블록체인 기반 물류정보 추적시스템 설계

장림초 [1], 항뢰 [2], 김도현 [1]
[1] 제주대학교 컴퓨터공학과
[2] Shanghai Normal University
zhanglinchao@jejunu.ac.kr, hl2708@sthu.edu.cn, kimdh@jejunu.ac.kr

Design of Logistics Information Traceability System Based on Blockchain

Linchao Zhang[1], Lei Hang[2], Dohyeun Kim [1]
[1] Dept. of Computer Science, Jeju National University
[2] Tianhua College, Shanghai Normal University

Abstract

In recent years, the logistics industry has greatly driven the world's economic development. Due to the frequent occurrence of logistics information leakage and forgery, it is necessary to find a solution that can accurately trace the logistics information and ensure the security and authenticity of the logistics information. The birth of blockchain technology has enabled the logistics industry to realize the development from quantitative change to qualitative change. The distributed storage idea, decentralization characteristics, immutable nature, complex encryption algorithm, and other technical characteristics of the blockchain technology make it have a wide range of application prospects in the logistics industry. The purpose of this paper is to apply blockchain technology to the whole chain of logistics information traceability, to indirectly store the corresponding data generated by the logistics circulation link on the blockchain, and to combine the researched consensus algorithm and searchable encryption algorithm to form A set of logistics information traceability system to achieve efficient and accurate traceability of logistics information.

1. Introduction

In recent years, with the rapid development of e-commerce, the close integration of the logistics industry and various Internet technologies, and the rapid progress of related technologies, many problems still need to be found for better solutions. For example, the problem of traceability of logistics information is not only to query the transportation information such as the origin, route, and destination of the goods but, more importantly, to ensure the authenticity of the information inquired. Blockchain technology is very suitable for logistics information traceability scenarios because of its decentralization. Data is encrypted and stored in a distributed form and cannot be tampered with. Therefore, how to make better use of blockchain technology to protect the privacy of logistics information, prevent logistics information from being tampered with, and improve the efficiency of logistics information traceability are issues that the logistics industry is exploring.

This paper aims to study the application of blockchain technology in the scenario of logistics information traceability. "Logistics information" refers to the corresponding data generated by each link of logistics circulation. In order to query and trace these data, this paper designs a blockchain-based blockchain. The logistics information traceability system, which stores all the logistics information indirectly on the blockchain, constructs a decentralized logistics blockchain. On the one hand, according to the characteristics of logistics information, combined with the research status and application progress of blockchain technology in the logistics industry in the relevant literature [1][2], a multi-center dynamic consensus algorithm MCDPBFT is proposed further improve the efficiency of logistics information traceability. On the other hand, based on the confidentiality of the logistics information itself, in order to ensure the authenticity of the traceable information, a logistics blockchain information traceability algorithm based on searchable encryption is proposed. Finally, the performance tests and comparisons of the proposed MCDPBFT are performed.

2. Multi-center Dynamic PBFT (MCDPBFT)

In this paper, each computer is defined as a node, and the distribution of the nodes is shown in Figure1. In the MCDPBFT algorithm, the nodes are divided into multiple parts. Each part is called a consensus set. Each consensus set has a main Node and the rest of the slave nodes. This paper assumes that the nodes are equally distributed, and each consensus set has the same number of nodes. Each consensus set has its blockchain and stores the transaction data of this consensus set. After the transaction reaches an agreement in the consensus set, it will eventually enter the global consensus. The global consensus set consists of the master nodes in each consensus set. After reaching the global consensus, the system considers that the transaction consensus is complete.

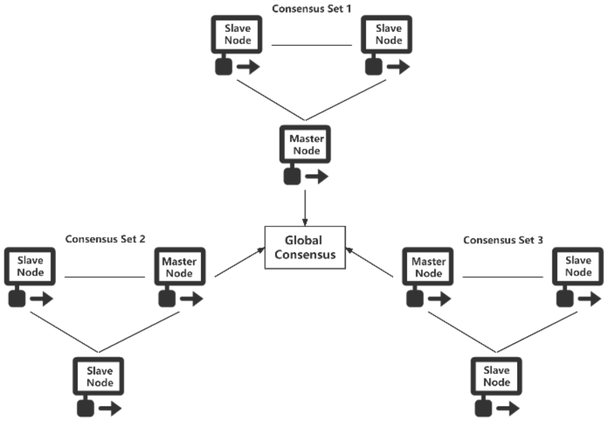

Figure1. Node Division Diagram

(1) Let the number of consensus sets in the system be K, and denote each consensus set (Consensus Sets) as CS_i, then $\{CSi \in \{CS, CS_2, \cdots, CS_K\}$

(2) Denote all master nodes in the cluster as N_P, $N_P = K$, and agent nodes as N_R, then the total number of nodes in the cluster N is:

$$N = N_P + N_R \tag{2.1}$$

(3) Let the number of malicious nodes in the number of N nodes in the cluster be f, then the number of cluster N must satisfy the formula:

$$N \geq \frac{3f+1}{K}$$

(4) This paper uses the authority authentication module in Hyperledger Fabric, namely Membership Service Provider (MSP), to manage the identity information of all nodes. The functions of setting MSP are as follows:

a) All nodes in the system must register identity information in MSP, such as node ID public key.

b) Assuming that a node wants to join the system, it must first register in the MSP and enter the system only after passing the MSP's review. Suppose node I want to exit the system and apply to MSP, and MSP can only go after approval.

3. Sub-Algorithm Design

Figure 2 is the consensus process of the MCDPBFT algorithm:

(1) First, the nodes in the Fabric architecture are evenly divided into K consensus sets, and the nodes in each consensus set to select the master node N_P according to formula;

(2) The client c initiates a transaction request m to the system and sends the request $< REQUEST, m, v, n, t, i >$ to each master node. Each request message records the summary m of the current news, the corresponding view v, the transaction sequence number n, the timestamp of the current request t, and the current master node number;

(3) If a node fails or changes dynamically, the MSP renumbers the node and adds or removes the node to the consensus set. At this time, the view switching protocol is not triggered, and when the master node fails and the current transaction consensus cannot be performed, the view v is renumbered;

(4) Each master node receives the request message from the client and broadcasts a prepared statement to all agent nodes in the consensus set, the message format is $< PREPARE, m, v, n, t, i >$;

(5) The agent node verifies the message and sends a confirmation message to the master node and the other agent nodes; that is, it enters the confirmation (COMMIT) stage, in the format $< COMMIT, m, v, n, t, i >$. At this point, the internal consensus of each slave consensus set ends;

(6) At this time, a global consensus will be carried out, and the master node that first receives the client request will be the master node of the international agreement, and the global peace will be carried out according to the above steps;

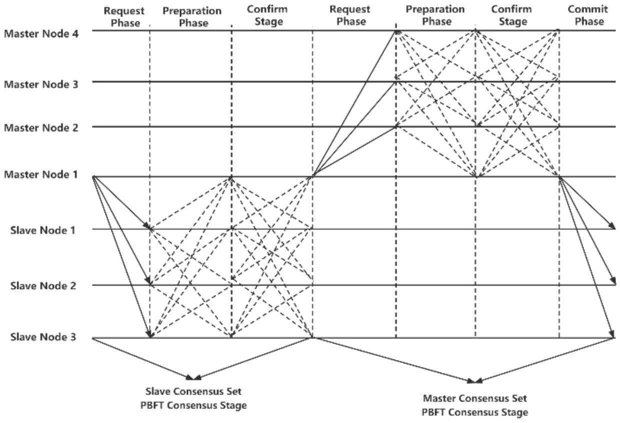

Figure 2 Consensus process of MCDPBFT algorithm

(7) After the global consensus is completed, the master node in each consensus set will package the transaction into a block and broadcast the block to all agent nodes in the respective consensus set. The block format is $< BLOCK, m, v, n, t, i >$. If two or more inconsistent messages are received, or there is no response from a node, go to step 9;

(8) The agent node verifies the block, and all agent nodes write the block to the blockchain in their own consensus set after reaching publicity and then execute step 10;

(9) Start view switch protocol, go to 2;

(10) All nodes in the consensus set send a consistent return

message $< REPLY, m, v, n, t, i, r >$ to the client, and the consensus round ends.

4. Information Traceability Algorithm Based on Searchable Encryption

The composition of the logistics information traceability algorithm based on searchable encryption is shown in Figure 3, which mainly includes the logistics information encryption process and the design of the keyword query algorithm. Through these two algorithms, the effective traceability of logistics information can be realized.

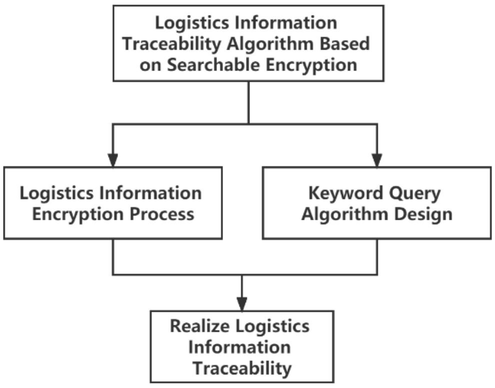
Logistics Information Traceability Algorithm Based on Searchable Encryption
Logistics Information Encryption Process
Keyword Query Algorithm Design
Realize Logistics Information Traceability

Figure 3. Composition of logistics information traceability algorithm based on searchable encryption

The algorithm process designed in this paper includes four entities: file uploader (logistics company), cloud server, blockchain database, and file user (user who queries information). The application process of searchable encryption is shown in Figure 4.

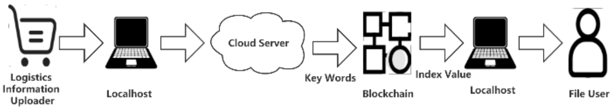

Figure 4. Searchable encryption application process

The searchable encryption steps are as follows:

(1) When logistics information managers use encryption algorithms to encrypt files, they can also use searchable encryption keys to protect keywords so that files can be submitted to the database under double protection.

(2) When the system performs a query in the background for the processing method of the keywords that the user wants to use for traceability, first of all, to ensure that the keywords are not leaked, the system can also perform searchable encryption on the keywords. Then the system will also have The corresponding trapdoors are generated for easy traceability. The trapdoors will keep the keyword information confidential and then communicate it to the database.

(3) In the previous step, a trapdoor for querying data was generated. The blockchain database uses the trapdoor as input to match the trapdoor data in the database. After the successful matching, the trapdoor corresponding to the data can be found. According to the index value, the system can link to the ciphertext file corresponding to the keyword in the cloud server according to the index value. At this time, the system automatically transmits back all the ciphertext files linked by the index value.

(4) The user can immediately receive the ciphertext file and decrypt it with the key pair to view the logistics information he wants to trace.

In this paper, based on the Hyperledger-fabric [3] framework as the blockchain application architecture, Hyperledger Fabric designs an MSP [4] component to manage the nodes on the chain. The identity information of each node on the chain needs to be reported and recorded at the MSP. Based on Certificate Administration (CA), MSP generates, validates, and revokes identity-related certificates. The fabric allows the default interface, either the Fabric CA API or an external CA. The design process of the correlation sub-algorithm is as follows:

(1) $KeyGen$ Algorithm: Given the security parameter γ, the key root algorithm generates the master key K , the asymmetric key pair k_{pr}, k_{pu} and the session key k , where K , (k_{pr}, k_{pu}) , $k_s \in (0,1)^{\gamma}$, and k_s Are shared with the cloud server. See Algorithm1 for the pseudocode of the algorithm.

Algorithm 1 $KeyGen$

```
1: Input：a security parameter $\gamma$
2：KeyGen：
        Generate random keys $K, k_s, (k_{pr}, k_{pu}) \leftarrow \{0,1\}$.
3：Output： Document identifiers $id(D_i)$
```

(2) $SigGen$ Algorithm: Given a public key K_{pu} This algorithm generates a unique signature corresponding to the client with the help of MSP and CA. See Algorithm 2 for the pseudocode of the algorithm.

Algorithm 2 $SigGen$

```
1: Input：a public key $\gamma$
2: $SigGen$：
        Send the public key $k_{pu}$ to the MSP.
        The CA the signature corresponding to the client.
3: Output： Signature ($Sig$)
```

5. MCDPBFT Performance Test

In this section, the MCDPBFT algorithm proposed in this paper is compared with the PBFT algorithm, SPBFT algorithm [4], and COMPBFT algorithm [5] in terms of network bandwidth consumption and network delay. The experimental simulation is carried out through MATLAB R2017a, and the number of nodes is 50, 100, 150, and 200. The experimental conditions are that there are no faulty nodes in the system. In this case, the size of the transmitted data is the same.

(1) Network Bandwidth

Since the block size is constant, the required network bandwidth will increase accordingly as the number of nodes increases. Different algorithms occupy different bandwidths. The changes in network bandwidth and the number of nodes of the four algorithms are shown in the figure below. The PBFT and SPBFT algorithms have three stages of message broadcasting, COMBFT has four sets of broadcasting, and MCDPBFT has only two locations of message broadcasting. Hence, the network is occupied. The bandwidth is smaller than the other three algorithms.

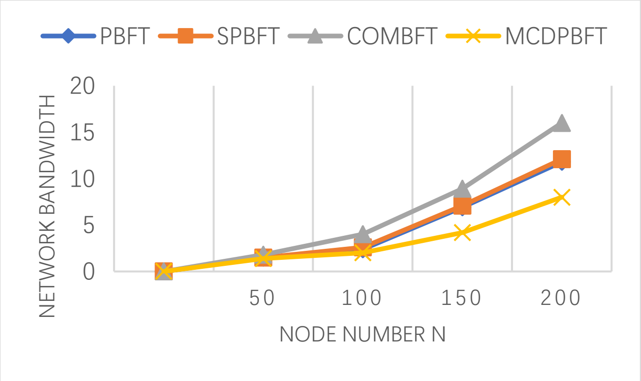

Figure 4. Comparison of Network Bandwidth of Different Algorithms With Different Numbers of Nodes

(2) Network Delay

The network delay is an important indicator reflecting the running speed of the blockchain system. The relationship curve between the network delay and the number of nodes of the four algorithms is shown in the figure below. It can be seen from the figure that with the increase of the number of nodes, the network delay is prolonged to a certain extent, and the network delay of the original PBFT algorithm is relatively low. This paper is low and relatively stable. It also shows that the scheme in this paper is more suitable for systems with a large number of nodes..

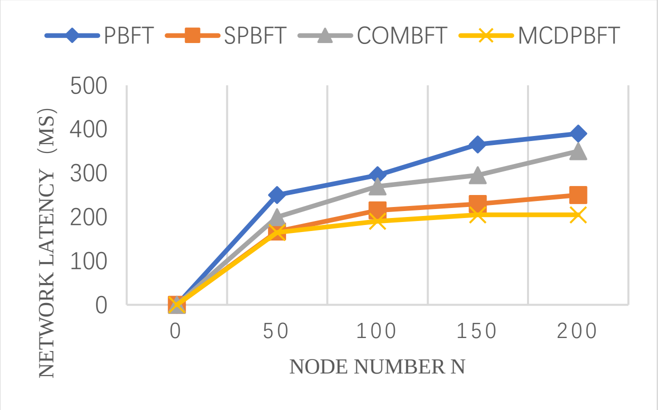

Figure 5. Comparison of Network Delays of Different Algorithms With Different Numbers of Nodes

6. Conclusion

In this paper, first, The relevant theoretical technologies involved in developing the blockchain logistics information traceability system are introduced. According to the characteristics of the logistics industry, a more efficient multi-center dynamic consensus algorithm MCPDBFT is proposed, and the basic model of the algorithm and the overall execution process of the algorithm are described. By analyzing the security and activity of the MCPDBFT algorithm, the feasibility of the algorithm is demonstrated; through the analysis of the number of communications and the fault tolerance rate, it is shown that the algorithm reduces the communication overhead to a certain extent; finally, from the network bandwidth and network delay, two Comparative experiments and simulations are carried out to verify that the algorithm can improve the efficiency of logistics information traceability. According to the characteristics of logistics information, a searchable encryption-based logistics blockchain information traceability algorithm is proposed. Firstly, the searchable encryption is outlined, and the research status is summarized; then, logistics information characteristics are substituted, and the corresponding encryption and query processes are designed in combination with logistics scenarios. Finally, the security and performance of the algorithm are analyzed, and the designed algorithm is proved. It can ensure the authenticity of logistics information and improve the efficiency of logistics information traceability.

7. References

[1] L. Barreto, A. Amaral, T. Pereira, Industry 4.0 implications in logistics: an overview, Procedia Manufacturing, Volume 13, 2017, Pages 1245-1252

[2] M.K.C.S. Wijewickrama, Nicholas Chileshe, Raufdeen Rameezdeen, J. Jorge Ochoa, Information sharing in reverse logistics supply chain of demolition waste: A systematic literature review, Journal of Cleaner Production, Volume 280, Part 1,2021,124359

[3] Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Yellick, J. (2018, April). Hyperledger fabric: a distributed operating system for permissioned blockchains. In Proceedings of the thirteenth EuroSys conference (pp. 1-15).

[4] B. Choi, J. Sohn, D. Han, and J. Moon, Scalable Network-Coded PBFT Consensus Algorithm, 2019 IEEE International Symposium on Information Theory (ISIT), Paris, France, 2019, pp. 857-861.

[5] Y. Rong, W. Wu, and Z. Chen. COMBFT: Conflicting-Order-Match-based Byzantine Fault Tolerance Protocol with High Efficiency and Robustness. In Proceedings of the 48th International Conference on Parallel Processing (ICPP 2019). Association for Computing Machinery, New York, NY, USA, Article 68, 2019, 1–10.