Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 199 (2022) 629–636

Procedia Computer Science

www.elsevier.com/locate/procedia

The 8th International Conference on Information Technology and Quantitative Management (ITQM 2020 & 2021)

A Food anti-counterfeiting traceability system based on Blockchain and Internet of Things

Yi Lu[a], Peng Li[a,c,*], He Xu[a]

[a]School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China
[c]Institute of Network Security and Trusted Computing, Nanjing 210023, China

Abstract

In this paper, a food anti-counterfeiting traceability system based on blockchain and the Internet of Things is proposed in response to the problems of data centre-based storage, easy data tampering and data silos in traditional food anti-counterfeiting traceability technology. The system makes use of the decentralized storage and untamperable characteristics of blockchain technology to store traceability data of food in the process of food production, sale and transportation, so as to ensure the uniqueness of food. At the same time, through the Internet of things technology to ensure the authenticity and reliability of the source data of the blockchain. The experimental results show that the system has higher security, lower transaction delay and lower communication cost.

Keywords: Blockchain; The Internet of things; anti-counterfeiting traceability system

1. Introduction

Food safety is a global issue, and in addition to legislative safeguards, society is in urgent need of technologies and tools that can safeguard food safety. At the same time, traditional food anti-counterfeit traceability technology faces problems such as data centre-based storage, easy data tampering and data silos.

In recent years, blockchain technology[1], which has come into the public eye as a result of Bitcoin[2], has developed very rapidly. Blockchain-based traceability systems provide a solution to the shortcomings of traditional traceability systems due to their decentralised and tamper-proof characteristics. Feng Tian[3] proposed a traceability system for agricultural products supply chain based on blockchain and RFID. Through the collection, transmission and sharing of real data of agricultural products production, processing, warehousing, distribution and sales, the traceability of information of the whole agricultural products supply chain was realized

* Corresponding author.
E-mail address: lipeng@njupt.edu.cn

10.1016/j.procs.2022.01.077

and food safety was effectively guaranteed. Chen Junhua[4] proposed an electronic product traceability system based on block chain and ORS(OID Resolution System), and designed an on-chain and off-chain joint management model. Digital summaries of key traceability brief information and detailed data of electronic products are recorded on the chain, and large capacity and detailed traceability data are managed by ORS below the chain. Wang Keke[5] proposed an efficient traceability system for the quality and safety of agricultural products based on the alliance block chain. Firstly, IPFS is used to hash[6] the agricultural product data to reduce the amount of single transaction data in the block. Secondly, the alliance blockchain model is established to verify the data. Wharton chain builds an anti-counterfeiting traceability system that combines RFID and blockchain. In Wharton chain, product traceability information, such as clothing fabric, origin and other information, will be recorded in the RFID tag of the product after the completion of production. At the same time, Wharton chain will store the verification information of the above information in the blockchain. To verify the authenticity of information stored in RFID.

In summary, the application of blockchain in the traceability system has been discussed on the theoretical basis[7] and the actual project research and development. However, most of the existing blockchain-based anti-counterfeiting traceability systems focus on resolving the imtamperability of data and the decentralization of the system, which cannot guarantee the authenticity and reliability of the blockchain-based source data. At the same time, most anti-counterfeiting traceability systems adopt private chains, which have problems such as high transaction delay, low system throughput and large resource consumption. To solve the above problems, this paper combines the blockchain technology[8] with the Internet of Things technology. Food traceability data is stored through the alliance blockchain to ensure the decentralized storage[9] of traceability data and the imtamperability of data. At the same time, the Internet of Things technology is used to ensure the authenticity and reliability of the source data of the blockchain, so as to realize the safe traceability of food.

2. Preliminaries

2.1. Blockchain Technology

According to the consensus algorithm[10] used, blockchain can be divided into public blockchain, alliance blockchain and private blockchain. Hyperledger Fabric[11] used in this paper is an implementation method of alliance blockchain. Compared to PoW and PoS used by the public blockchain, the consensus algorithm of PBFT[12] used by Hyperledger Fabric does not produce bifurcating and has high consensus efficiency. Meanwhile, based on the business requirements of food security traceability, Hyperledger Fabric provides a high degree of confidentiality, elasticity[13], flexibility and expansibility[14]. It supports pluggable implementations of different components and accommodates the complexity that exists in an economic system.

2.2. Internet of Things technologies

Internet of things technology[15] plays a crucial role in food security traceability, and it can ensure the authenticity and reliability of the source data of blockchain. The Internet of Things connects any item to the Internet through intelligent sensors[16], RFID(Radio Frequency Identification Devices)[17], GPS(Global Positioning System)[18] and other information sensing devices, forming an Internet that connects people to things and things to things, and realizing the information and intelligent management.

3. System design

The food security traceability system based on blockchain and Internet of Things proposed in this paper is mainly aimed at food manufacturers, transporters and consumers. In terms of functions, the food security traceability system can be divided into five parts: the Internet of Things part, the blockchain part, the front end part, the back end part and the applet part. This section first introduces the design scheme of the system, then introduces the overall architecture of the system, and finally introduces the detailed design of the Internet of Things part, blockchain part, front and back end part and applet part respectively.

3.1. Design scheme

As shown in Fig. 1, information such as temperature, humidity, weight and geographical location of food is obtained through IoT devices in the production, processing, storage and transportation of food. The data collected by the sensors is uploaded to the AliCloud IoT platform through the MQTT protocol. Producers and transporters obtain IoT information of food products from AliCloud IoT platform through AMQP protocol. The production and transportation data of food products are permanently stored on the blockchain through chain codes. Consumers purchase food through the online mall, and after receiving the food, they scan the QR code to trace the food through the applet.

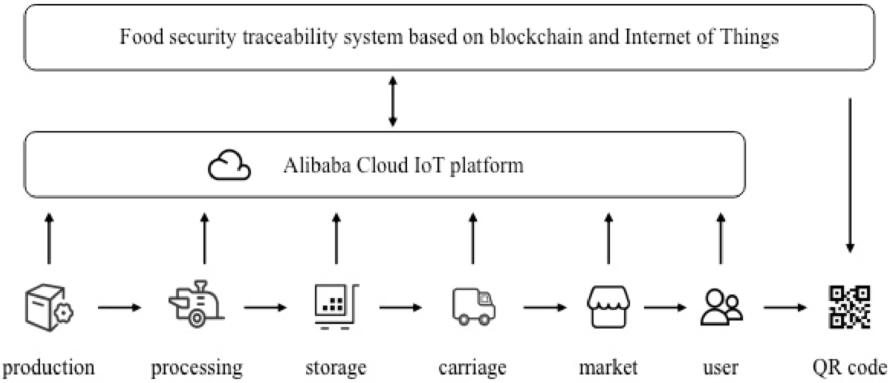
Food security traceability system based on blockchain and Internet of Things
Alibaba Cloud IoT platform
production
processing
storage
carriage
market
user
QR code

Fig. 1. Design scheme

3.2. Overall architecture

The overall architecture of this system is shown in Fig. 2, which is mainly divided into IoT layer, network layer, data layer, platform layer, application layer and external interface layer.

The IoT layer is used to collect data such as temperature and humidity, weight and geographical location of food. The collected data is stored to the AliCloud IoT platform. The main components in this layer include temperature and humidity sensors, pressure sensors, GPS, tags and QR codes.

The data layer is used to store both traceable and non-traceable data. Traceability data is stored via a blockchain. Each record in the blockchain contains a unique timestamp as well as a cryptographic signature. Each entity in the system requires a digital signature from the entity to operate on the traceability data. The digital signature guarantees the non-repudiation of the data in the event of a food issue. Non-traceable data includes IoT data, user data, shop data, order data, etc. Non-traceable data is stored through a relational database. Among them, IoT data is stored on the AliCloud IoT platform, and user avatars and pictures of food products are stored on AliCloud OSS.

The platform layer is used to manage the entire food anti-counterfeiting and traceability platform, including user management module, role management module, permission management module, front-end management module and data analysis module. Among them, the user management module aims to manage manufacturers, transporters and consumers. The role management module is used to assign different roles to the aforementioned users. The rights management module assigns different rights to the different roles, i.e. the functions that the user can use and the pages that they can access. The Frontend Management module manages the frontend online shop. The data analysis module collects operational data of the platform in real time and visualises and analyses the data through Echarts.

The application layer includes IoT applications, blockchain applications, frontend applications, backend applications and applet applications. The IoT application obtains data such as temperature and humidity, weight and geographical location of food through IoT devices. It also stores the IoT data to AliCloud IoT platform. The blockchain application stores the traceability data of the data layer through the chain code. The data data is stored on each node of the blockchain system. The data is also guaranteed to be tamper-evident through consensus algorithms. The front-end application is the online shopping mall, through which consumers purchase food products. The backend application is for producers and transporters, with producer applications including food management and order management, and transporter applications including courier management. The applet application obtains food traceability data by scanning QR codes.

The external interface layer includes IOT application interface, blockchain application interface, front-end application interface, back-end application interface and applet interface. The system adopts the development method of separating the front and back ends, and the front and back ends communicate data through the interfaces. Users can access the services through the access interface.

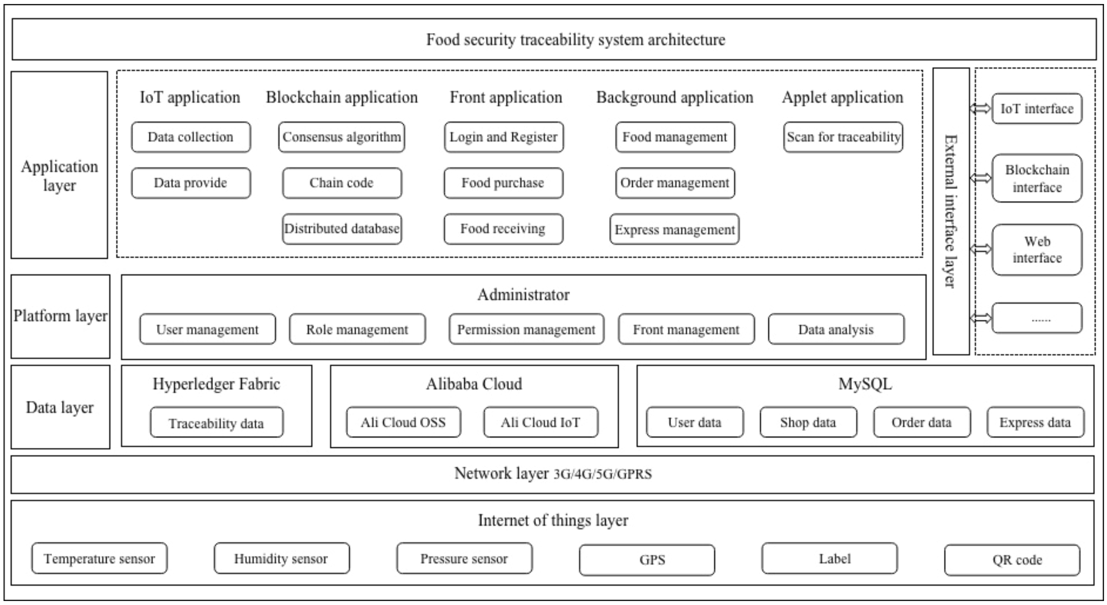

Fig. 2. Overall architecture

3.3. Detailed design

1) Internet of Things

As shown in Fig. 3, the Stm32 development board integrates temperature sensors, humidity sensors, pressure sensors and GPS sensors. After collecting data, the collected data is uploaded to the AliCloud IoT platform via the MQTT protocol. The user application obtains the IoT data from the AliCloud IoT platform via the AMQP protocol. The data provides data support for blockchain anti-counterfeit traceability.

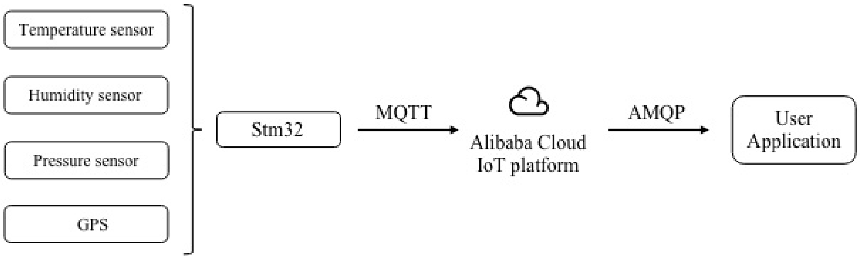

Fig. 3. IoT component architecture

2) Blockchain

As shown in Fig. 4, the blockchain architecture includes the front-end, back-end and Fabric three-layer architecture. The front-end architecture is mainly the back-end management page of the producer, the back-end management page of the transporter, the front page of the online mall and the traceability applet page. Hyperledger mainly consists of three nodes: producer, transporter and consumer, and smart contracts. Each node has a CA, and the smart contract is packaged into a chain code and deployed on top of each channel, and the nodes call the methods in the smart contract through the chain code.

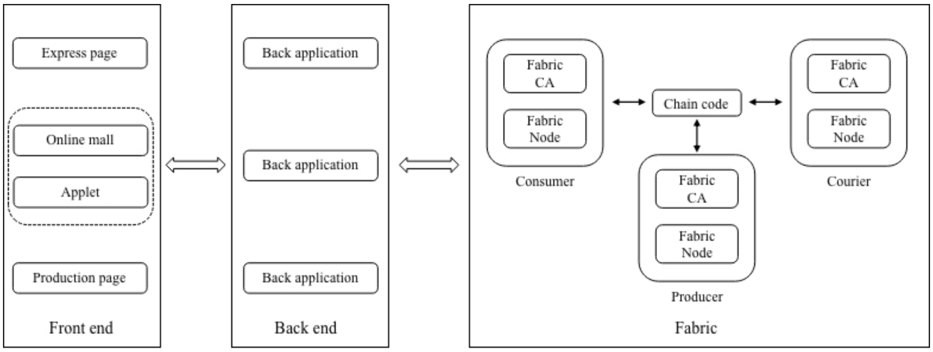

Fig. 4. Blockchain component architecture

3) Front and backend

The front and backend are developed using a separate front and backend development approach. As shown in Fig. 5, the front-end uses the Vue framework and uses the Element UI framework to build pages quickly. The back-end uses SpringBoot and MyBatis Plus, and the database uses MySQL and AliCloud's Object Storage Service OSS.

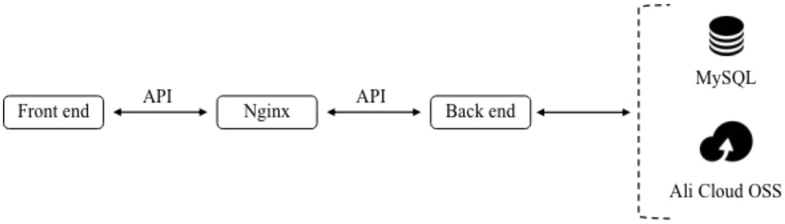

Fig. 5. Front end and back end component architecture

4) Applet

Users use the applet to scan the QR code of the food to query the traceability information of the food. The food ID in the QR code can be obtained through backend decoding, and the applet initiates a query request to the server via the ID. The server queries the traceability data in the distributed ledger through the blockchain node and returns the traceability result to the applet. The applet renders the traceability results dynamically to the user.

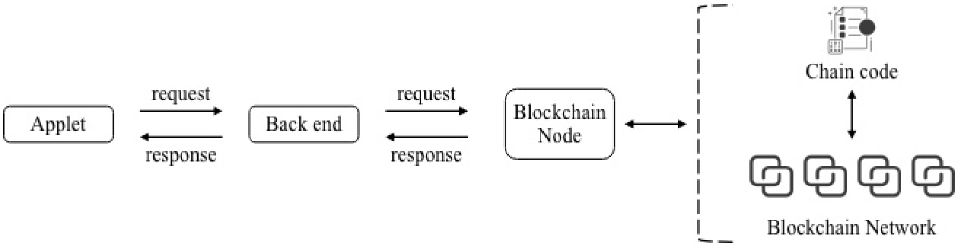

Fig. 6. Applet component architecture

4. Experiment

In this section, experimental analysis is made on the food security traceability system implemented in this paper from the three aspects of fault tolerance, transaction delay and communication cost.

4.1. Experimental steps

The blockchain system of this system is built based on Hyperledger Fabric, and the chain code is written by JavaScript. The Internet of Things system adopts STM32F103C8T6 integrated temperature and humidity sensor, pressure sensor and GPS.

The experimental hardware environment was a MacBook Pro with an Intel Core i5 (1.4GHz) CPU, 16GB of RAM and MacOS Mojave operating system. The experiment uses Golang to implement the PBFT algorithm of Hyperledger Fabric. To test the performance of PBFT, this article uses Golang's reflection mechanism to simulate RPC remote procedure calls. PBFT nodes are simulated by simulated RPC. Blockchain nodes can be divided into master nodes, slave nodes and client nodes. Nodes can communicate with each other through broadcast communication or peer-to-peer communication. The simulated RPC can obtain the communication times between nodes, the size of communication data, the running time of the consensus algorithm and the running results. Based on these data, this paper analyzes the fault tolerance, transaction latency and communication cost of PBFT.

4.2. Experimental Analysis

1) fault tolerance analysis

Fault tolerance is the main manifestation of blockchain storage security, which ensures that the blockchain system can reach consensus on messages even in the presence of Byzantine nodes. When the number of Byzantine nodes is 1, Fabric can reach consensus in a system with a number of nodes of 4. When the number of Byzantine nodes is f, Fabric can reach consensus in a system with a number of nodes of $3f + 1$.

2) Trading delay

Transaction delay is one of the important indicators of system performance analysis. The main functions of the system are food traceability data on the chain and on the chain data query. Traceability data on the chain is the process of reaching consensus among the nodes of the blockchain. This paper carried out delay tests on different numbers of nodes, and the test results are shown in Fig. 7. As the number of nodes increases, the impact of the number of nodes on the latency increases. When the number of nodes reaches 100, the transaction latency reaches about 338-483 milliseconds.

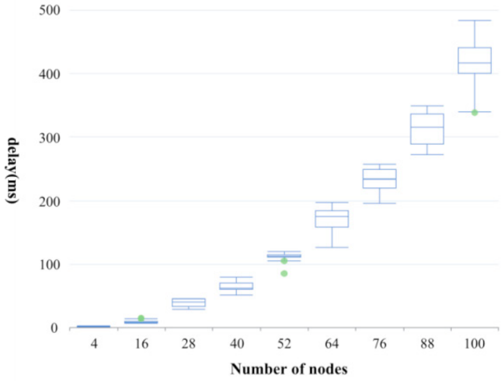

Fig. 7. Trading delay

3) Cost of communication

Fig. 8 describes the communication costs required by the first round of consensus in the case of different number of nodes of PBFT, and Fig. 9 describes the communication costs required by different number of consensus rounds of PBFT when the number of nodes is fixed at 4. As can be seen from Fig. 8, the communication cost of PBFT algorithm keeps increasing with the increase of the number of nodes. When the number of nodes is 100, the communication cost of PBFT is 483.91KB. As can be seen from Fig. 9, when the number of consensus rounds is 100, the communication cost of PBFT is 81.47KB.

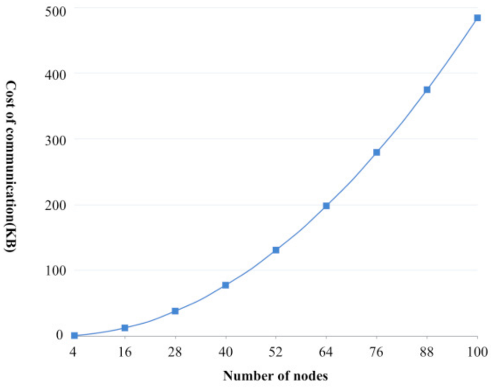

Fig. 8. Cost of communication(a)

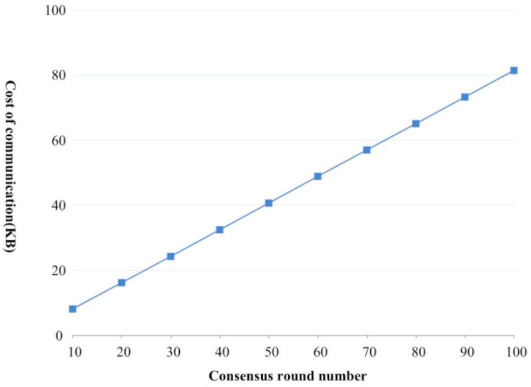

Fig. 9. Cost of communication(b)

5. conclusion

Aiming at the existing problems of traditional food security traceability technology, this paper proposes an anti-counterfeiting traceability system based on blockchain and Internet of Things. The system collects food temperature and humidity, weight and geographical location information through Internet of Things devices, and stores food traceability data in the process of production, transportation and sales through blockchain. Experimental results show that the system has higher security, lower transaction delay and lower communication cost. The future work of this paper is to improve the PBFT algorithm, further reduce the transaction delay and network communication costs, and improve the throughput and performance of the system to meet the needs of food security traceability under high concurrency.

Acknowledgements

The subject is sponsored by the National Key R&D Program of China (No. 2018YFB1003201), the National Natural Science Foundation of P. R. China (No. 61872196, No. 61872194, and No. 61902196), Scientific and Technological Support Project of Jiangsu Province (No. BE2019740, No. BK20200753, and No. 20KJB520001), Major Natural Science Research Projects in Colleges and Universities of Jiangsu Province (No. 18KJA520008), Six Talent Peaks Project of Jiangsu Province (RJFW-111), Postgraduate Research and Practice Innovation Program of Jiangsu Province (No. SJKY19_0761, No. SJKY19_0759, No. KYCX20_0759).

References

[1] Shao QF, Jin CQ, Zhang Z, et al, “Blockchain technology:architecture and progress”, Journal of Computer Science, 2018, 41(5): 969-988.

[2] Nakamoto S, “Bitcoin: a peer-to-peer electronic cash system”, http://bitcoins.info/bitcoin.pdf, March 5, 2021.

[3] Feng T, “An agri-food supply chain traceability system for China based on RFID & blockchain technology”, 13th International Conerence on Service Systems and Service Management, IEEE, 2016: 1-6.

[4] Chen JH, Zhang X, Shangguan PF, “Electronic Product Traceability System Based on Blockchain and ORS”, Computer Engineering and Design, 2021, 42(02): 349-355.

[5] Wang KK, Chen ZD, Xu J, “Efficient traceability system for quality and safety of agricultural products based on alliance block chain”, Application of Computer, 2019, 39(08): 2438-2443.

[6] Carter J L, Wegman M N, “Universal classes of hash functions”, Journal of computer and system sciences, 1979, 18(2): 143-154.

[7] Shao QF, Zhang Z, Zhu YC, et al, “Review of Enterprise Blockchain Technology”, Journal of Software, 2019, 30(09): 2571-2592.

[8] Yuan Y, Wang FY, “Blockchain Technology Development Status and Prospect”, Acta Automatica Sinica, 2016, 42(04): 481-494.

[9] Wang QS, Wang HZ, Zheng B, “An efficient distributed storage strategy for blockchain”, 2019 ACM Turing Celebration Conference, ACM, 2019: 1-5.

[10] Yuan Y, Ni XC, Zeng S, et al, “Progress and Prospects of Blockchain Consensus Algorithms”, Acta Automatica Sinica, 2018, 44(11): 2011-2022.

[11] Androulaki E, Barger A, Bortnikov V, et al, “Hyperledger fabric: a distributed operating system for permissioned blockchains”, Proceedings of the Thirteenth Eurosys Conference, ACM, 2018:30.

[12] Castro M, Liskov B, “Practical Byzantine fault tolerance”, OSDI. 1999, 99(1999): 173-186.

[13] Pan C, Liu ZQ, Liu Z et al, “Research on Blockchain Scalability: Problems and Methods”, Computer Research and Development, 2018, 55(10): 2099-2110.

[14] Xie JF, Yu FR, Huang T, et al, “A Survey on the Scalability of Blockchain Systems”, IEEE Network, 2019, 33(5):166-173.

[15] Gubbi J, Buyya R, Marusic S, et al, “Internet of Things (IoT): A vision, architectural elements, and future directions”, Future generation computer systems, 2013, 29(7): 1645-1660.

[16] Akyildiz I F, Su W, Sankarasubramaniam Y, et al, “Wireless sensor networks: a survey”, Computer networks, 2002, 38(4): 393-422.

[17] Bouet M, Santos A, ″RFID tags: Positioning principles and localization techniques″, 2008 1st IFIP Wireless Days, Dubai, 2008: 1-5.

[18] Bulusu N, Heidemann J, Estrin D, “GPS-less low-cost outdoor localization for very small devices”, IEEE personal communications, 2000, 7(5): 28-34.