Research on the Application of Blockchain in the Traceability System of Agricultural Products

Jing Li, Xinyan Wang
Intelligent Science and Information Engineering College
Xi'an Peihua University, Xi'an, China
28328715@qq.com, 36404843@qq.com

***Abstract*—You must be familiar with the word "organic agricultural products", but because of the lack of universal credit vouchers in the market, people can't be reassured by the purchase of organic agricultural products. Therefore, it is particularly important to trace the agricultural products. The Blockchain technology has developed rapidly in recent years. This technology has aroused the attention of experts and scholars, and has become a hot topic. The Blockchain has the characteristics of decentralization, information security and trustworthiness. If the Blockchain is applied to the traceability system of agricultural products, the authenticity of organic agricultural products can be well tested. This paper introduces the formation process of Blockchain, describes the characteristics of Blockchain, and analyzes the model and the key technologies of Blockchain system. At last, the paper constructs a traceability system model based on the Blockchain technologies.**

Keywords—Blockchain technologies; Organic agricultural products; Traceability system

I. INTRODUCTION

With the continuous improvement of the material life level, people's demand for the quality of agricultural products is getting higher and higher. People pay more attention to organic, healthy and safe agricultural products.However, in the market, the fake organic agricultural products can be seen everywhere. Because of the lack of unified standard for judging organic agricultural products, the authenticity of organic agricultural products can not be confirmed. Faced with this phenomenon, the technology of Blockchain characterized by trust, openness, collective maintenance and no- tampering can seal the organic agricultural products with "credit certification". By installing a physical indicator sensor on a farm, we can collect the real-time information about fertilization, watering, pest monitoring and so on. This information will automatically enter the traceability system after the data is generated. Removing the intermediaries and the anthropogenic factors, all the information is true and reliable[1].

II. WHAT IS THE BLOCKCHAIN

Blockchain, in simple terms, is composed of "block" and "chain". It is a kind of underlying technology based on distributed accounting. It is a new application model about distributed data storage, point to point transmission, consensus mechanism and encryption algorithm. Bitcoin is popular in these two years, it is one of the applications about Blockchain.

In a narrow sense, Blockchain is a chain data structure composed of data blocks sequentially connected in time sequence, and it is a distributed accounting book that is not tampered with and cannot be forged by cryptography.

In essence, the Blockchain is a distributed public account, which links each block into a chain. It enables a group of interconnected computers to maintain a account together safely, each computer is a database (server), and there is no need for the third party server in the middle. Therefore, the Blockchain is not a particular kind of software, but a design idea of a specific technology.

The main function of the Blockchain is to store information. Any information that needs to be saved can be written into the Blockchain and also can be read out from Blockchain, so Blockchain is a database. Anyone can set up a server and join the Blockchain network, then becomes a node. In the world of Blockchain, there are no central nodes, each node is equal, and the whole database is kept. You can write / read data to any node, because all nodes are finally synchronized to ensure that the Blockchain is consistent.

III. THE FORMATION PROCESS OF BLOCKCHAIN

Block chains are made up of blocks. A block is very like a database record, and each time the date is written, it is to create a block. Each block contains two parts: block head and block body. The block head contains a number of eigenvalues of the current block: the generation time, the Hash of the actual data (that is, the block body), the Hash of the last block, and so on. "Hash" means that a computer can calculate a characteristic value of the same length for any content. The Hash length of the block is 256 bits, that is to say, no matter what the original content is, a binary number of 256 bits will be calculated at the end. And it can be guaranteed that as long as the original content is different, the corresponding Hash must be different. The block corresponds to Hash one by one, and the Hash of each block is calculated for the "block head". That is to say, the characteristic values of the block are connected in order to make up a very long string, and then the Hash is calculated for the string. The block head contains a lot of content, including the Hash of the current block, and the Hash of the previous block. This means that if the content of the current block changes, or the Hash of the previous block changes, it will certainly cause the Hash change of the current block.

978-1-5386-1803-5/18/$31.00 ©2018 IEEE

This is of great significance to the Blockchain. If someone changed a block, the Hash of the block would change. In order to make the subsequent blocks can be connected to it (because the next block contains the Hash of the previous block), the person must modify all the blocks in turn, otherwise the blocks that has been removed will be separated from the block chain. Because Hash's calculation is very time-consuming, it is almost impossible to modify a number of blocks in a short time, unless someone has mastered the computing power of more than fifty-one percent of the whole network.

It is through this linkage mechanism that the Blockchain ensures its own reliability, and once the data is written, it cannot be tampered. It's like history, what happened was happening, and never changed. Each block is connected to the previous block to form a chain, which is the origin of the name "Blockchain".

During the formation of Blockchain, there is another problem should be solved: if two persons write data to Blockchain at the same time, that is to say, there are two blocks join the Blockchain at the same time, because they are all connected to the same previous block, so that a bifurcation is formed.

Which block should be adopted at this time? The rule now is that the new node always uses the longest Blockchain. If the Blockchain has a fork, which branch will look at the back of the bifurcation point to reach 6 new blocks (called "six confirmation"). According to ten minutes and one block calculation, one hour can be confirmed. Because the speed of generation of new blocks is determined by computing power, this rule means that the branch that possesses most computing power is the authentic Blockchain.

IV. THE MODEL AND THE KEY TECHNOLOGY OF BLOCKCHAIN SYSTEM

A. The Model of Blockchain system

Generally speaking, the Blockchain system is composed of data layer, network layer, consensus layer, incentive layer, contract layer and application layer. The Blockchain system model is shown in Figure 1.

Among them, the data layer encapsulates the underlying data blocks and the underlying data and basic algorithms, such as data encryption and timestamp. The network layer includes distributed network mechanism, data communication mechanism and data verification mechanism, etc. The consensus layer mainly encapsulates all kinds of consensus algorithms for network nodes. The incentive layer integrates the economic factors into the Blockchain technology system, mainly including the issue mechanism and the distribution mechanism of the economic incentive. The contract layer mainly encapsulates all kinds of scripts, algorithms, and intelligent contracts, which are the basis of the programmability of Blockchain. The application layer encapsulates various application scenarios and cases of Blockchain. In this model, the chained block structure based on timestamp, the consensus mechanism of distributed nodes, the economic incentive and flexible programmable intelligent contracts based on consensus computing power are the most representative innovation of Blockchain technology.

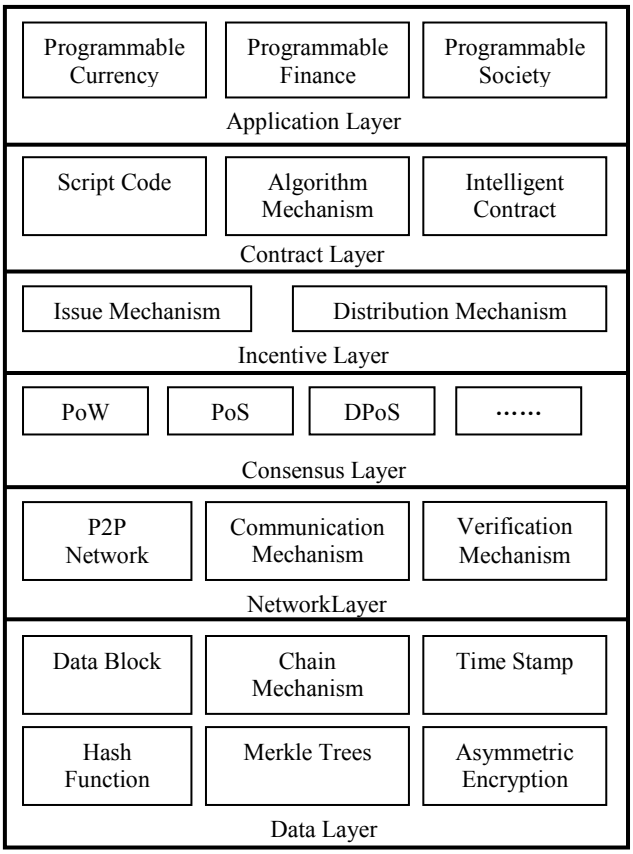

Fig.1. Blockchain System Model

B. The Key Technology of Blockchain system

The Blockchain mainly solves the problem of trust and security of the transaction, so it puts forward four technological innovations for this problem

(1) The Distributed Account

Distributed account means transaction accounting is done by multiple nodes distributed in different places, and each node records the complete account, so they can participate in the supervision of transaction legitimacy, and they can also testify jointly. Different from the traditional center accounting scheme, no single node can record the accounts alone, so then to avoid the possibility of single entry is controlled or bribe note books. On the other hand, because the accounting nodes are enough, in theory, the accounts will not be lost unless all the nodes are destroyed, thus the security of the account data is guaranteed.

(2) Asymmetric Encryption and Authorization Technology

The transaction information stored on the block chain is public, but the identity information of the account is highly encrypted. It can be accessed only when the data owner is authorized, so as to ensure the security of the data and the privacy of the individual[2].

(3) The Consensus Mechanism

The consensus mechanism is how to reach a consensus between all the bookkeeping nodes and identify the validity of a record. This is both a means of identification and a way to prevent tampering. Blockchain has proposed four different consensus mechanisms for different application scenarios, and balance between efficiency and security. Taking bitcoin as an example, the workload proof is used. It is possible to forge a non-existent record only when controlling the accounting node of more than 51% of the total network. When there are enough nodes to join the Blockchain, it is basically impossible, thus eliminating the possibility of counterfeiting[3].

(4) The Intelligent Contract

The intelligent contract is based on these trusted and no tampered data, and it can execute some predefined rules and clauses automatically. Taking insurance as an example, if everyone's information (including medical information and risk information) is authentic and credible, it's easy to make automatic claims in some standardized insurance products.

V. THE CHARACTERISTICS OF BLOCKCHAIN

A. *Decentralization*

Due to the use of distributed accounting and storage, there is no centralized hardware or management organization. The rights and obligations of any node are all equal. The data blocks in the system are maintained by the nodes which have the maintenance function in the whole system[4].

B. *Openness*

The system is open. Besides the private information of the transaction parties is encrypted, the data of the Blockchain is open to everyone. Anyone can query the Blockchain data and develop related applications through the open interface, so the whole system information is highly transparent.

C. *Autonomy*

Blockchain adopts the rules and protocols based on consensus (such as a transparent algorithm), it allows all nodes in the whole system to be able to exchange data freely and safely in a trusted environment, and it makes the trust of "man" changed to the trust of the machine, and any human intervention does not work.

D. *The Information cannot be tampered with*

Once the information is verified and added to the Blockchain, it will be permanently stored. Unless we can control more than fifty-one percent nodes in the system at the same time, the modification to the database on a single node is invalid, so the data stability and reliability of the Blockchain are very high.

E. *Anonymity*

Due to the exchange between the nodes follows a fixed algorithm, the data interaction does not need to be trusted. (The rules of program in the Blockchain will judge whether the activity is valid.) Therefore, the counterparty does not have to make the other person trust by the way of public identity, which is very helpful to the accumulation of credit.

VI. THE APPLICATION OF BLOCKCHAIN TECHNOLOGY IN THE TRACEABILITY SYSTEM OF AGRICULTURAL PRODUCTS

Since 2003, China has continuously promoted the construction of the traceability system of food, and traceability Technology has also made some progress. Compared with the traditional technology of agricultural product traceability system, the traceability system based on Blockchain technology has no difference from the front-end. Relying on the network, it collects various kinds of data with the help of radio frequency device, object fingerprint and recognition device, all kinds of application sensors and information acquisition terminals. The difference between the two is the back-end. The Blockchain has the characteristics of decentralization. Therefore, in the technical level, the Blockchain is no-database, as shown in Figure 2.

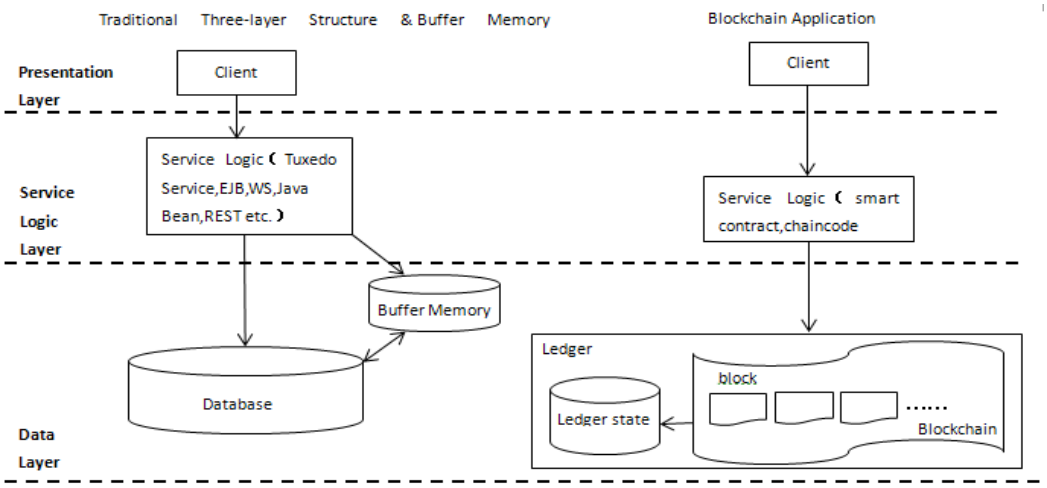

Fig.2. Blockchain's De - Database

The application of the Blockchain is not the same as that of the tradition because it keeps the data in the ledger and reads and writes the ledger through an intelligent contract. An intelligent contract is a piece of code. Its functions are similar to those of traditional applications such as EJB, Servlet, Web service, Java Bean and so on. The intelligent contract is used to implement service logic. The ledger mainly includes two pieces: Blockchain and state. Blockchain is a series of connected blocks. The Blockchain corresponds to a file which is used to record historical transactions. Blockchain is written in an append way, and it can not be tampered. State corresponds to the current state of the ledger, which is a Key-value database.

Taking agricultural products as an example, the Blockchain cloud service BCS of the Oracle is used at the back-end. The front-end adopts the open source framework JET of Oracle[5]. Build a traceability system model based on Blockchain technology, as shown in Figure 3.

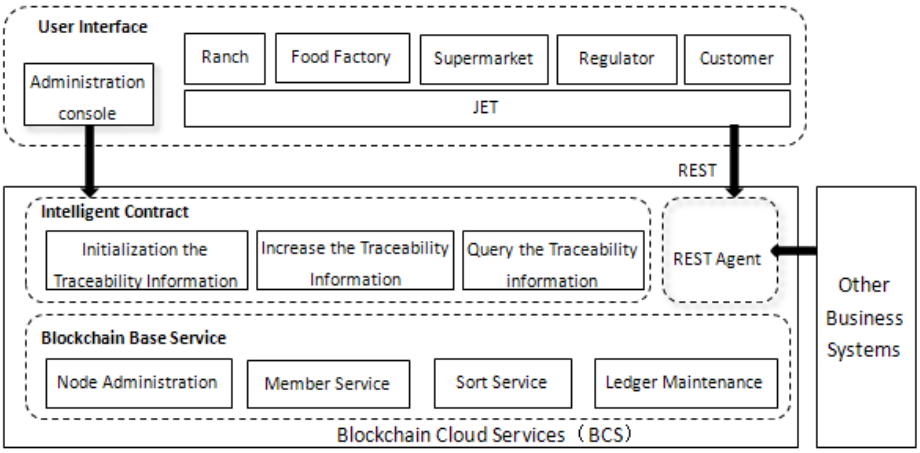

Fig.3. The Traceability System Model Based on Blockchain Technology

Blockchain provides a new tool for tracing business, compared with the previous central ledger model, the distributed ledgers guarantee the openness and transparency of the ledger and avoid the possibility that the stakeholders can tamper with the ledgers. Compared with the traditional traceability system, the application of Blockchain technology to the traceability system has obvious advantages, as shown in table I.

TABLE I. The Advantages of Traceability Platform Based on Blockchain

Comparative Items	Traceability System Based on Blockchain	Traditional Traceability System
Data Authenticity	Data cannot be tampered with	The data can be tampered with in the background
Data Security	Distributed multi node complete data storage	Single center node data storage
Government Regulation	The data is automatically and synchronously stored in the government node	The government can't trust the authenticity of the traceability data
User Perception	The information of the traceability scene can be verified	Dubious information of traceability scene

VII. CONCLUSIONS

Blockchain technology is applied to the traceability system of agricultural products, the technical implementation is not only to change the traditional product traceability system into a central server platform based on the underlying protocol of the Blockchain, but to provide an interactive network of data and information with a weak centralization of the parties. In this network, retailers, wholesalers, agricultural products quality testing institutions, seed traders, farmers, and financial organizations that provide financing credit can share real time data on chains. Through the strict encryption characteristics of Blockchain and the chain ledgers, people can enjoy the convenience, efficiency, and trust. In order to improve their enjoyment of these rights, these nodes also shoulder the obligation to jointly maintain the reliability of the data.

As the characteristics of the data that can not be tampered and the data can be synchronized in real time, the Blockchain technology is suitable for various traceability classes, such as vehicle parts traceability, drug traceability and so on.

REFERENCES

[1] Wang Deng, Zeng Xiaoshan, Bai Qianlan, Sun Yaojie. Traceability Technology of Food Safety Based on Blockchain [J]. Food Science.2018,02.

[2] [2] Tuo Xiaozhong. Research and Design of Encrypted Information Backup System Based on Blockchain [D]. Southwest Petroleum University.2017.

[3] [3] Huang Zheng, Li Xiangxue, Lai Xuejia, Chen Kefei. The Technology and Application of Blockchain [J]. Journal of Information Security Research, 2017,3..

[4] [4] Zhang Hanyi. Discussion on the Development Path of China's Agricultural Products E-commerce Based on Blockchain [J]. Business economy research.2017,12.

[5] Lv Furong, Chen Sha. Research on the Construction of China's Agricultural Product Quality Safety Traceability System Based on Blockchain Technology [J]. Rural Finance Research.2016,12.