

# *Design and Implementation of Blockchain-based Anti-Counterfeit Traceability System for Beef Cattle Products*

Pingping Xiang\*, Xinrong Liu, Yipeng Han

*College of Management Science, Chengdu University of Technology, Chengdu, Sichuan, China*

*\*Corresponding author*

**Keywords:** RSA algorithm, traceability ID, blockchain, anti-counterfeiting, traceability

**Abstract:** Aiming at beef cattle product quality safety, the traditional anti-counterfeit traceability methods have serious data centering. To guarantee data security and reliability, this paper adopts blockchain technology with traceability characteristics, takes beef cattle products as the research object, constructs a supply chain traceability model of beef cattle products based on blockchain technology, and builds an anti-counterfeiting traceability system based on Hyperledger Fabric platform. The organizations at the management end of the same supply chain use the snowflake algorithm to generate corresponding IDs, which are interrelated with each other and then combine the traceability ID, blockchain, and QR code to realize anti-counterfeiting traceability, finally complete data verification between the traceability ID and local information and return relevant information. At the same time, to guarantee the security of the QR code, the improved RSA algorithm is used to generate the key pair, the public key is used for encryption, and the private key is used to generate the encrypted QR code for the traceability ID, and the consumer can obtain the traceability ID by scanning the code and decrypting it. In order to verify the effectiveness of the RSA algorithm and the performance of the anti-counterfeiting traceability system, the system is tested and applied in this paper, and the test results show that the anti-counterfeiting function of the traceability system is realized, and the system performs well without the phenomenon of chain code collapse. Meanwhile, it is found that the efficiency of the consensus algorithm of various organizations needs to be improved, to ensure anti-counterfeiting traceability.

## 1. Introduction

The issue of food safety affects the health of the nation and has always been a livelihood issue of great concern to governments [1]. Taking beef cattle products as an example, the current online and offline trading fields are facing the problem of anti-counterfeit traceability, and the traditional anti-counterfeit traceability stores data uniformly in the central database, but the data centering is serious and cannot defend against the updated information tampering technology in modern society, and the encryption system is extremely easy to be breached when it is not strong. The supply chain is a typical example in the physical field. Due to the numerous and mixed ends of the supply chain, its traceability is difficult and data security is low, and it is difficult to trace products to specific links when quality problems occur. However, blockchain can effectively solve this problem. Originally derived from Bitcoin, blockchain has the characteristics of high efficiency, low cost, and distribution, as well as

stability, traceability, and immutability of decentralized data [2]. Through its traceability, the data stored on the blockchain can be traced to achieve the purpose of anti-counterfeit identification.

This paper takes beef cattle products as the research object, constructs a blockchain-based supply chain traceability model for beef cattle products, and builds an anti-counterfeit traceability system based on the Hyperledger Fabric platform to provide reliable support for improving the transparency and security of the traceability information of beef cattle products and guaranteeing the product quality and safety of beef cattle products.

Currently, the research on beef cattle products at home and abroad mainly focuses on two aspects: anti-counterfeit traceability of QR codes and blockchain traceability system design. On the one hand, for the research of QR code anti-counterfeiting traceability, Wannan Qiao proposed the idea of combining QR code information encryption with image geometry processing. Zhanhong Zhang et al. proposed the combination of microservice architecture, QR code technology and AES symmetric encryption algorithm to realize a QR code anti-counterfeiting traceability system [3]. Xi Huang combined the national secret algorithm with NFC to complete the design and implementation of the anti-counterfeiting system [4]. Zheng et al. constructed an anti-counterfeiting system with statistical analysis of the sequence of feature differences corresponding to a single key region [5]. Lu et al. designed a food anti-counterfeiting traceability system based on blockchain and IoT [6]. Qiu et al. proposed to build an edge computing ownership-based traceable anti-counterfeiting system [7]. Xie et al. conceived a two-level quick response code-based anti-counterfeiting architecture for traceability system, which transformed the problem of product anti-counterfeiting detection into the problem of replication detection of 2LQR code tags [8].

On the other hand, for blockchain traceability system design, Turki et al. proposed NFT-IoT pharmaceutical chain, an IoT drug traceability system based on blockchain and irreplaceable tokens [9]. Sezer et al. proposed TPPSUPPLY: a traceable and privacy-preserving blockchain system architecture for the supply chain [10]. Uddin proposed a blockchain-enabled Medledger system [11]. Mothukuri et al. proposed the BlockHDFS approach, which is to build trusted data security and traceability in HDFS [12]. Alamsyah et al. designed a model to convert supply chain business processes in the coffee industry into traceable blockchain workflows [13]. Li et al. introduced blockchain technology after, storing data traceability information in blockchain can effectively ensure the trustworthiness and integrity of traceable information [14]. Chen et al. constructed a blockchain-based anti-counterfeit traceable NBA digital transaction card management system [15]. Yang et al. designed a blockchain technology-based product information storage and query traceability system for agricultural supply chains [16]. A new framework, Vacledger, was proposed that can be used for supply chain traceability and counterfeit detection of covid - 19 vaccines using blockchain network [17].

## 2. Encryption and Decryption Structure

In the whole supply chain circulation of beef cattle products, task numbers are generated according to different states of circulation, and the IDs added in the process of beef cattle breeding are taken as global IDs, the IDs added in each process link are taken as circulation IDs, and the IDs added after the consumer products are signed and received are taken as traceability IDs, and the organizations in the same chain are associated with each other to constitute distributed services and strengthen the network resistance to attacks. In the process of encryption and decryption of traceability ID, the improved RSA algorithm is used to generate key pairs, the public key and private key, and then the public key is stored in the local database for encrypting the traceability ID and the private key is stored in the blockchain, and finally, the ciphertext generated by encryption is placed in the QR code, and consumers obtain the traceability ID by scanning the QR code, and the blockchain returns to the

private key and decrypts it locally.

## 2.1. Improved RSA Algorithm Key Security Performance Optimization

As the most widely researched and applied encryption method, the traditional RSA algorithm relies on huge computation and the separation of public and private keys to ensure security, but with the development of technology, hackers can obtain the components of modulo  $n$  and derive, public and private keys through attacks, making its possibility of being cracked elevated. To ensure security, this paper will use the improved three-prime factor RSA algorithm to increase the factor and increase the decryption complexity while reducing the computation of the key generation process. The encryption core of RSA algorithm is modulo  $n$ , and the hidden key  $N$  is used to replace modulo  $n$  when generating the key, which can reduce the attack and ensure security.

The steps to improve the RSA algorithm are as follows (Figure 1) [18]:

- (1) Randomly generate three prime factors with small differences in size  $p, q, r$ ;
- (2) Calculate modulus  $n = pqr$ , calculate the value of the Euler function

$$\varphi(n) = (p - 1)(q - 1)(r - 1) \quad (1)$$

- (3) Generating the alternative modulus  $N$  by the maximum convention satisfies

$$GCD(N, n) = 1, \quad (2)$$

And

$$n - \max < N < n, \quad (3)$$

where  $\max$  is the maximum value of  $p, q, r$ ;

- (4) Choose the value of  $e$  that satisfies

$$GCD(e, \varphi(n)) = 1, \text{ and } 1 < e < \varphi(n) \quad (4)$$

- (5) Solve the operation by Fermat's theorem and use the modulo

$$ed \bmod \varphi(n) = 1. \quad (5)$$

operation of  $e$  and  $\varphi(n)$  to find the private key  $d$ . From this, we can obtain the public key  $(e, N)$  and the private key  $(d, N)$ , where  $\bmod$  is the modulo operation function;

- (6) Suppose  $M$  is plaintext,  $C$  is ciphertext, the encryption process of plaintext  $M$  is

$$C = M^e \bmod N. \quad (6)$$

the ciphertext  $C$  decryption process is

$$M = C^d \bmod N. \quad (7)$$

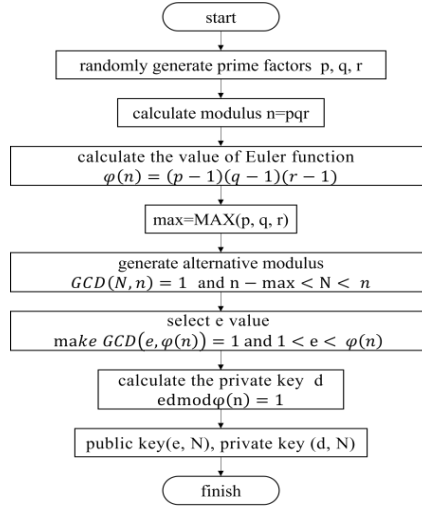


Figure 1: Three prime factor RSA algorithm replaces key generation

## 2.1. Montgomery Powering Ladder to Optimize the Operation Efficiency

Montgomery Powering Ladder is an optimization algorithm for fast calculation of power module operations. It is mainly used in cryptography such as key exchange and digital signatures. It supports parallel computing and further improves computational efficiency by using multi-core CPU to achieve fast and efficient large-number operations. The power module operation is the core of the RSA algorithm. By optimizing the computational efficiency, the speed of encryption and decryption can be improved to ensure the security and stability of the system. The specific steps are as follows:

(1) First use the Montgomery power module method by shifting the fast power module,  $b$  can be expressed as a binary  $b_{r-1}, b_{r-2}, \dots, b_1, b_0$ , namely

$$b = b_0 + 2b_1 + \dots + 2^{r-1}b_{r-1}. \quad (8)$$

(2) Then the modular exponentiation operation is converted into modular multiplication to reduce the operation and improve the computational efficiency, as follows:

$$M = \left[ a^{b_0} (a^2)^{b_1} \dots (a^{2^{r-1}})^{b_{r-1}} \right] \text{ mod } c, \quad (9)$$

let

$$a = A_0, \quad (10)$$

$$A_i = (A_{i-1})^2 \text{ mod } c, i = 1, 2, \dots, r-1, \quad (11)$$

Get

$$M = A_0^{b_0} A_1^{b_1} \dots A_{r-1}^{b_{r-1}} \text{ mod } c \quad (12)$$

## 3. System Architecture

The blockchain architecture is an open-source basic development based on the smart contract program of the Ethereum platform. It is a blockchain data structure. Each block will have a permanent timestamp to represent identity and verification. It can effectively solve the problem that anti-counterfeiting information is easy to tamper with, correct the defects of traditional single-agency authentication, and the upload of data will only update the data without deleting the data. The blockchain also has technical advantages such as decentralization, tamper-proof, safe and reliable,

and distributed storage. According to different permissions, the blockchain can be divided into three categories: public chain, alliance chain and private chain.

Considering that the supply chain process of beef cattle products needs multi-party cooperation, the blockchain adopts a relatively stable alliance chain structure with central nodes and uses the Hyperledger Fabric framework. Based on this technical architecture of beef cattle product anti-counterfeiting traceability system, this paper will start from the participation end and the management end. According to the circulation link of the whole beef cattle product supply chain, the participation end can be divided into breeding enterprises, slaughtering and processing enterprises, logistics distribution enterprises, sales enterprises, consumers and other subjects. The management side provides the role account for each participant, and the participant logs the account, adds the information that they need to upload to the chain in different interfaces and stores the backup locally. For the determination of their own traceability information, the following principles need to be followed:

- (1) Clear all the enterprise information involved in the supply chain circulation of beef cattle products;
- (2) To clarify the information affecting the quality of beef cattle products;
- (3) Clear information is accurate, reliable and easy to collect;
- (4) Clear information is consistent with the requirements of national laws and regulations.

Based on the above principles, from the perspective of supply chain anti-counterfeiting traceability, the traceability information needed to ensure the quality of beef cattle products includes the information of four supply chain links of beef cattle breeding, slaughtering, logistics distribution and segmentation sales, as well as the information of related enterprises (farms, slaughterhouses, logistics distribution enterprises, sales enterprises) involved in the links. The specific information is shown in Figure 2.

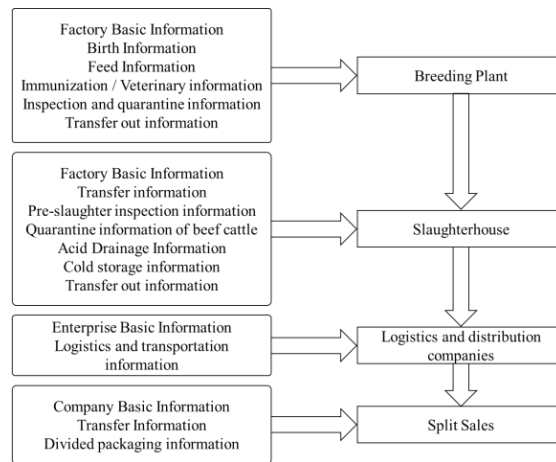


Figure 2: Beef cattle product supply chain traceability information framework

### 3.1. Blockchain Network System Design

The blockchain network system is composed of basic layer, core layer and application layer. The basic layer is the data layer, which is composed of data infrastructure. The Hyperledger Fabric network architecture is applied, which is flexible and less dependent on hardware, and realizes P2P. The core layer is the execution layer, which may include virtual environment, blocks, transactions and smart contracts. It is necessary to perform value transfer, smart contracts and block generation, and organize and sort through orderer to realize chain code operation and information upload, improve block chain efficiency and scalability; the application layer provides an interface on the basis of data upload, so as to call the blockchain network and facilitate the query of data details at any time.

It can realize the rich query of chain code through CouchDB [19]. The specific implementation process is shown in Figure 3:

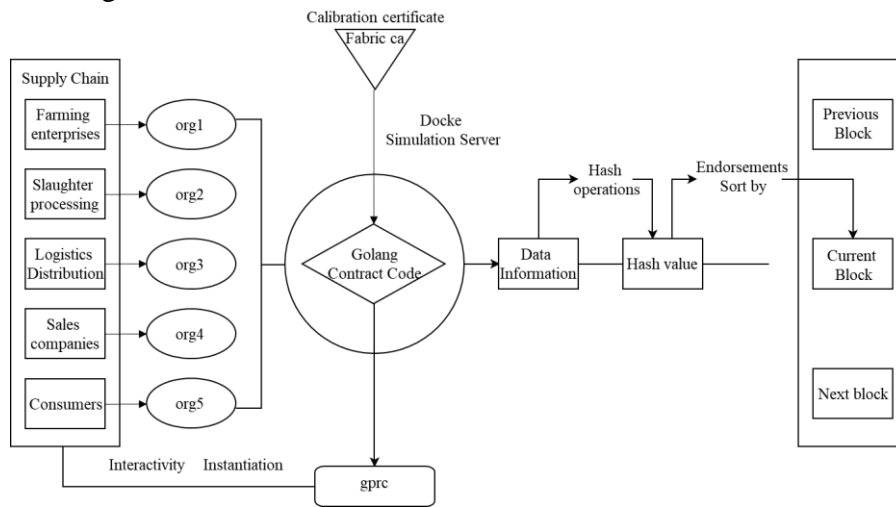


Figure 3: Block details

The organizations involved in beef cattle production upload information through the management side, run the smart contract chain code written by Golang in the Docker simulation server, instantiate and complete the test with the organization through the gprc protocol and solo, and reach a consensus with all parties. After that, it can be linked, and the registration information is given a key by Fabric ca certificate, and finally all the supply processes are completed to form a blockchain network system.

### 3.2. Smart Contract Design

The smart contract is a piece of code deployed on the blockchain. Combined with blockchain technology, it has the advantages of non-tampering and free contract establishment. It is a digital protocol that automatically runs the code when the trigger condition is reached. It can be signed from a third-party self-executing contract to ensure the stability of the contract. The smart contract using the Hyperledger Fabric framework in the super ledger is also called on-chain code, which is divided into system chain code and user chain code. It is written in go and javaScript languages [20]. It runs in a protected docker container, and its interactive communication is completed with peer organizations through the gprc protocol [21]. The implementation of the smart contract can be divided into three steps: construction, storage and invocation. After the multi-user jointly formulates the contract, the protocol is written to the system and uploaded to the blockchain network. The organization periodically verifies whether the trigger condition is met and the contract is concluded. In the contract, both the participating end and the management end can obtain information through the specified permissions and operations to ensure data security and the smooth operation of the traceability system. The functional structure of the smart contract code in this system is shown in Figure 4.

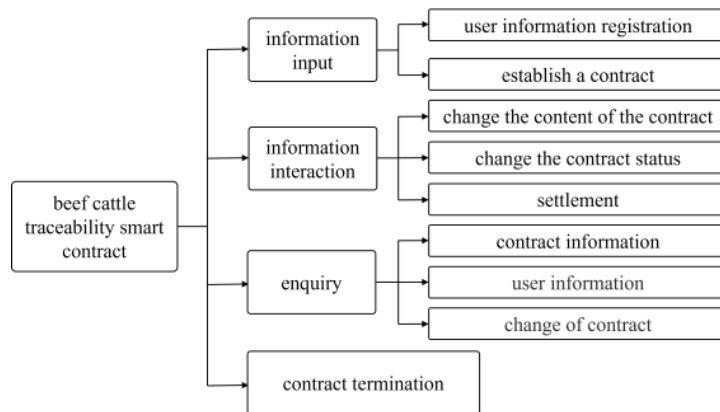


Figure 4: Beef cattle traceability intelligent contract function structure diagram

### 3.3. Traceability ID Design

The snowflake algorithm was originally used by Twitter to generate a unique ID in its internal distributed environment. It can meet the requirements of high availability, uniqueness, high performance, and incrementality of distributed ID generation, and can prevent crawlers from crawling data based on the self-increment of ID. Its core idea is to generate a 64-bit long type global unique ID. The optimized snowflake algorithm has higher efficiency in generating ID, which is composed of time difference, workerID and sequence number. The time difference is the total time difference between system time and base time, which supports time callback processing and can adapt to the unique ID of generating critical time. WorkerID is the only ID used to distinguish different machines and applications. The number of sequences is set by the parameter SeqBitLength. By optimizing the snowflake algorithm, the ID added in the beef cattle breeding process is used as the global ID, the circulation ID is generated in each process link, and the traceability ID is generated after the consumer product is signed.

### 3.4. System Implementation Process

The traceability system consists of a client, a database and a server. The client is connected to the system through a B/ S architecture. It needs to be implemented collaboratively under Web-side services, Mysql database server, Docker container, Hyperledger Fabric framework, development language Go, JavaScript, and development framework Node. Js.

The system can be divided into management end and participation end according to the user role. The management end manages the system and has the power to add account information and give the key. When the information is entered, the API interface is called to complete the data chaining, and the data is encoded and exchanged in the form of JSON.

The function of the traceability system determines that it has many participants, such as enterprises, consumers, and regulatory authorities. Among them, enterprises have information entry rights. When information is entered, it is confirmed by the chain code query on Fabric, and the corresponding smart contract is automatically called. After the agreement conditions are met, the executable program saves the data into the database; consumers have the right to trace the whole process of product production and consumption. When tracing information, consumers send requests to the server. After receiving the query request, the server judges the legality of the request and verifies the user account. By pointing the instructions of different users to different chain codes, the product traceability ID is returned and the corresponding search results are displayed to realize data query. The implementation process of the traceability system is shown in Figure 5.



Consumers can obtain the plaintext traceability ID after the private key of the blockchain network is decrypted through the server. The system matches the local traceability information with the traceability ID, and verifies the data on the chain and the local database at the same time. If it passes the verification at the same time, it returns the query result corresponding to the instruction, and then queries the irreversible Hash value generated by the traceability ID encrypted on the organization server, and sends the Hash value to the blockchain.

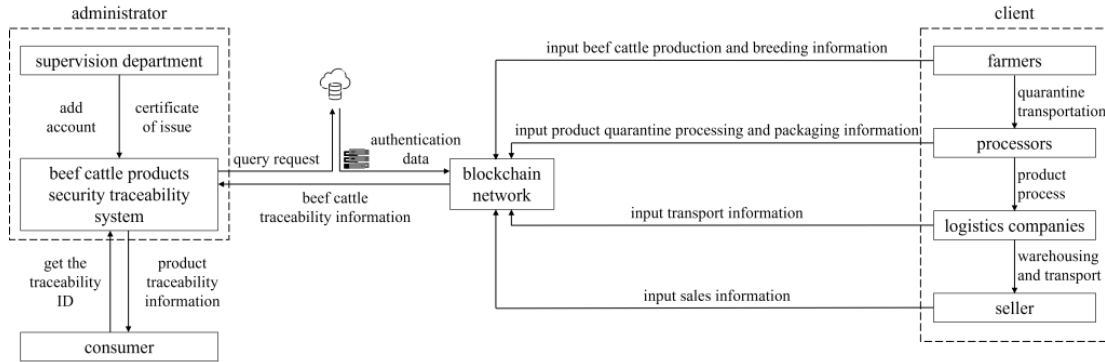


Figure 5: Traceability system implementation process

#### 4. System Application and Test

The beef cattle product anti-counterfeiting traceability system includes data module and blockchain module, as shown in Figure 6. The data module mainly includes data processing and data storage. Firstly, the data processing part mainly generates the traceability ID through the snowflake algorithm, and then encrypts and decrypts the traceability ID through the improved RSA algorithm. The traceability ID is obtained by the consumer scanning code; secondly, the data storage part includes uploading the information added by the organizations of the alliance chain to the blockchain and the local database, storing the data hash abstract and RSA private key, and completing the data verification. When the traceability ID matches the local traceability information and the hash verification is successful, the data on the chain is returned to the front end, that is, the correctness verification of the data is completed. The blockchain module is mainly used to display the participating block height, participating organization, data hash, transaction ID, and timestamp in the browser to ensure the accuracy of the data and perform block verification.

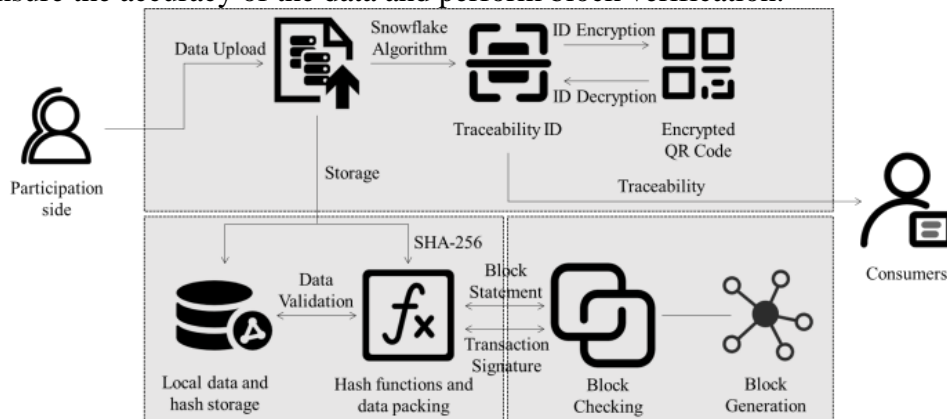


Figure 6: System structure diagram



## 4.1. Blockchain Network

In the blockchain system, the information is uploaded to the chain by the way of organizing interaction with smart contracts and sharing privacy certificates. The uploaded information is open on the chain after the chain code query and verification on the Fabric, and is recognized by the organizations in the chain and stored in the system. Through the information of beef cattle, the binding of beef cattle under the chain and the ID on the chain is realized, and the information of the whole process of beef cattle production and circulation is uploaded to the chain to realize the new industrial model of “beef cattle + blockchain”. Taking the farm as an example, the uploaded beef cattle breeding information is shown in Figure 7.


```
Query has completed, checking results
Response is {"id":"7315284726181425834","birth_time":"2022-6-15
13:47:22", "cattle_cattle__name":"aberdeen angus","fodder":"corn
stalk", "quarantine":"qualification", "end_time":"2023-3-12"}
```

Figure 7: Upload beef cattle breeding information

## 4.2. Traceability Process and Test Structure

Consumers obtain ciphertext from the anti-counterfeiting traceability system by scanning the two-dimensional code, so as to decrypt and obtain the traceability ID, and then perform secondary decryption on the traceability ID by improving the RSA algorithm. The Montgomery modular exponentiation method is used to achieve rapid optimization and improve the secondary decryption efficiency. Then the traceability ID is obtained from the blockchain network by the virtual machine through IP, and the data verification is performed. After the verification is successful, the chain code of each organization is called to query the data, and the basic information of the beef cattle product is returned to the front end. Taking the obtained traceability ID of 7315284726181425834 as an example, some traceability information is displayed as follows:

The breeding information is shown in Figure 8, including the return of beef cattle varieties, the birth time of beef cattle, the name of feeding feed, whether the inspection and quarantine is qualified, the transfer time, and the location of the farm.



Farming Slaughter Logistics Sales

7315284726181425834
Beef cattle breeds: Angus cattle
Beef cattle birth date: 2022-6-15
Feeding feed: corn stover
Is the quarantine qualified: qualified
Beef cattle turn out time: 2023-3-12

Figure 8: Beef cattle breeding information


Slaughter and processing information as shown in Figure 9, return to the transfer time, slaughter time, pre-slaughter inspection is qualified, beef cattle quarantine is qualified, transfer time, slaughterhouse location and other information.



7315284726181425834
Beef cattle turn-in time: 2023-3-18
Beef cattle slaughter time: 2023-4-1
Whether the test is qualified: qualified
Beef cattle turn out time: 2023-4-3

Figure 9: Beef cattle slaughter and processing information


Logistics distribution information is shown in Figure 10, returning logistics ID, location and time.



7315284726181425834
Logistics ID: 7315284726181425333
Departure time: 2023-4-5
Driver: Chen Cheng
Tel: 13546723458
Arrival date: 2023-4-9

Figure 10: Beef cattle product logistics distribution information

The sales information is shown in Figure 11, returning information such as transfer-in time, sales form, sales time, and sales company name.



7315284726181425834
Product transfer date: 2023-4-9
Product sales form: channel sales
Product sale date: 2023-4-10

Figure 11: Beef cattle product sales information

### 4.3. Performance Test

The performance test of the traceability system is carried out. The blockchain performance test tool of Hyperledger Caliper is used to monitor the operation of the system in real time. The system throughput and transaction delay are selected as the indicators of this performance test. The test conditions are set to be 100 transactions and the running time is 30 seconds. Set 10 performance tests, each test uses Caliper to initiate a simulated transaction, the number of concurrent transactions is 1000, a total of 10,000 times. The test results are shown in Figure 12 and Figure 13. The horizontal axis is concurrent transaction volume, and the vertical axis is system throughput and average transaction delay. On the whole, the average transaction delay is proportional to the concurrent transaction volume. Before the transaction volume reaches 400, it is stable at about 0.5 s, and the growth rate of transaction delay has increased significantly since then. When the concurrent trading volume is 100-300 TPS, the system throughput increases with the increase of trading volume, and

then remains at about 254/ s. At this time, it is the maximum throughput of the system and can be applied to actual production practice. There was no collapse during multiple tests, which met the performance requirements of the traceability system.

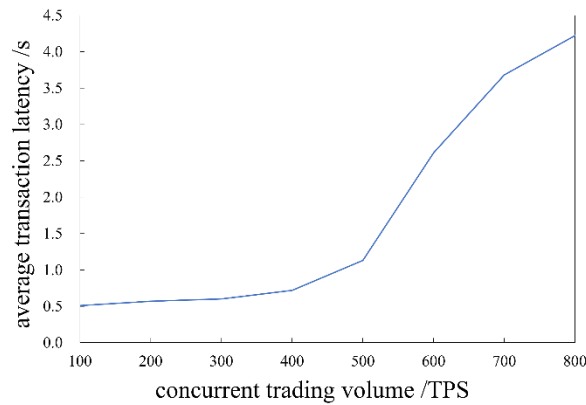


Figure 12: Average transaction delay

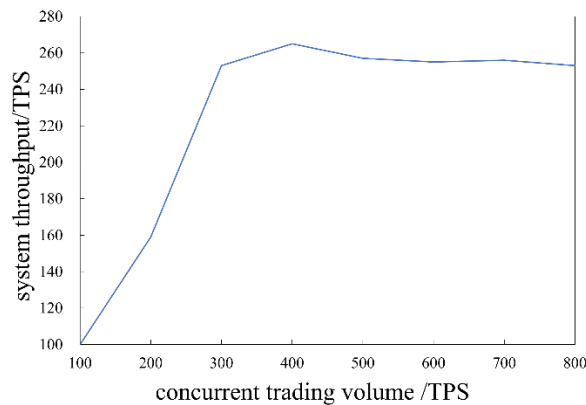


Figure 13: System throughput

## 5. Conclusion

In this paper, the anti-counterfeiting traceability system of beef cattle products is designed by combining blockchain technology with improved RSA algorithm, which provides a theoretical basis and reference framework for realizing the quality traceability management of beef cattle products. This paper mainly draws the following conclusions: First, based on the snowflake algorithm, the circulation ID and traceability ID are generated. Combined with the improved RSA algorithm, the anti-counterfeiting function of the traceability system is realized, which effectively improves the efficiency of the traceability information of the beef cattle product supply chain. At the same time, the performance of the system is tested. The system performs well and there is no chain code collapse, which can meet the basic needs of consumers' traceability query. Then, the blockchain network data is open, transparent, decentralized and tamper-proof, and the blockchain technology has a good application prospect in the field of anti-counterfeiting. In this paper, beef cattle products are taken as the object of supply chain, an anti-counterfeiting traceability framework based on Hyperledger Fabric is built, and an anti-counterfeiting traceability system based on blockchain technology is constructed. The whole supply chain of beef cattle products from breeding, slaughtering, logistics distribution, segmentation and sales is simulated and tested, but the efficiency of each organization consensus algorithm needs to be improved, and it still needs to be improved in subsequent research.

## Acknowledgment

This work is sponsored by National Undergraduate on Innovation and Entrepreneurship Project, No. 202210616013.

## References

- [1] Zhao, W. (2019) *Research on agricultural food safety traceability system based on blockchain technology*. *Techno-economic and management research*, (01): 16-20.
- [2] Wang, L., Ren, J., Wang, T., et al. (2023) *Design and implementation of grain anti-counterfeiting traceability system based on blockchain*. *Science and technology and engineering*, 23 (04): 1625-1634.
- [3] Zhang, Z., Xu, H., He, J., et al. (2021) *micro-service two-dimensional code anti-counterfeiting traceability system*. *computer knowledge and technology*, 17 (20): 1-4 + 8.
- [4] Huang X. (2022) *NFC anti-counterfeiting traceability system design based on blockchain and national secret algorithm*. *Modern Information Technology*, 6 (04): 41-44.
- [5] Zheng, Z., Zheng, H., Ju, J., et al. (2021) *A system for identifying an anti-counterfeiting pattern based on the statistical difference in key image regions*. *Expert Systems with Applications*, 183: p. 115410.
- [6] Lu, Y., Li, P. and Xu H. (2022) *A Food anti-counterfeiting traceability system based on Blockchain and Internet of Things*. *Procedia Computer Science*, 199: p. 629-636.
- [7] Qiu, Z., and Zhu Y., (2023) *Traceability anti-counterfeiting system based on the ownership of edge computing on the blockchain*. *Journal of Ambient Intelligence and Humanized Computing*, 14(1): p. 257-270.
- [8] Xie, S., and Tan, H. (2021) *An Anti-Counterfeiting Architecture for Traceability System Based on Modified Two-Level Quick Response Codes*. *Electronics*, 10(3): p. 320.
- [9] Turki, M., Cheikhrouhou, S., Dammak, B., et al. (2023) *NFT-IoT Pharma Chain: IoT Drug traceability system based on Blockchain and Non Fungible Tokens (NFTs)*. *Journal of King Saud University - Computer and Information Sciences*, 35(2): p. 527-543.
- [10] Sezer, B. B., Topal, S., and Nuriyev, U. (2022) *TPPSUPPLY: A traceable and privacy-preserving blockchain system architecture for the supply chain*. *Journal of Information Security and Applications*, 66: p. 103116.
- [11] Uddin, M. (2021) *Blockchain Medledger: Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry*. *International Journal of Pharmaceutics*, 597: p. 120235.
- [12] Mothukuri, V., Cheerla, S., Parizi, R., et al. (2021) *BlockHDFS: Blockchain-integrated Hadoop distributed file system for secure provenance traceability*. *Blockchain: Research and Applications*, 2(4): p. 100032.
- [13] Alamsyah, A., Widiyanesti, S., Wulansari, P., et al. (2023) *Blockchain traceability model in the coffee industry*. *Journal of Open Innovation: Technology, Market, and Complexity*, 9(1): p. 100008.
- [14] Li, X. Q., Jiang, P., and Chen, T. (2020) *A survey on the security of blockchain systems*. *Future Gener Comput Syst* 107:841–853
- [15] Chen, C., Fang, C., Zhou, M., et al. (2022) *A Blockchain-Based Anti-Counterfeit and Traceable NBA Digital Trading Card Management System*. *Symmetry*, 14(9): p. 1827.
- [16] Yang, X., Li, M., Yu, H., et al. (2021) *A Trusted Blockchain-Based Traceability System for Fruit and Vegetable Agricultural Products*. *IEEE Access*, 9: p. 36282-36293.
- [17] Munasinghe, U. J., and Halgamuge M. N., (2023) *Supply chain traceability and counterfeit detection of COVID-19 vaccines using novel blockchain-based Vacleger system*. *Expert Systems with Applications*, p. 120293.
- [18] Gao, L., Xue, L., Ma, Z., et al. (2023) *Big data RSA public key encryption security two-way detection simulation*. *Computer simulation*, 40 (02): 410-414.
- [19] Cheng, J., Zhang, Y., Yuan, Y., et al. (2022) *PoEC: A Cross-Blockchain Consensus Mechanism for Governing Blockchain by Blockchain*. *Computers, Materials & Continua*, 73 (1): p. 1385-1402.
- [20] Ma, C., An, J., Bi, W., et al. (2018) *Smart contracts in blockchain*. *Information network security*, (11): 8-17.
- [21] Yang, Y., Lin, T., Chen, J., et al. (2022) *Design of fully homomorphic encryption smart contract in edge computing mode*. *Journal of Information Security*, 7 (02): 150-162. DOI: 10.19363/J.cnki.cn10-1380/tn.2022.03.10.