

A Food Traceability Framework Based on Permissioned Blockchain

Jiuliang Liu^{1,*}, Xingming Sun¹ and Ke Song²

¹School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing, 210044, China

²Xuchang XJ Wind Power Technology Co., Ltd., Xuchang, 461000, China

*Corresponding Author: Jiuliang Liu. Email: 17751750682m@sina.cn

Received: 27 April 2020; Accepted: 28 June 2020

Abstract: In recent years, food safety problems have become increasingly serious. The traditional supply chain traceability solution faces some serious problems, such as centralization, data tampering, and high communication costs. To solve these problems, this paper proposes a food traceability framework based on permissioned blockchain. The proposed framework is decentralized, and the supply chain data of the framework cannot be tampered with. The framework divides supply chain entities into five organizations, and each organization deploys its own chaincode onto the blockchain. The chaincode specifies the query permission of each organization, which can effectively protect the user's sensitive information. The PBFT consensus algorithm adopted by the framework improves the performance of processing transactions. The transactional throughput experiment shows that the proposed framework can achieve a high number of transactions per second. Query efficiency experiment demonstrates that the framework has lower query latency and good user experience.

Keywords: Food traceability; supply chain; blockchain; chaincode

1 Introduction

Supply chain traceability is a technology that traces the life cycle of a product. It monitors the acquisition of raw materials, production, processing, transportation, distribution, and sales of products. In recent years, food safety issues such as toxic milk powder, mad cow disease and clenbuterol have frequently occurred, which has seriously threatened people's physical and mental health. Therefore, it is essential to design an excellent food traceability system for effective supervision of food supply chain.

Although food traceability has been valued by all walks of life, food traceability technology still faces many difficulties. In a distributed traceability system, each node maintains different databases and lacks a unified standard, so the cost of each node and the communication cost between nodes are very high. In addition, distributed systems are difficult to meet the performance and functional requirements of food traceability. For example, the query speed is too slow, and no advanced search function is provided.

Therefore, the centralized food traceability system is more commonly used at present. However, a centralized system requires the trust of various participants in the market, which is difficult to achieve in a market economy. When the data in the central organization is against a party, the recorded information is likely to be maliciously tampered with. And the central organization is vulnerable to a single point attack. In addition, traditional food traceability schemes are difficult to ensure consumer privacy. The administrator of the traceability system can query the consumer's personal information.

Blockchain technology provides new ideas for solving the problem of food traceability. In 2008, Satoshi Nakamoto released the Bitcoin white paper [1]. Blockchain was born as the underlying technology of Bitcoin. There is no definite central institution in the blockchain system, and it has the



advantages of immutability and security. Blockchain technology also solves the double-spend problem [2] and the Byzantine general problem [3] in encrypted digital currency, so it has attracted a lot of attention of academia and industry in recent years. The Ethereum [4] blockchain can run Turing complete scripts-smart contracts, marking the arrival of the blockchain 2.0 era. Taking advantage of smart contracts, nodes can upload business information to the blockchain and can process business logic on the blockchain. Blockchain-based traceability system can solve the centralization problem and data tampering problem of traditional traceability solutions. However, the blockchain-based traceability system still faces challenges such as improving transaction throughput, improving query efficiency, and protecting user privacy.

A food traceability framework based on blockchain is designed in this paper. The framework is based on the Hyperledger Fabric and is a permissioned blockchain suitable for enterprises. The framework divides the entities in the supply chain into five organizations, and each organization deploys its own chaincode to the blockchain. Each chaincode is responsible for processing the business of each organization, such as uploading information and querying information. Consumers can call the method of querying traceability information in the chaincode to quickly obtain the complete supply chain information of the product. The chaincodes also control the query authority of each organization, effectively protecting the user's private information.

The organizational structure of the paper is as follows. The Section 2 introduces related work; the Section 3 introduces the proposed framework in detail; the Section 4 shows the experimental results; the Section 5 summarizes the full text and looks forward to future work.

2 Related Work

Tian et al. [5] designed a food supply chain traceability system based on the Internet of Things and blockchain. By combining with traditional supply chain management methods, the system enhances the safety of the food supply chain. Subsequently, Tian et al. [6] Designed a real-time food traceability system using HACCP and BigchainDB [7]. BigchainDB combines the characteristics of a distributed database and a blockchain to improve the throughput and query efficiency of the traceability system. Toyoda et al. [8] designed a RFID (radio frequency identification)-attached product ownership management system for the post supply chain. The system uses Ethereum smart contracts to manage business information in the supply chain. Chen et al. [9] proposed a blockchain-based supply chain quality management framework, which provides a basis for intelligent quality management in the supply chain. ElMessiry et al. [10] proposed a textile supply chain traceability system based on blockchain. The system can record the entire process of textiles from raw materials to sales, and realize cross-chain information sharing in near real time.

Kamath et al. [11] showed two test cases of Walmart's traceability schemes based on Hyperledger Fabric in China, and discussed the technical challenges faced by blockchain traceability in implementation. Mao et al. [12] proposed a credit evaluation system based on blockchain. The system employs smart contracts to collect evaluation content from the users, and then analyzes the collected evaluation content through LSTM (Long Short-Term Memory). Therefore, the system can enhance food supply chain supervision from the perspective of public opinion evaluation. Lin et al. [13] utilized Ethereum to implement a food supply chain traceability system based on EPC (Electronic Product Code) information services. The system uses off-chain data to alleviate the block data explosion problem, and uses smart contracts to prevent the leakage of sensitive information. Ding et al. [14] proposed a two-layer blockchain traceability framework aimed at solving problems such as government regulation, privacy protection, and performance bottlenecks.

As can be seen from the above literature, the food traceability technology based on blockchain is gradually attracting social attention. However, there is no existing optimal blockchain traceability solution. The transaction throughput, query efficiency, and privacy protection of the traceability system still need to be improved.

3 The Proposed Blockchain-Based Food Traceability Framework

3.1 Overall Framework

The proposed food traceability framework based on blockchain is shown in Fig. 1.

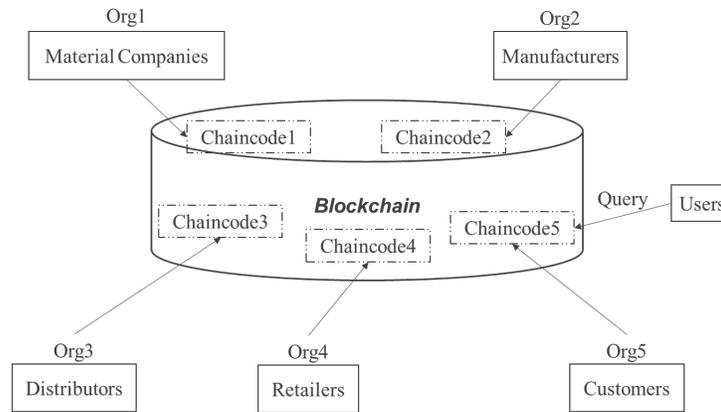


Figure 1: The overall framework of the proposed scheme

In the figure, Org represents the organization. There are five organizations in the figure, which are Material Companies, Manufacturers, Distributors, Retailers and Customers. Each organization has multiple members. These members belong to the same role in the supply chain traceability, so they undertake the same task in the blockchain system. The five organizations deploy five different chaincodes to the blockchain. The chaincode is also called smart contract, that is, a program running on the blockchain. Each chaincode processes the business logic and uploads the traceability information of the corresponding organization. Users can be consumers or auditors. The user can query the complete traceability information of food products from raw materials to sold products through the method in Chaincode5.

There are multiple blockchain nodes in each organization, which are used to store all block data, and also have the functions of deploying chaincodes and sending transactions. Nodes need to generate a certificate before joining the blockchain, that is, to obtain a license to become a member of the food traceability blockchain. Therefore, the proposed scheme belongs to the alliance blockchain, that is, the permissioned blockchain. Compared with the public blockchain, the permissioned blockchain has a higher transaction speed and is more suitable for market demand.

3.2 Layered Architecture

The blockchain layered architecture of the proposed food traceability system is shown in Fig. 2. The data layer encapsulates all the data in the block, and the most basic unit of data is the transaction. The traceability information uploaded by all nodes is stored in the transaction in the form of key-value pairs, and then the transaction is stored in the block in the form of Merkle tree. The data layer also employs techniques such as hash functions, asymmetric encryption algorithms and time stamps to ensure data security. Network layer includes p2p network and the verification mechanism of transactions. The consensus algorithm adopted by the consensus layer is a Practical Byzantine Fault Tolerance (PBFT) algorithm. The PBFT algorithms is efficient, can meet business needs, and does not require the use of digital currency. The contract layer includes five chaincodes written in Golang language. The application layer provides users with interfaces written in Java and User Interface (UI) written in HTML5.

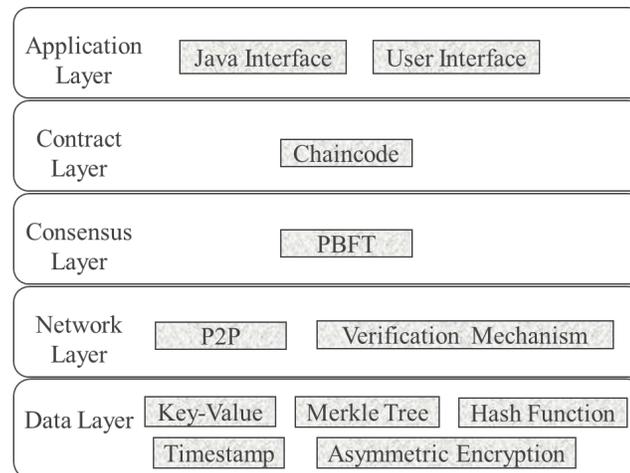


Figure 2: The layered architecture of blockchain

3.3 Chaincodes

Part of the key-value pairs and functions of the five chaincodes are shown in Fig. 3.

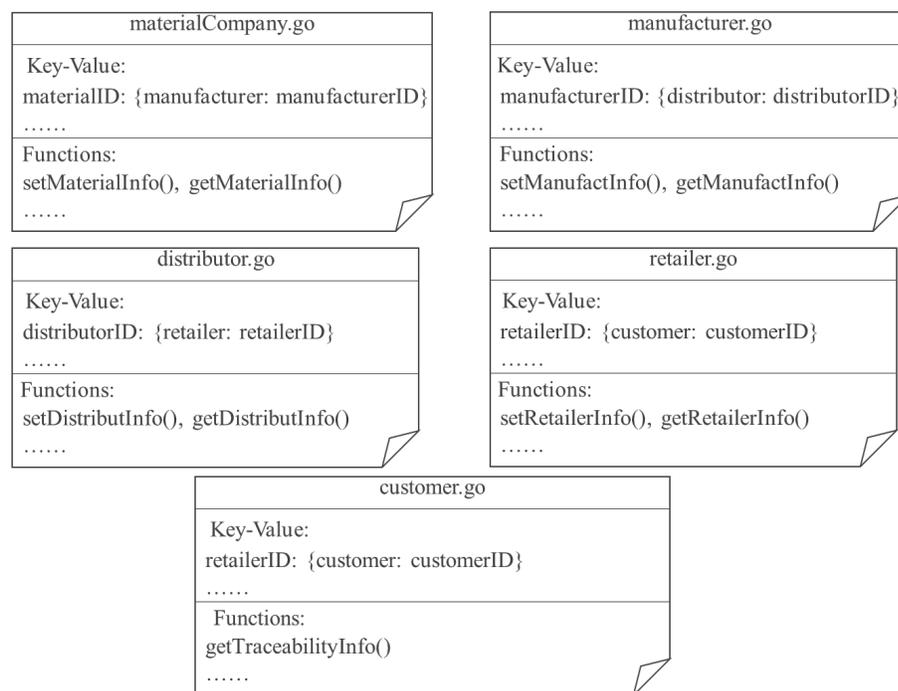


Figure 3: The deployed chaincodes

The material company's chaincode is `materialCompany.go`, responsible for uploading and querying information related to raw materials. `materialID` is the unique identifier of the raw material, and `manufacturerID` is the unique identifier of the manufacturer. Therefore, `materialCompany.go` records the logistics information from the raw material to the manufacturer. Other information of materials can also be recorded by key-value pairs, such as the origin and time of raw materials.

`materialCompany.go` contains some functions such as `setMaterialInfo()`, `getMaterialInfo()` and `Init()`. The `setMaterialInfo()` function is responsible for uploading key-value information to the blockchain. `getMaterialInfo()` is responsible for querying related raw material information. `Init()` is responsible for initializing the chaincode.

Similarly, *manufacturer.go*, *distributor.go* and *retailer.go* are responsible for uploading and querying the corresponding key-value information to the blockchain. Consumers can obtain information such as *retailerID* and *customerID* after purchasing goods. Using *customerID* and *getTraceabilityInfo()* functions, consumers can query the complete supply chain information of the commodity. *getTraceabilityInfo()* can get the *retailerID* according to the *customerID*, and then get the *distributorID* according to the *retailerID*, so that the recursive query will eventually obtain the complete supply chain information of the goods.

In order to protect the consumer's personal sensitive information, the proposed solution determines different query permissions based on the identity of the caller. For example, manufacturers and distributors do not have the right to query consumers' personal information. In addition, users can encrypt sensitive information, and then upload the encrypted information to the blockchain.

4 Experiment and Analysis

The proposed food traceability system is based on Hyperledger Fabric 2.0. The operating system used is ubuntu18.04, the programming language of blockchain and chaincode is Golang, the programming languages of application layer are Java and HTML5.

The hardware equipment used in the experiment is similar to that of ordinary computers used daily. The CPU used is i5-6300HQ, the memory is 8GB, and the hard disk is a 1TB mechanical disk.

4.1 Transactional Throughput

The number of transactions per second of the proposed blockchain traceability system is shown in Fig. 4.

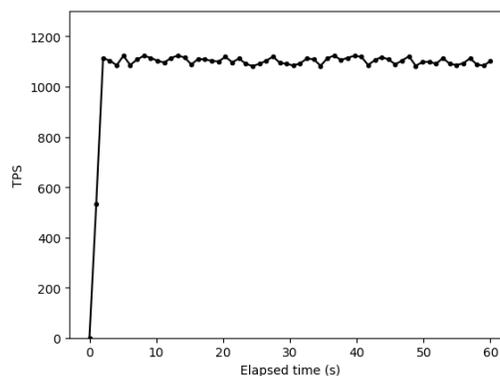


Figure 4: The TPS figure of the proposed scheme

The number of transactions per second, or TPS, is an important indicator of blockchain performance. Apache Jmeter tool is used to perform performance tests on the proposed blockchain system. The abscissa in the figure represents the elapsed time in seconds; the ordinate represents the number of transactions per second. It can be calculated from the figure that the average TPS of the blockchain traceability system is greater than 1100. Under ordinary hardware conditions, the proposed solution can obtain a TPS of about 1100, so it can be competent for supply traceability of ordinary enterprises.

Bitcoin can process about 7 transactions per second, and Ethereum can process about 10-20 transactions per second, which is difficult to meet people's consumption needs. The main reason for their low transaction throughput is the adoption of a PoW-based consensus mechanism. The PoW consensus mechanism requires miners to calculate difficult problems, so it will consume a lot of computing power and time. For example, it takes about 10 minutes for Bitcoin to generate a block. The proposed blockchain traceability framework adopts PBFT as a consensus mechanism, thus improving transaction throughput. PBFT is a consensus algorithm based on message passing and does not require miners to spend time solving problems. Therefore, the consensus delay of the PBFT algorithm is about 2-5 seconds, which can meet the needs of high-frequency transactions.

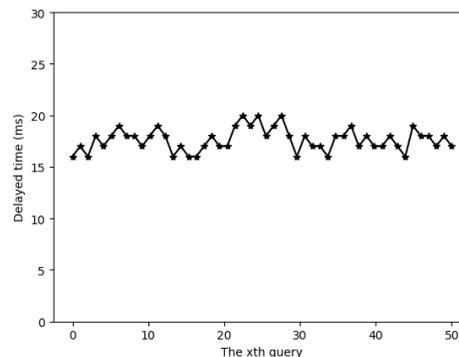
Table 1: The TPS comparison between different blockchains

Blockchain	TPS
Bitcoin	7
Ethereum	20
Double-layer chain	990
Our scheme	1100

The TPS of our solution and other blockchain systems are shown in Tab. 1. It can be seen from Tab. 1 that Bitcoin and Ethereum have lower TPS. Because they are both public blockchains and the consensus mechanism adopted is not efficient enough. The double-layer chain is a permissioned product traceability blockchain proposed by Ding et al. [14]. The TPS of this blockchain is close to 1000. As can be seen from the table, the TPS of our scheme is better than the other three blockchain systems.

4.2 Query Efficiency

The delay for the user to query the traceability information is shown in Fig. 5.

**Figure 5:** The query delay

The abscissa indicates the xth query of traceability information, and the ordinate indicates the corresponding delay time. It can be seen from the figure that the average delay of the query of the proposed traceability system is about 17 milliseconds, and there is no network congestion or long delay. Therefore, users can get a good query experience.

Generally, querying traceability information is to read data from the blockchain ledger. However, the proposed traceability framework queries information from “World State”. The World State is determined by the blockchain ledger, which is essentially a database that stores key-value pairs. Using World State, the querier can directly obtain the current value without traversing the entire blockchain ledger, thus improving query efficiency.

4.3 Privacy Protection Analysis

The proposed traceability scheme uses the chaincode to control the query permission of the nodes, so it can protect the consumer privacy effectively. In addition, consumers and other roles can encrypt sensitive information and upload it to the blockchain to prevent the leakage of private information.

5 Conclusion and Future Work

The paper proposes a food traceability framework based on a permissioned blockchain. The framework is based on the Hyperledger Fabric and divides the roles in the supply chain into five organizations. The five organizations deploy five different chaincodes to the blockchain. These chaincodes can handle the business logic of each organizations. The chaincode permission control and encryption mechanism enhance the privacy protection of the traceability framework. The transaction

throughput experiment shows that the traceability framework achieves a higher number of transactions per second. The experiment of query efficiency shows that the query delay of the proposed traceability framework is low and stable.

Certainly, the proposed blockchain traceability framework still can be improved. For example, although the PBFT consensus algorithm has high consensus efficiency, it can only tolerate 1/3 malicious nodes, which is slightly lower than 1/2 of the PoW (proof of work) algorithm. In addition, the storage space of blockchain nodes is limited, therefore it is a difficult problem to allocate the on-chain data and off-chain data. Finally, the zero-knowledge proof algorithm can be used to further improve the privacy protection of the proposed traceability framework.

Funding Statement: This work is supported by the National Natural Science Foundation of China under Grant U1836110, U1836208.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

- [1] S. Nakamoto, *A Peer-to-Peer Electronic Cash System*. 2008. [Online]. Available: <https://bitcoin.org/bitcoin>.
- [2] J. H. Hoepman, "Distributed double spending prevention," in *International Workshop on Security Protocols*, pp. 152–165, 2007.
- [3] L. Lamport, R. Shostak and M. Pease, "The Byzantine generals problem," in *Concurrency: the Works of Leslie Lamport*, pp. 203–226, 2019.
- [4] V. Buterin, "A next-generation smart contract and decentralized application platform," *White Paper*, pp. 1–37, 2014.
- [5] F. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," in *2016 13th International Conference on Service Systems and Service Management*, pp. 1–6, 2016.
- [6] F. Tian, "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things," in *2017 International Conference on Service Systems and Service Management*, pp. 1–6, 2017.
- [7] T. McConaghy, R. Marques, A. Müller, D. D. Jonghe, T. McConaghy *et al.*, "Bigchaindb: a scalable blockchain database," *White Paper*, 2016.
- [8] K. Toyoda, P. T. Mathiopoulos, I. Sasase and T. Ohtsuki, "A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain," *IEEE Access*, vol. 5, pp. 17465–17477, 2017.
- [9] S. Chen, R. Shi, Z. Ren, J. Yan, Y. Shi *et al.*, "A blockchain-based supply chain quality management framework," in *2017 IEEE 14th International Conference on e-Business Engineering*, pp. 172–176, 2017.
- [10] M. ElMessiry and A. ElMessiry, "Blockchain framework for textile supply chain management," in *International Conference on Blockchain*, pp. 213–227, 2018.
- [11] R. Kamath, "Food traceability on blockchain: Walmart's pork and mango pilots with IBM," *The Journal of the British Blockchain Association*, vol. 1, no. 1, pp. 47–53, 2018.
- [12] D. Mao, F. Wang, Z. Hao and H. Li, "Credit evaluation system based on blockchain for multiple stakeholders in the food supply chain," *International Journal of Environmental Research and Public Health*, vol. 15, no. 8, pp. 1–21, 2018.
- [13] Q. Lin, H. Wang, X. Pei and J. Wang, "Food safety traceability system based on blockchain and EPCIS," *IEEE Access*, vol. 7, pp. 20698–20707, 2019.
- [14] Q. Ding, S. Gao, J. Zhu and C. Yuan, "Permissioned blockchain-based double-layer framework for product traceability system," *IEEE Access*, vol. 8, pp. 6209–6225, 2019.