ISSN 2616-5775 Vol. 5, Issue 5: 69-74, DOI: 10.25236/AJCIS.2022.050509

A Supply Chain Traceability Scheme Based on Blockchain

Peng Zhao[1,a], Shiren Ye[1,b,*]

[1]School of Computer Science and Artificial Intelligence, Changzhou University, Changzhou, Jiangsu, China
[a]874992250@qq.com, [b]yes@cczu.edu.cn
**Corresponding author*

Abstract: *The traditional supply chain management system generally uses the centralized server to store the data, which has the problems of opaque transaction information, high maintenance cost of the central server and low database security factor. In order to improve the transparency and security of data in the supply chain system, this paper uses blockchain technology for supply chain management. In addition, the cost of maintaining the anti-counterfeiting traceability platform in the traditional supply chain management system is very high, and the anti-counterfeiting code is easy to be stolen. In order to reduce the hardware cost of the anti-counterfeiting traceability platform, this paper designs a set of anti-counterfeiting traceability mechanism of supply chain products based on asymmetric encryption and digital signature technology, which improves the function of the system application layer. In order to reduce the hardware cost of the anti-counterfeiting traceability platform, this paper designs a set of anti-counterfeiting traceability mechanism of supply chain products based on asymmetric encryption and digital signature technology, which improves the function of the system application layer. In order to further improve the data processing efficiency and stability of blockchain network, this paper improves the master peer selection algorithm in fabric network.*

Keywords: *Blockchain, Supply Chain, Hyperledger Fabric, Cryptography, Consensus algorithm*

1. Introduction

With the development of blockchain technology, researchers all over the world continue to explore the technical potential of blockchain, combine blockchain technology with all walks of life, and hope to solve the pain points in some industries through the characteristics of decentralization, tamper proof and easy traceability of blockchain technology [1]. In the field of supply chain management, blockchain technology is widely combined with Internet of things, digital radio frequency code and other technologies, which has achieved good results and attracted the attention of all sectors of society [2].

The traditional supply chain management system is generally dominated by the core enterprises. The core enterprises have the right to speak in the supply chain. The evil cost of the core enterprises is low, the demands of the bottom enterprises in the supply chain are difficult to be conveyed, and the trust foundation among enterprises in the supply chain network is weak [3]. The traditional supply chain management system is based on the centralized server. The upper limit of system load is seriously restricted by the performance of the central server. It is very expensive to maintain a high-performance server, and once the centralized server and database are broken, it will bring serious security threats to the whole supply chain. In addition, the traditional supply chain management system should maintain a high-cost anti-counterfeiting traceability platform when carrying out anti-counterfeiting traceability [4].

In order to solve the above problems, combined with the characteristics of blockchain, which is highly transparent, tamper proof and easy to trace, this paper proposes a supply chain tracing scheme based on blockchain technology. The second section of the article expounds the application of relevant blockchain technology in the field of supply chain. The third section describes the alliance chain consensus mechanism and master node selection mechanism used in this paper. The fourth section describes the anti-counterfeiting encryption algorithm of supply chain goods and the traceability mechanism of supply chain goods. In The fifth section, we summarize the current research and point out the problems to be solved in the future.

ISSN 2616-5775 Vol. 5, Issue 5: 69-74, DOI: 10.25236/AJCIS.2022.050509

2. Related work

Since 2016, blockchain and its application have attracted the attention of researchers, engineers and practitioners. The special meeting of "blockchain International Conference" held in 2018 focused on the application of blockchain technology and smart contract in various industries including supply chain [5].

Behnke [6] investigated and analyzed the cases in the food supply chain, determined 18 boundary conditions for the traceability of the supply chain, analyzed the feasibility of using bitcoin network to build the food supply chain, and pointed out that before applying bitcoin technology to the supply chain system, it is necessary to customize the supply chain structure to meet the corresponding boundary conditions. Chen [7] summarized the development process of supply chain management based on blockchain technology by analyzing the relevant literature in recent years, and pointed out that the combination of smart contract technology with Internet of things (lot), radio frequency identification (RFID), short-range wireless communication (NFC) and other technologies can promote the automation of supply chain management. The early research on the supply chain management platform based on blockchain technology focused on using blockchain technology to improve the transparency and traceability of data in the supply chain network. For example, Tian [8] et al. combined supply chain management with RFID tags and blockchain, labeled the data generated in the process of production, processing, storage and transportation with RFID tags and stored them in the blockchain, realizing the traceability of supply chain data. Antonucci [9] et al. designed a highly transparent wood traceability system through Internet of things devices and RFID tags, and stored the wood data and identity tags in the database and blockchain respectively.

With the maturity of supply chain traceability scheme based on blockchain, scholars' research direction turns to blockchain system design, data security, credit evaluation, privacy protection and so on [10]. Liang [11] used Stackelberg game to analyze the risk decisions of manufacturers and retailers in the supply chain, and analyzed the impact of blockchain technology on supply chain risk aversion through weighted numerical simulation. The results show that the application of blockchain technology can break the information barrier between enterprises and save unnecessary expenses caused by information occlusion among supply chain members. Shahid [12] and others used aiFang platform to provide a complete solution for traceability of agricultural food supply chain, and analyzed the security and availability of supply chain management scheme based on smart contract. Caro [13] et al. proposed a blockchain solution agriblockiot for agricultural products supply chain management in combination with Internet of things technology, which realizes the information traceability of agricultural products in the whole process of production and sales. However, the solution has the problem of insufficient computing power of edge peers, resulting in low overall system throughput. Although more and more blockchain based supply chain management projects have been implemented one after another, the blockchain platform still has the problem that the data throughput is difficult to meet the needs of massive data in the supply chain. In order to solve the problem of insufficient blockchain network throughput, Salah [14] and others combined blockchain technology with distributed file system (IPFs), improved the throughput of the whole system by compressing the data on the blockchain, and provided a supply chain system with high transparency and traceability in a safe, reliable and efficient manner.

3. Consensus algorithm design

3.1. Kafka Consensus Configuration

The hardware platform of the system is as follows: Intel Core i7 8700k 4.3GHz processor, NVIDIA RTX2080TI graphics card, DDR4 32G memory, 1T solid state drive. The software platform is as follows: Ubuntu 16.04 operating system, Hyperledger Fabric1.4, Golang 1.8, Docker 2.0.

This paper adopts Apache Kafka consensus mechanism. Compared with the tradi-tional consensus mechanism based on workload proof, Kafka consensus speed is faster, and the hardware overhead is small and will not cause energy waste. Compared with the consensus algorithm based on Byzantine fault tolerance, Kafka consensus still has better system throughput when it accommodates more peers. Compared with Proof of Work and Proof of Stake, Kafka consensus has sufficient fault tolerance but poor resistance to malicious attacks. Considering that general enterprise databases are deployed in the intranet, and only enterprises with a foundation of trust can join. Therefore, this paper selects the more powerful Kafka consensus mechanism without considering the existence of external attacks. The simulation platform of this paper adopts the consensus mechanism based on Kafka cluster as shown in Figure 1.

ISSN 2616-5775 Vol. 5, Issue 5: 69-74, DOI: 10.25236/AJCIS.2022.050509

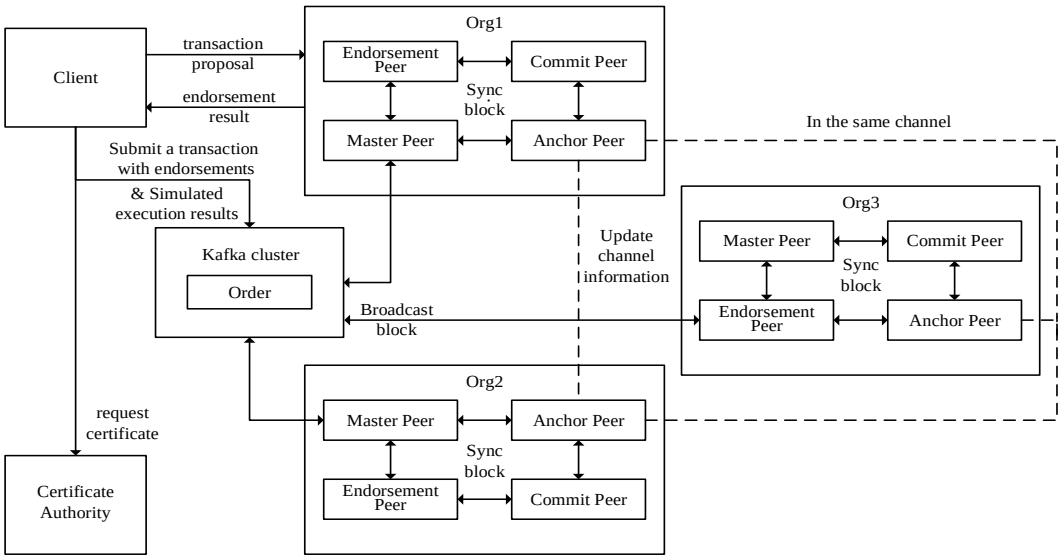

Figure 1: Kafka consensus architecture.

3.2. Dynamic Leader peer election

In fabric network, when a transaction needs to go up the chain, it needs to go through the following steps: first, the client submits the transaction proposal to the endorsement peer; After endorsing and verifying the proposal, the endorsement peer sends the proposal result back to the client; Sending the simulated transaction result and execution result to the client; The sorting peer sorts and packages the transactions, broadcasts the newly generated blocks to the network, and allows the peers in the network to receive the blocks and update the peer status and ledger information. When the master peer leader receives the information distributed by the sorting peer, it will send the message to other peers in the same organization. Generally, fabric defines the master peer in the organization through the configuration file, which will define one or more peers in the organization as the master peer of the organization. This way of specifying the master peer through the configuration file is called the static election of the master peer. Its advantage is that it eliminates the process of peer election, and its disadvantage is that when the master peer in the organization fails, the data can not be synchronized. The specific master peer selection process is shown in Figure 2.

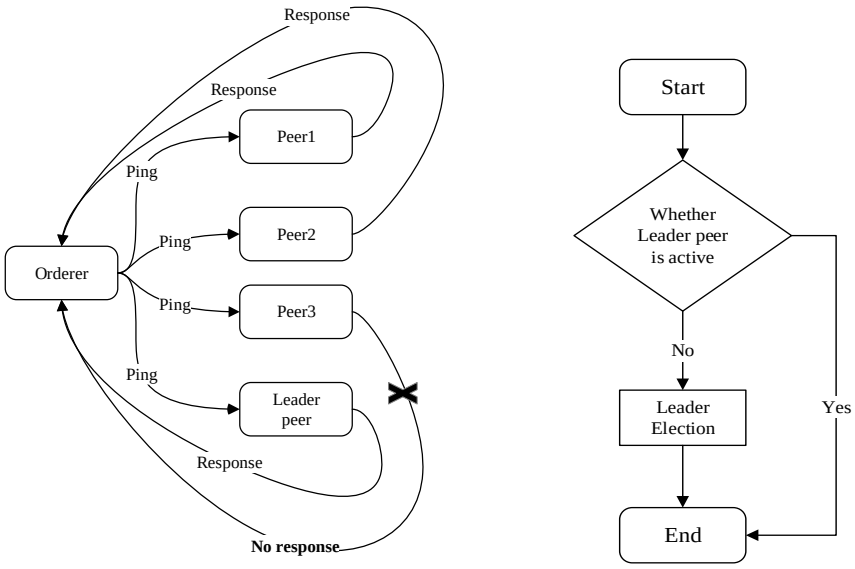

Figure 2: Dynamic Leader peer selection process.

In the static master peer election, defining a small number of master peers may lead to the failure of data synchronization due to peer failure. Defining a large number of master peers will consume a lot of performance of sorting peers. Therefore, this paper adopts the method of dynamic master peer selection to select the master peer, selects a peer peer in each organization as the master peer through the election

ISSN 2616-5775 Vol. 5, Issue 5: 69-74, DOI: 10.25236/AJCIS.2022.050509

algorithm, detects the connectivity of the master peer at regular intervals, and re selects a new master peer once the master peer goes down and the pseudo code is shown in Table 1.

Table 1: Algorithm of Leader peer selection.

Algorithm: Leader peer selection

```
Func (le *leaderElectionSvcImpl) leaderElection(){
//Ping all peers and receive reponsese
Le.logger.trace("starting ping");
//  Add all active peers to the list
List [leader.PingRespones] = pingRespones(pingTimeout).append();
If (pingRespones == null){
   Return No ping responses;
}
For i in PingRespones
      // Judge whether the Leader peer is in the list
      If i is leader;
         Return leader peer is actice
//  Weed out peers that can not be Leader peer
      If i does not ringt for become leader
         Remove pingRespones[i];
      //  Randomly select an active peer as the Leader peer
       Leader = radom.choice(PingRespones)
         Return leader election success;
```

4. Traceability Method Design

4.1. Analysis of the Influence of the Number of Peers on the System Performance

After purchasing the products produced by enterprises within the supply chain alliance, consumers need to trace the identity of the products. After leaving the factory, the products in the supply chain not only have the ID ID code of the products themselves, but also include the anti-counterfeiting code of the products. The generation algorithm of the anti-counterfeiting code is as follows: The production enterprises in the supply chain alliance use the elliptic curve algorithm to produce a pair of public-private key pairs, including private key K and public key kg. Firstly, after the manufacturer produces the product, the identity ID of the product is hashed and mapped through the sha256 algorithm. Then, the manufacturer uses the asymmetric encryption algorithm to generate the public-private key pair, and uses the private key to digitally sign the hash summary of the identity ID. when the product anti-counterfeiting verification is required, the user uploads the anti-counterfeiting code, and the manufacturer de signs and authenticates the anti-counterfeiting code through its own public key. If the verification fails, it indicates that the commodity is not genuine. Assuming that the ID of the product is, the digital summary after the sha256 algorithm is. The generation process of the digital summary is shown in the formula:

$$m' = \text{sha}\,256(m) \tag{1}$$

Then, the private key used by the manufacturer digitally signs the digital summary to generate the anti-counterfeiting code. The generation process of the manufacturer's public-private key pair is as follows. Select the key pair (,) which is the manufacturer's private key and the manufacturer's public key, where the point is a point on the elliptic curve in the finite field in Riemannian geometry, and. The points on the elliptic curve meet the following conditions. If a straight line has three intersections with the elliptic curve, where 0 is the infinity point on the elliptic curve, the relationship is shown in formulas (2), (3):

$$P + Q + R = 0 \tag{2}$$

$$P + Q = -R \tag{3}$$

If point P and the tangent of the elliptic curve are also compared with point R of the elliptic curve, it is recorded as:; That is, and R are points symmetrical to each other about the symmetry plane. From this, we can calculate the value we can calculate by N times of addition. When an ellipse is on a finite field, find a large enough one by analogy to make the equation hold. If there are points, and satisfy the following

ISSN 2616-5775 Vol. 5, Issue 5: 69-74, DOI: 10.25236/AJCIS.2022.050509

formula (4):

$$\mathrm{R}(X_r, Y_r) = P + Q \tag{4}$$

When $(P \neq Q)$,the value of λ is shown in formulas (5) and (6), and the value of is shown in formula (7).

$$Y_r = (\lambda(X_p - X_r) - Y_p) \bmod P \tag{5}$$

$$Y_r = (\lambda(X_p - X_r) - Y_p) \bmod P \tag{6}$$

$$\lambda = \frac{(Y_q - Y_p)}{(X_q - X_p)} \bmod P \tag{7}$$

When $(P = Q)$, the value of λ is shown in formula (8);

$$\lambda = \frac{(3X_p^{\ 2} + a)}{2Y_p} \bmod P \tag{8}$$

The generation process of anti-counterfeiting code is as follows: select the private key, base point, and calculate the digital signature according to the random number and digital summary, as shown in formula (9), as the anti-counterfeiting code.

$$S = \frac{(m' + kx)}{r} \tag{9}$$

After the anti-counterfeiting code is uploaded to the verification platform, the platform carries out the verification process according to formula (10) through the manufacturer's public key.

$$\frac{m'G}{S} + \frac{xQ}{S} = \frac{m'}{S} + \frac{xkG}{S} = \frac{(m' + xk)G}{S} = \frac{r(m' + xk)G}{(m' + kx)} = rG \tag{10}$$

The anti-counterfeiting code is de signed and verified by the manufacturer's private key. If it can be de signed successfully, it shows the authenticity of the data. In the elliptic curve encryption algorithm, it is easy to calculate the public key according to the given private key and base point. However, through the given public key and base point G, it is required that the most effective algorithm complexity of solving the private key is, where is the order of, and P is the maximum prime factor of the order. At that time, it was unrealistic to break through the elliptic curve algorithm with the current computing power.

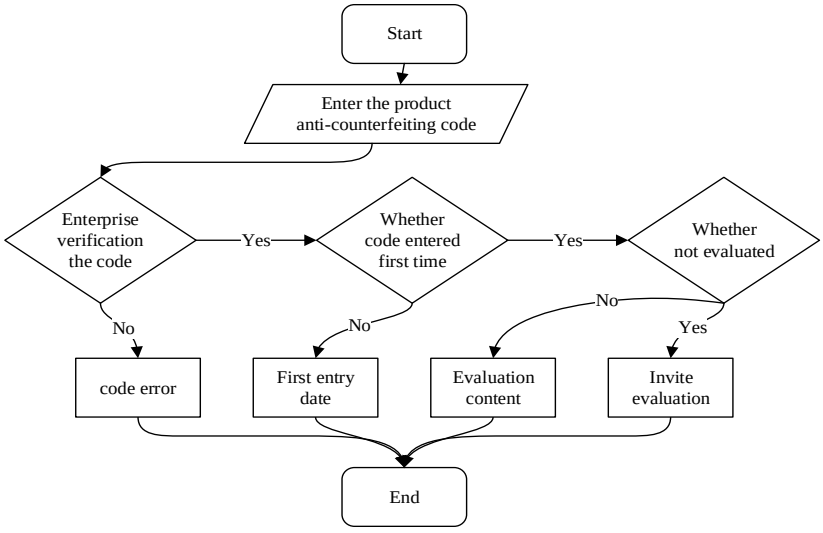

Figure 3: Product anti-counterfeiting verification process.

The anti-counterfeiting code is generated through the elliptic curve encryption algorithm to ensure that the anti-counterfeiting code cannot be forged. In order to prevent the product from being recorded by criminals in the process of circulation, check whether the anti-counterfeiting code is verified for the first time through the platform. If the anti-counterfeiting code has been verified, return the first

ISSN 2616-5775 Vol. 5, Issue 5: 69-74, DOI: 10.25236/AJCIS.2022.050509

verification date; If the product has been evaluated, the evaluation result is returned; if the product has not been evaluated, the user is invited to evaluate. The specific flow chart of product anti-counterfeiting verification is shown in Figure 3.

5. Conclusions

With the advent of the era of blockchain 3.0, the concept of blockchain + business database has received extensive attention from all walks of life in society, and the blockchain network has been applied to various fields as a trust network. This paper designs a supply chain transaction processing architecture based on block-chain technology, and uses experiments to demonstrate the feasibility and effi-ciency of this architecture. This article uses the Hyperledger Fabric framework to design, realizes the transaction processing in the supply chain, uses the channel isolation method to realize the protection of private data in the transaction process, and guarantees the transaction processing speed and data storage efficiency through the multi-layer database design. This paper designs a set of anti-counterfeiting and traceability mechanism of supply chain products based on asymmetric encryption and digital signature technology, which improves the function of the system application layer. In addition, this paper designs a set of anti-counterfeiting and traceability mechanism of supply chain products based on asymmetric encryption and digital signature technology, which improves the security of the supply system.

This solution still has some problems to be solved later, such as how to achieve rapid product traceability on the chain under the premise of meeting privacy data protection is still difficult, and how to further improve the efficiency of the con-sensus algorithm. These issues are worthy of further study.

References

[1] Naimi A I, Westreich D J. Big data: a revolution that will transform how we live, work, and think [J]. American Journal of Epidemiology, 2014, 179(9): 1143-1144.

[2] Kouhizadeh M, Saberi S, Sarkis J. Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers [J]. International Journal of Production Economics, 2021, 231: 107831.

[3] Meiklejohn S, Pomarole M, Jordan G, et al. A fistful of bitcoins [J]. Communications of the Acm, 2016, 59(4): 86-93.

[4] Kim H M, Laskowski M. Toward an ontology-driven blockchain design for supply-chain provenance [J]. Intelligent Systems in Accounting, Finance and Management, 2018, 25(1): 18-27.

Pierro, Di M. What is the Blockchain [J]. Computing in Science & Engineering, 2017, 19(5): 92-95.

[5] Stoepker I, Gundlach R, Kapodistria S. Robustness analysis of Bitcoin confirmation times [J]. ACM SIGMETRICS Performance Evaluation Review, 2021, 48(4): 20-23.

[6] Behnke K, Janssen M. Boundary conditions for traceability in food supply chains using blockchain technology [J]. International Journal of Information Management, 2020, 52: 101969.

[7] Chang S E, Chen Y. When blockchain meets supply chain: A systematic literature review on current development and potential applications [J]. IEEE Access, 2020, 8: 62478-62494.

[8] Tian F. An agri-food supply chain traceability system for China based on RFID & blockchain technology [C]// 2016 13th international conference on service systems and service management (ICSSSM). IEEE, 2016: 1-6.

[9] Figorilli S, Antonucci F, et al. A blockchain implementation prototype for the electronic open source traceability of wood along the whole supply chain [J]. Sensors, 2018, 18(9): 12.

[10] Di Pierro M. What is the blockchain? [J]. Computing in Science & Engineering, 2017, 19(5): 92-95.

[11] Liang L, Futou L, Ershi Q. Research on risk avoidance and coordination of supply chain subject based on blockchain technology [J]. Sustainability, 2019, 11(7): 2182.

[12] Shahid A, Almogren A, Javaid N, et al. Blockchain-based agri-food supply chain: A complete solution[J]. IEEE Access, 2020, 8: 69230-69243.

[13] Caro M P, Ali M S, Vecchio M, et al. Blockchain-based traceability in Agri-Food supply chain management: A practical implementation[C]// IoT Vertical and Topical Summit on Agriculture-Tuscany, 2018: 1-4.

[14] Salah K, Nizamuddin N, Jayaraman R, et al. Blockchain-based soybean traceability in agricultural supply chain [J]. IEEE Access, 2019, 7: 73295-73305.