ISSN: 2414-1895 DOI: 10.6919/ICJE.202003_6(3).0041

Research on High-security Product Traceability Method Based on Blockchain

Shaoke Liu

School of Economics and Management, Xidian University, Shaanxi 710100, China

askliu1022@163.com

Abstract

With the rapid development of the logistics industry, the problem of product information traceability in the supply chain is becoming more and more serious. However, the traditional product traceability system has some shortcomings, such as the vulnerability of centralized database, the inability to avoid tampering, and the difficulty in accountability and positioning. The decentralized, traceable and tamper-proof features of blockchain can improve the existing supply chain and solve the above problems. This paper firstly analyzed the information exchange of products in the supply chain, and then proposed the product information tracing scheme combining block chain, in which the improved DH key exchange algorithm and RC4 encryption algorithm were used to encrypt the product information to improve the security of the information.

Keywords

Product traceability; Blockchain; Supply chain; Encryption algorithm.

1. Introduction

At present, most logistics systems adopt Internet of things technology to improve the information level of logistics system. However, this approach does not solve the disadvantages of data-centric storage, and there are still some problems, such as lack of trust. Due to the opaque manufacturing and transportation processes, the downstream links of the supply chain cannot trust the intermediate links without the phenomenon of shoddy quality. There are also problems of information security. For example, the way of information centralized storage may also lead to the leakage of users' purchase supply information and other private data, and the centralized storage is vulnerable to attacks.

The decentralization and traceability of blockchain can improve the above problems. Therefore, this paper proposes a scheme to realize product information traceability in the supply chain based on block chain technology, and USES improved DH key exchange algorithm and RC4 encryption algorithm to encrypt product information to improve information security.

2. Related Work

2.1 Blockchain

Blockchain is a kind of distributed ledger technology which is jointly maintained by many parties and uses cryptography to ensure the security of transmission and access. It can realize consistent storage and is hard to be tampered. In the blockchain system, all submitted things are stored in the chain. When the new transaction is confirmed, the length of the chain will be increased without modifying the previous data, thus ensuring the completion of the data.

Pradeka Brilyan Purwandoko[2] analyzed the rice supply chain in Java and designed the traceability system architecture based on information technology using information system analysis method, which is still essentially a centralized system. YONG WANG[4] designed a cloud-assisted EHR sharing and security and privacy protection scheme based on alliance chain. The proposed system architecture ensured that patient case data could not be obtained by malicious means, protected patient privacy, and the proposed block structure improved search efficiency. Daouda Ahmat[3] designed an improved multi-path DH key exchange algorithm, which avoids the problem that traditional DH algorithms are vulnerable to man-in-the-middle attacks. Simone Figorilli[6] designed a block chain traceability prototype for the whole process of wood supply chain based on RFID sensor. Jin Hyeong Jeon et al. [5] proposed a more secure service configuration of Internet of things platform based on Ethereum's smart contract and encryption method, aiming at the vulnerability of the database of Internet of things platform. Zhijie Li Shell et al. [1] proposed a hybrid ledger for supply chain, which applies both public and private chains to a system to store different levels of information to ensure user privacy.

Based on the above researches, this paper proposes a traceability scheme based on consortium blockchain and improved DH algorithm after analyzing the information flow of the supply chain.

2.2 Diffie-hellman key exchange algorithm

This algorithm can determine the symmetric keys of both parties on the premise of secure transmission. The core of this algorithm is that the private keys of both parties do not enter the network transmission process. The same Key can be calculated based on the public Key of the other party and the private Key of the other party.

However, Diffie-Hellman algorithm has an obvious flaw: it is vulnerable to man-in-the-middle attack. For example, attacker C plays B when communicating with A and act A when communicating with B. Both A and B negotiate A key with C, and then C can listen and pass the communication.

3. Information flow in the supply chain

The main purpose of traceability is to record the product information and the corresponding information of the product in the supply chain, so that the above information can be inquired to make decisions when needed.

3.1 Use-case diagram analysis

Use case diagrams describe the interactions between one or more participants in a system, so this section uses use-case diagrams to analyze the flow of information in the supply chain.

As shown in the Figure 3-1, each participant records some information. For example, the supplier shall record the name, origin and date of the raw materials; Manufacturers record processing details, such as raw material purchase data, production batches, quality testing, etc. Distributor manages information about the product distribution process; Retailers record the date of purchase and the information of products sold to consumers. The above information is then stored in the block chain in their respective links so that users can retrieve product information based on the data available in the system.

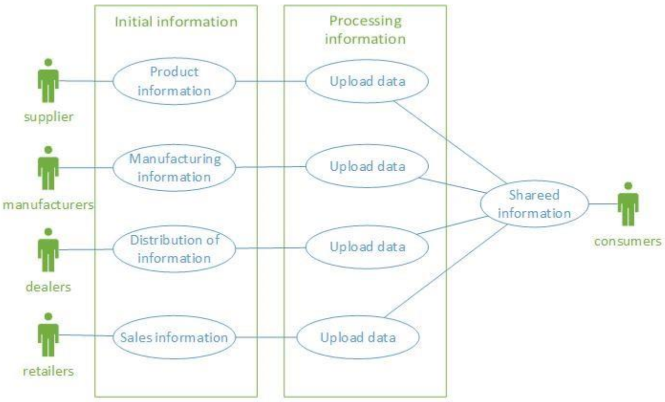


Figure 3-1 use-case diagram

ISSN: 2414-1895
DOI: 10.6919/ICJE.202003_6(3).0041

3.2 Sequence diagram analysis

Sequence diagrams describe how an object interacts with other objects in a system and describe the behavior of objects by describing the messages sent and received between objects. Sequence diagrams are used to communicate business processes by looking at the interactions between objects. The sequence diagram shown depicts the exchange of information between participants in the supply chain.

If a consumer wants to see information about the product he has bought, he can request information about that product, and all participants in the supply chain should provide the required information in real time. Figure 3-2 shows the messages sent by each participant during the traceability process.

Combining the use case diagram with the sequence diagram, we analyze in detail the information that needs to be exchanged.

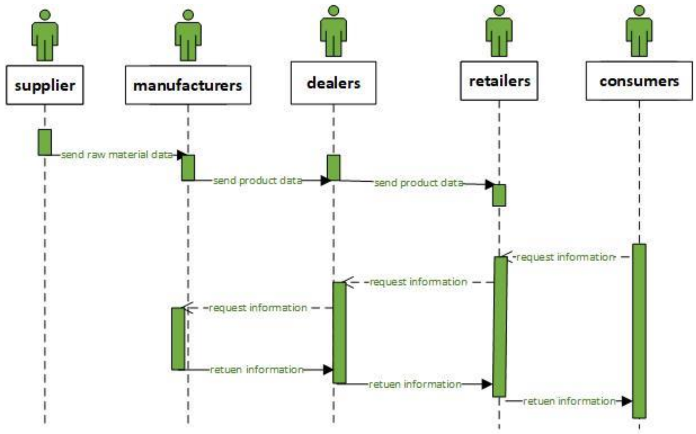


Figure 3-2 sequence diagram of information exchange in the supply chain

While providing raw materials to manufacturers, suppliers also upload the id (such as 1), name, origin, acquisition date, supplier delivery date and other information to the block chain. After receiving the raw materials, the manufacturer will process the products and then upload the product id (such as 1-1), the manufacturer's delivery date, delivery address, product quality and other information to the block chain before delivering the products to the distributor. After the distributor receives the shipment, it sends the product to the designated retailer and uploadesthe product id (such as 1-1-1), the distributor's delivery date, and the shipping address to the blockchain. After receiving the goods, retailers upload the product id (such as 1-1-1-1 -1), delivery date, delivery address and other information to the block chain.

In the above description, the change of product id is due to the one-to-many relationship between raw materials and products in the process of transportation. For example, suppliers sell a batch of raw materials to multiple manufacturers, and manufacturers sell products to multiple retailers through multiple dealers. Therefore, the unique format of product id can help users to find the source of products.

The data is stored in the form of json. Take the supplier as an example, the data to be uploaded to the block chain is as follows:

```
{
    "Id": "1",
    "Name ": " wood ",
    "Place of origin": "Yunnan",
    "Cutting date": "2019.12.1",
    "Supplier delivery date": "2020.1.1"
}
```

ISSN: 2414-1895 DOI: 10.6919/ICJE.202003_6(3).0041

3.3 information flow analysis

In summary, it can be concluded that the information flow in a system that realizes product information traceability in the supply chain should be as shown in the Figure 3-3. In the process of uploading information, suppliers, manufacturers, distributors and retailers need to upload relevant product information, processing information, distribution information and sales information into the block chain in their own links. Since consumers only buy goods and do not participate in the previous links, they do not need to do the above operations. In the process of querying information, all supply chain nodes including consumers can query the product traceability information.

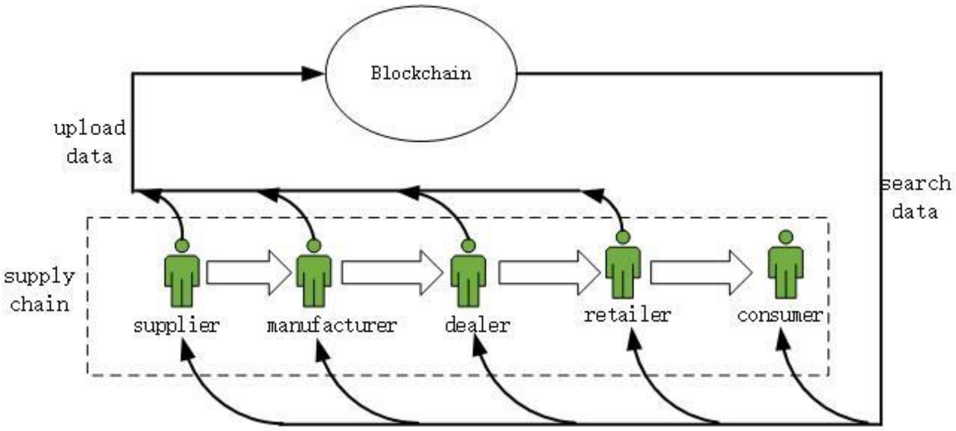


Figure 3-3 information flow in the traceability process

4. Traceability scheme

The proposed traceability scheme framework as shown in the Figure 4-1, including supply chain module, service module and blockchain module.

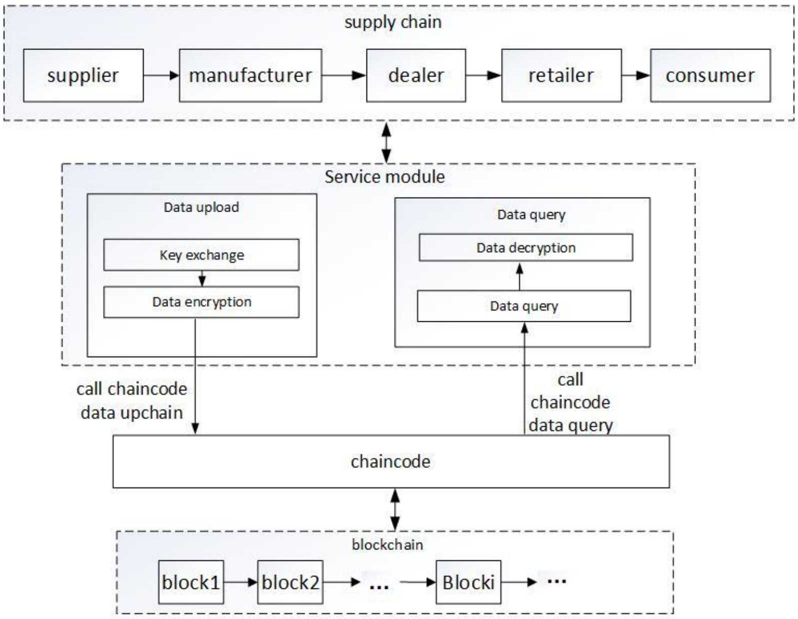


Figure4-1 product traceability scheme

4.1 Supply chain module

The supply chain module includes suppliers, manufacturers, distributors, retailers and consumers. Suppliers, manufacturers, dealers and retailers can upload data and query data, while consumers can only query.

4.2 Service module

The service module includes data uploading and data query.Data uploading includes key exchange and data encryption. Data queriy includes data retrieval and data decryption.

The key exchange adopts the improved DH key exchange algorithm, and the data encryption and decryption adopts RC4 encryption algorithm.

4.2.1 Improved Diffie-Hellman key exchange algorithm

Because the traditional DH algorithm is vulnerable to man-in-the-middle attacks, the key is decomposed into multiple sub-keys, passed through multiple paths, and then reconstructed by another user to avoid man-in-the-middle attacks.

The key exchange protocol includes two steps: Firstly, using Diffie-Hellman algorithm to generate the key $\mathrm{K} = g^S \, mod \, p$; Secondly, splitting the key into n sub-keys, and then the other party will rebuild the key from its sub-key $s_{k0}, s_{k1}, \ldots, s_{kn}$.

(1) key decomposition

In order to generate a subkey, the communicator first needs to create a key $S^k = s$, then a polynomial $f^l(X)$, and $f^l(0) = g^s \, mod \, p$, as shown in algorithm 1.

Valuing $f^l(0) = a_0 = g^s \, mod \, p$, and valuing i from 1 to k-1, then calculating $l_i(X) = a_iX^i$and finally getting polynomial $f^{'}(X) = f^{'}(0) + a_1X + a_2X^2 + a_3X^3 + \cdots \ldots + a_{k-1}X^{k-1}$.

Algorithm 1: Creation of polynom of degree *k*

```
createPolynom(k, gs(mod p)) return Polynom;
$f^l(0) \leftarrow g^s \, mod \, p$
i ← 1
while i ≤ k − 1 do
$a_i$ ← getRandomCoefficient()
if i = k − 1 and $a_i = 0$ then
continue;
$l_i(X) = a_iX^i$;
i ← i + 1;
$f^{'}(X) = \sum_{i=1}^{k-1} l_i(X) + f^{'}(0)$
return $f^{'}(X)$
```

then for $x_i (0 < i < n)$ where $x_i \neq 0$, calculating the $f'(x_i)$, Finally, all the interpolation points $(x_i, f^l(x_i))$ except $(x_0, f^l(x_0))$ are stored in the subKeyList, As shown in algorithm 2.

Algorithm 2: Subkeys generation

```
Input $k, n, g^s \, mod \, p$
$f^l(\mathrm{X}) =$ createPolynom($k, gs(\mathbf{mod}\, p)$)
subKeysList← ⊥
i ← 1
while i ≤ n do
$x_i$ ← getRandomValue();
$f^l(x_i) = \left(x_i, f^l(x_i)\right)$;
```

```
storeInSubKeysList( $f^l$(X), subKeysList[i]);
i ← i + 1;
```

(2) key reconstruction

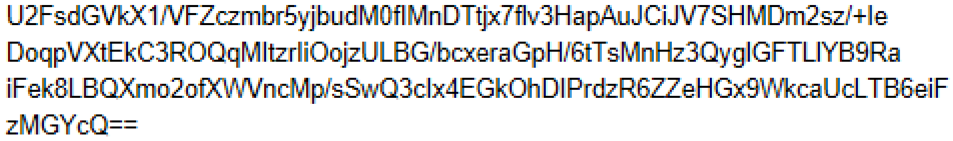
After receiving $\left(x_{i,}\ f^l(x_i)\right)$，（$0 \le i \le n$） the communicator uses algorithm 3 to rebuild the key $K = g^s \, mod \, p$ according to the received sub-key $s_o, s_1, \dots\dots$， s_{p-1} . $F^l(X) = \sum_{i=0}^{p} y_i \, l_i(X) = f^l(x_i) \prod_{j=0, j\neq i}^{n} \frac{X - x_J}{x_i - x_j}$, where $l_i(X) = \prod_{j=0, j\neq i}^{n} \frac{X - x_J}{x_i - x_j}$ and $y_i = f^l(x_i)$.

Algorithm 3: Reconstitution of key from received subkeys

```
Input  $k$, $(x_i, y_i)_{0 \le i \le n}$
Output key
if $|(x_i, y_i)_{0 \le i \le n}| < k$ then
    return ⊥;
else
    foreach $i \in [\![0, n]\!]$ do
        $l_i(X) \leftarrow \prod_{j=0, j\neq i}^{n} \frac{X - x_i}{x_i - x_j}$
        $j \leftarrow 0$
        $f_l(X) \leftarrow 0$
        while $j \le n$ do
            $f_l(X) \leftarrow y_i \times l_j(X) \times f_l(X)$
            $j \leftarrow j + 1$
    return $f_l(0)$
```

Before the user uploads the information, key exchange is conducted first, and then the data to be uploaded is encrypted with the key and then the smart contract is called to upload to the block chain. When the user makes a query, the smart contract is called to get the data from the block chain, and then the key is used to decrypt the data.

For the supplier data mentioned above, after RC4 encryption of the json plaintext data, the cipher text is obtained :



U2FsdGVkX1/VFZczmbr5yjbudM0flMnDTtjx7flv3HapAuJCiJV7SHMDm2sz/+le
DoqpVXtEkC3ROQqMltzrliOojzULBG/bcxeraGpH/6tTsMnHz3QyglGFTLlYB9Ra
iFek8LBQXmo2ofXWVncMp/sSwQ3clx4EGkOhDlPrdzR6ZZeHGx9WkcaUcLTB6eiF
zMGYcQ==

4.3 Blockchain Module

In combination with the characteristics of supply chain, alliance chain is adopted here. Different members in the alliance chain have different permissions. All nodes except consumers can share data, that is, upload data. The uploaded information is ciphertext, so it can effectively protect privacy.

(1) Administrator

Suppliers, manufacturers, distributors, retailers constitute the main members of the alliance chain. Each organization has a node that ACTS as a management node to execute their decisions. The manager is responsible for approving new nodes and verifying valid transactions and blocks. Moreover, the management node can also upload data and query data as an ordinary node.

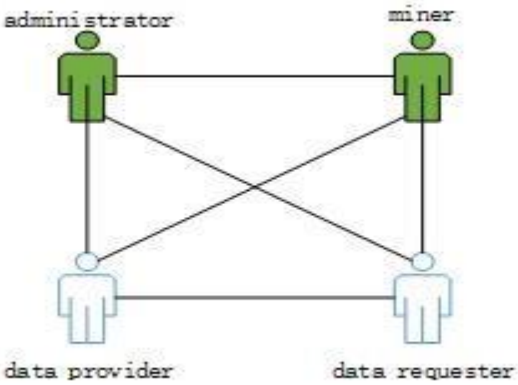


Figure 4.4 nodes in the scheme

(2) Miner

Miners are randomly selected from management nodes. They are responsible for packaging transactions and production blocks. Each partner must provide at least one miner candidate to keep the blockchain working.

(3) Data Provider and Data Requester

Suppliers, manufacturers, distributors and retailers in the supply chain, as data providers in the chain, upload the data to be Shared to the block chain. All nodes, including consumers, can query product information as data requesters. It can be seen that the miner, as the management node, also has the rights of the data provider and the data requester.

5. Conclusion

This paper first proposed to use the improved DH algorithm to achieve a more secure key exchange, and used RC4 algorithm to encrypt and decrypt product information to protect product information security from illegal acquisition. Then the information exchange in the supply chain is analyzed by use case diagram and sequence diagram, and its information flow is summarized. Finally, a scheme design based on block chain is proposed to realize the traceability of product information among participants in the supply chain.

References

[1] Zhijie Li, Haoyan Wu, Brian King, et al. A Hybrid Blockchain Ledger for Supply Chain Visibility. ISPDC 2018: 118-125.

[2] Pradeka Brilyan Purwandoko, et al. Design Framework of a Traceability System for the Rice Agroindustry Supply Chain in West Java. Information 10(6): 218 (2019).

[3] Daouda Ahmat1, Marayi Choroma2. Multipath Key Exchange Scheme Basedon the Diffie-Hellman Protocol and the Shamir Threshold. International Journal of Network Security, Vol.21, No.3, PP.418-427.

[4] Yong Wang, Aiqing Zhang, Peiyun Zhang, Huaqun Wang. Cloud-Assisted EHR Sharing With Security and Privacy Preservation via Consortium Blockchain. IEEE Access 7: 136704-136719 (2019).

[5] Jin Hyeong Jeon, Ki-Hyung Kim, Jai-Hoon Kim. Block chain based data security enhanced IoT server platform. ICOIN 2018: 941-944.

[6] Simone Figorilli, Francesca Antonucci, et al. A Blockchain Implementation Prototype for the Electronic Open Source Traceability of Wood along the Whole Supply Chain. Sensors 18(9): 3133 (2018).

[7] Magdi ElMessiry, Adel ElMessiry. Blockchain Framework for Textile Supply Chain Management - Improving Transparency, Traceability, and Quality. ICBC 2018: 213-227.

[8] Mar á Alejandra Rubio, Giovanny Mauricio Tarazona, et al. Big Data and Blockchain Basis for Operating a New Archetype of Supply Chain. DMBD 2018: 659-669.

[9] Yuqiao Zhang, Ujjwal Guin. End-to-End Traceability of ICs in Component Supply Chain for Fighting Against Recycling. IEEE Trans. Information Forensics and Security 15: 767-775 (2020).

[10] Liu, Pingzeng Liu, Wanming Ren, Yong Zheng, Chao Zhang, Junmei Wang. The Traceability Information Management Platform of Duck Product Industry Chain. ICCCS (6) 2018: 144-153.

[11] Jiawen Kang, Zehui Xiong, Dusit Niyato, Ping Wang, Dongdong Ye, Dong In Kim. Incentivizing Consensus Propagation in Proof-of-Stake Based Consortium Blockchain Networks. IEEE Wireless Commun. Letters 8(1): 157-160 (2019)

[12] Raja Jayaraman, Khaled Saleh, Nelson King. Improving Opportunities in Healthcare Supply Chain Processes via the Internet of Things and Blockchain Technology. IJHISI 14(2): 49-65 (2019)

[13] Yonggui Fu, Jianming Zhu. Big Production Enterprise Supply Chain Endogenous Risk Management Based on Blockchain. IEEE Access 7: 15310-15319 (2019).

[14] Michail Sidorov, Ming Tze Ong, et al. Ultralightweight Mutual Authentication RFID Protocol for Blockchain Enabled Supply Chains. IEEE Access 7: 7273-7285 (2019).