Food Safety Traceability Method Based on Blockchain Technology

Yajie Wang¹, Kai Chen¹, Miao Hao² and Bing Yang¹*

¹ Guizhou Provincial Key Laboratory of Public Big Data, Guiyang, Guizhou, 550000, China
² Guizhou Academy of Sciences, Guiyang, Guizhou, 550000, China
*Corresponding author’s e-mail: yangbing@gzbsi.com

Abstract. Food safety is a major issue related to the vital interests of the people. In recent years, food safety incidents have emerged in an endless stream in China. However, the existing food safety traceability methods lack of data sharing, which makes it difficult to conduct unified supervision on food safety. In view of the problems existing in the current food safety traceability method, this paper introduces blockchain technology in food safety traceability field, selects milk as the object of food safety traceability in this paper, analyzes the whole process of milk supply chain, designs the overall framework of milk traceability scheme according to the demand analysis and design principles of milk safety traceability scheme, and designs the scheme's business function module, and chooses ECP-96 traceability coding scheme to ensure the uniqueness as well as security of milk traceability source. In view of the current application of blockchain technology, Hyperledger Fabric is creatively selected as the blockchain technology platform, and Go language is used to develop and implement the traceability method. Through the deployment of multiple nodes and functional testing, the expected food safety traceability goal is achieved.

1. Introduction

The current situation of food safety is worrying. In view of the frequent safety incidents in the food industry, China has formulated many relevant food safety laws and regulations to supervise and restrict the food production and processing industry, and has achieved certain results. However, if we want to really supervise every link of the food supply chain, ensure the quality and safety of food, and truly protect the rights and interests of consumers, we need to establish a set of perfect food traceability system, because food safety problems may occur in any link of food circulation. By recording and tracking the whole process of food from production to sales, and uploading the data of each link to the food traceability system, consumers can query the whole process information of the supply chain at any time and anywhere to meet the needs of consumers for food safety. At the same time, it can also facilitate the supervision and control of food quality by the regulatory authorities. Once the food safety problems are found, the specific link can be found out through the traceability system, which can quickly and accurately locate the person responsible for the relevant safety accidents, and at the same time, the product can be recalled quickly [1].

The research on food traceability is very necessary. At present, the main methods of food traceability are: traditional method traceability, physical technology traceability, chemical traceability and biological traceability. However, although there are many methods for food traceability, the implementation efficiency is not high, can not be widely used, and the effect is not very ideal. At
present, there are many disadvantages in the commonly used centralized traceability methods. For example, before the enterprise information can not be shared, the traceable information is less, the data is not open and transparent, the data is easily tampered with in the hands of the core enterprises, and the traceability methods of each enterprise are also lack of unified management and planning. Based on the problems of the above food traceability methods, this paper proposes a food safety traceability method based on blockchain technology. Since the blockchain technology has the advantages of decentralization, distributed storage, openness and transparency, and can not be tampered with, the application of blockchain technology in the field of food traceability will effectively solve the problems existing in the current centralized traceability method. This method can reduce the supervision cost, transaction complexity and transaction risk, and improve the safety of food and the credibility of information records. To ensure the authenticity and reliability of the information recorded in the system, ensure the safety traceability of food, and solve the problems existing in the current food traceability methods, such as information collection is not standard, data storage process has security risks, centralized methods are easy to be attacked, and information is not shared between enterprises. Every transaction on the blockchain can not be tampered with and traceable. Once a certain link of food circulation goes wrong, it can be traced back to the specific responsible person through this method [2-3].

2. Blockchain Technology

2.1. Asymmetric encryption algorithm
Asymmetric encryption algorithm occupies an important position in the blockchain, the main role is to ensure the security of the data on the blockchain. In the asymmetric encryption algorithm, there is a pair of keys, namely public key and private key. The public key is stored in the database publicly. All users in the system can see the public key of other users, and the private key is saved by the user himself. The private key is a string of fixed length strings, which is generated by the system using SHA256 hash algorithm, and then the private key is generated by other hash algorithms. The public key can be calculated from the private key, but the private key cannot be calculated from the public key in reverse. Asymmetric encryption algorithm is mainly used to realize data encryption and signature verification [4-5]. The schematic diagram of asymmetric encryption algorithm is shown in Figure 1.

![Figure 1. Schematic diagram of asymmetric encryption algorithm.](image)

The data encryption process of the asymmetric encryption algorithm is: the sender user 1 uses the public key of the receiver user 2 to encrypt the information to be sent. After receiving the cipher text,
the user 2 decrypts the information with its own private key to obtain the plain text. This process guarantees To improve the security of data transmission, the function expression of this process is:

\[
E(key_1, P) = C \tag{1}
\]
\[
D(key_2, C) = P \tag{2}
\]

Where \( E \) represents the encryption algorithm, \( D \) is the decryption algorithm, \( key_1 \) is the encryption key, \( key_2 \) is the decryption key, \( P \) is the plaintext information to be transmitted, and \( C \) is the ciphertext obtained after plaintext encryption. The process of data signature and verification of asymmetric encryption algorithm is as follows: sender user 1 signs the message to be sent with his private key, and receiver user 2 verifies the signature with user 1’s public key after receiving the information sent by user 1. The process of signing and verifying data with asymmetric encryption algorithm can prove the identity of both parties to the transaction and ensure the correctness and security of information transmission integrity.

2.2. Hyperledger Fabric

Hyperledger is the first time to apply blockchain technology to the application scenario of distributed alliance ledger, which introduces permission control, and further increases the security mechanism of blockchain system. The structure of Hyperledger mainly includes membership system, blockchain and code on chain. The characteristics of Hyperledger are to provide modular function, high security, interactive operation and sound interface. Among them, the most widely used, most active and most famous is the Hyperledger fabric framework. Hyperledger fabric can be used to build distributed application solutions, mainly including ledger, transaction, chain code, event and authority management modules. The Hyperledger fabric adopts a modular design, which is divided into three layers from top to bottom, namely network layer, consensus mechanism, authority management and business layer [6]. The overall functional module structure is shown in Figure 2 below.

![Overall function module diagram of Fabric](image)

Since Hyperledger Fabric is a good application of Block Chain technology, this method chooses the architecture of Hyperledger Fabric as the technical platform of block chain, and will do the application research of traceability method based on Fabric Framework.
3. Design of Milk Safety Traceability Scheme Based on Block Chain Technology

3.1. Overall schema structure
This paper designs a milk safety traceability scheme based on block chain technology, and the overall architecture is shown in Figure 3.

![Architecture diagram of milk traceability scheme](image)

From the bottom up, there are mainly seven layers. At the bottom is the operation layer, which is mainly responsible for the data collection of the whole process from milk production to sales. Data collection layer mainly uses bar code, RFID radio frequency technology to collect milk-related information, including the origin of dairy cows, feed, vaccine status, health environment, nutritional content of milk, production date, shelf life, storage environment and conditions, logistics information and sales information, which are important information related to milk quality and safety. The data layer stores the information collected from the job layer, mainly composed of the underlying technologies of block chain, including the data structure of block chain, Merkle tree, asymmetric encryption algorithm and other core technologies. Consensus layer and network layer refer to the consensus mechanism of block chain, including workload proof mechanism, equity proof mechanism and Byzantine consensus mechanism, which are mainly used to ensure the consistency of information of all nodes in the system. The network layer mainly uses the whole method of network dissemination and message validation. Block chains mainly use peer-to-peer network, that is, P2P network, for data transmission without centralized servers. Business and application layers are mainly the rules of milk production safety and transportation, mainly through intelligent contracts to write related rules. The presentation layer mainly uses B/S architecture, which is browser/server mode. The advantage of using this mode is that as long as there is a network, you can query, browse and other business operations anytime, anywhere, without downloading the client. The presentation layer presented to
users also uses web page technologies such as HTML, CSS and JS. The user layer mainly targets the milk producers, processors, transporters, related regulatory departments, core related enterprises and final consumers. Producers, processors, transporters and related core enterprises are responsible for the entry of information. Regulatory departments and consumers can query product information through this system.

3.2. Design of network architecture

This method proposes a milk security traceability network architecture based on blockchain technology, as shown in Figure 4.

![Figure 4. Network architecture](image)

In order to access the system, the processing workers, packaging and storage operators, logistics transporters, sellers, regulatory authorities and consumers in the milk supply chain need to register first. The regulatory authorities can monitor the authenticity of the information in the milk supply chain process, and if there is a problem in a certain link, the specific responsible person can be traced immediately through this method. The important information related to milk products can be input by producers, packers, transporters and sellers. Consumers have the right to query traceability information, but they have no right to modify information. Users with different identities in the supply chain will have different access and read-write permissions. The relevant regulatory departments and law enforcement departments have the highest authority of the system to monitor the orderly and stable operation of each link of the method.

After successful registration, each user will get a public key and a private key. The public key pair is public in the whole Traceability Method and can be seen by all participants. It is mainly used for information verification. The private key is kept by the user himself, which is the key to verify the identity information in the login system and information input. The information of the whole process of milk supply chain from cow breeding to sales is stored in the milk safety traceability method based on blockchain technology. A participant cannot modify the running rule of the traceability method, because the rule is automatically executed by the smart contract in the blockchain, and the smart
contract is the code written in advance to run in the isolated environment. Therefore, the milk safety traceability method based on blockchain technology can ensure the authenticity and reliability of traceability information, and the data in the system will not be arbitrarily changed by illegal nodes.

3.3. Traceability coding design

In the design of milk safety traceability scheme based on blockchain technology, the design of a unified and unique traceability source code of products is the basis for the realization of complete traceability function, and it is necessary to ensure that each product has a unique corresponding traceability source code, so as to realize the real and effective traceability of milk products. Consumers can query the detailed information of each link of the milk supply chain by querying the source code. Once a milk safety incident occurs, the relevant regulatory departments and law enforcement departments can quickly track the specific responsible person through the information of traceability method, and timely recall the products, which will greatly improve the efficiency of the government and maximize the protection of consumers' rights and interests. Therefore, the design of milk traceability code is very important. EPC C electronic product code is adopted in this scheme. The data is uploaded through RFID and the information is transmitted through the blockchain network. The advantage of EPC code is that each commodity has a unique code, good confidentiality and anti-counterfeiting, and the stored data has international standards [7-8]. There are three types of EPC codes, namely EPC-64, EPC-96 and EPC-256. In this paper, EPC-96 code is selected, and the encoding method is hexadecimal.

4. Conclusion

This paper studies the Traceability Method of food safety based on blockchain technology. This paper analyzes and studies the key security technology of blockchain, and creatively selects hyperledger Fabric. By selecting milk as the object of food traceability, we study the milk security traceability method and propose the milk security traceability scheme based on blockchain technology, and design the corresponding overall architecture and network architecture. Finally, the traceability code is introduced to code it. Using this scheme for food traceability, the safety of data can be effectively guaranteed, and the data is not easy to be tampered with, which reduces the centralization degree of the traditional traceability system and makes the data collection more standardized and accurate.

Acknowledgments

This work was supported by Major Scientific and Technological Special Project of Guizhou Province (No.20183002), Scientific and Technological Project of Guizhou Province (No.20185404).

References

[1] Allard, M.W., Bell.R., Ferreira, C.M., et al. (2017) Genomics of foodborne pathogens for microbial food safety. Current Opinion in Biotechnology., 49: 224-229.
[2] Tsang, Y.P., Choy, K.L., Wu, C.H., et al. (2019) Blockchain-driven IoT for Food Traceability with an Integrated Consensus Mechanism. IEEE Access., 7: 129000-129017.
[3] Wu, M., Wang, K., Cai, X., et al. (2019) A Comprehensive Survey of Blockchain: From Theory to IoT Applications and Beyond. IEEE Internet of Things Journal., 6: 8114-8154.
[4] Wang, Y., Quan, C., Tay, C.J. (2016) Asymmetric optical image encryption based on an improved amplitude–phase retrieval algorithm. Optics & Lasers in Engineering, 78: 8-16.
[5] Monika Agrawal, Pradeep Mishra. (2012) A Modified Approach for Symmetric Key Cryptography Based on Blowfish Algorithm. International Journal of Engineering & Advanced Technology, 6:79-83.
[6] Kramer M. (2019) AN OVERVIEW OF BLOCKCHAIN TECHNOLOGY BASED ON A STUDY OF PUBLIC AWARENESS[J]. Global Journal of Business Research.,
13:83-91.

[7] Brubaker S A, Wilson D. (2010) Coding and traceability: cells and tissues in North America. Cell & Tissue Banking., 11:379-389.

[8] Strong D M, Rüdiger von Versen. (2010) Coding and traceability for products of human origin. Cell & Tissue Banking., 2010, 11:325-327.