the origin of the goods. Therefore, the transaction information of rice in every link of the supply chain will be truthfully recorded in the blockchain. Consumers can check the real circulation links of rice according to the specific identity code of rice, and truly understand how the brand of rice is transported and traded to their own hands through layers of transportation.

Through the intelligent contract technology of blockchain, we can do a better and more comprehensive intelligent management and control of all aspects of the rice supply chain, and greatly save the human cost. For example, in the rice purchase process, through the smart contract, the supplier can timely understand the inventory situation, purchase from

the manufacturer in time, and use the smart contract to monitor the storage conditions and quality of rice, so as to ensure the high-quality rice source of the brand. In the process of rice transportation, the temperature and humidity in the process of rice transportation can be monitored in real time through smart contract, and the corresponding prompt will be given once the temperature and humidity are not up to standard. In addition, in the sales process, online payment platform can also be built through smart contract to realize intelligent online payment on delivery, default refund and other services.

6 Prospect

The application of blockchain technology in the field of supply chain management and the construction of supply chain information management will bring essential changes to the management of supply chain, and form a new theory and method of information storage, transmission, processing and retrieval. At present, with the continuous development of supply chain finance, many credit risk problems are still unavoidable in the financing process. Due to the existence of asymmetric information, it is difficult for small and medium-sized enterprises to obtain complete credit information. Compared with the core enterprises in the supply chain, small and medium-sized enterprises are weak in response to emergencies, and usually face greater risks More difficult.

The addition of blockchain technology can provide a new risk management support information management for the supply chain, and open up a new situation for the financing of small and medium-sized enterprises in the supply chain. First of all, the intervention of blockchain breaks through the isolated data island between the upstream and downstream of the supply chain, broadens the data sources available on the supply chain, and ensures the authenticity and credibility of the data by using its unforgeable and unforgeable characteristics. The distributed bookkeeping method makes every transaction record recorded on the blockchain as the basis of credit granting and provides financing for enterprises in the supply chain The problem provides a sufficient data base.

In addition, the application of blockchain is still in the initial stage of development. The lack of infrastructure and many uncertainties in practical application have brought many challenges to the development of blockchain. Although many enterprises have not put the blockchain technology into use, they are still waiting for its further maturity in practical application. Nevertheless, blockchain has now demonstrated its powerful processing ability in terms of value and assets. In addition, the application exploration and practice of blockchain technology in various aspects are constantly developing, and it is believed that it will eventually lead the enterprise form of many industries from a completely closed system to a widely open distributed system.

This work was supported by the National Social Science Foundation of China (18ZDA309), the National Natural Science Foundation of China (71531012, 62072463), the Natural Science Foundation of Beijing (4172032), and the Project of Beijing Academy of Capital Development and Strategy Renmin University of China.

References

1. Y. Yuan, F. Wang. Development status and prospect of blockchain technology. Acta Automatica Sinica, (2016) **42** 481-494
2. H. Song. Innovation trend of supply chain finance based on industrial ecology. China's Circulation Economy, (2016) **30** 85-91,
3. X. Ma, M. Du. Supply chain financial service platform based on blockchain, Big Data, (2018) **4** 13-21