

Received March 23, 2020, accepted March 29, 2020, date of publication April 7, 2020, date of current version April 23, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2986220

Research on Key Technologies of Logistics Information Traceability Model Based on Consortium Chain

XIAOFANG LI¹, FURU LV², FENG XIANG³, ZHE SUN², AND ZHIXIN SUN^{2,4}

¹School of Computer Information Engineering, Changzhou Institute of Technology, Changzhou 213022, China

²Technology Research and Development Center of Postal Industry of State Post Bureau (Technology of Internet of Things), Nanjing University of Posts and Telecommunications, Nanjing 210003, China

³National Engineering Laboratory for Logistics Information Technology, YTO Express Company, Ltd., Shanghai 200000, China

⁴Key Laboratory of Broadband Wireless Communication and Sensor Network Technology of Ministry of Education, Nanjing University of Posts and Telecommunications, Nanjing 210003, China

Corresponding author: Zhixin Sun (sunzx@njupt.edu.cn)

This work was supported by the National Natural Science Foundation of China under Grant 61972208, Grant 61672299, and Grant 61802200.

ABSTRACT In order to trace the logistics information and make use of the characteristics of the Consortium Blockchain, a logistics information traceability model based on the Consortium chain is proposed. The research focuses on two key technologies in the model, namely Multi-center Practical Byzantine Fault Tolerance (MCPBFT) consensus algorithm and Information Matching mechanism. In MCPBFT algorithm, many nodes involved in logistics information are divided into multiple consensus sets, and the consistency protocol is improved into two phases based on PBFT algorithm. In the information matching mechanism, the authenticity of the recorded on-chain information is ensured by matching the updated logistics information with the information stored on the chain in advance. By analyzing the two key technologies, the feasibility and superiority of these two technologies are explained. Among them, MCPBFT algorithm can effectively improve the efficiency of consensus and ensure that the logistics information can be updated in time; the information matching mechanism can be safely applied to the traceability model and improve the practicability of the traceability model.


INDEX TERMS Consortium chain, logistics information, traceability model, MCPBFT consensus algorithm, information matching mechanism.

I. INTRODUCTION

As e-commerce enters the era of rapid development, China's express delivery volume is experiencing an explosive growth trend, the society is becoming more and more informatized, the combination of logistics and the Internet is deepening, forming a huge logistics industry. The rise of a large number of logistics companies has promoted the rapid development of our economy. The informationization of logistics management makes the methods, tools and strategies of logistics management operations change every day. In 2008, Satoshi Nakamoto invented Bitcoin [1], and virtual currencies began to spread around the world. Bitcoin's blockchain technology has attracted widespread attention from scholars at home and abroad for its decentralization, tamper resistance,

and traceability. Blockchain technology can establish a transparent and unified information platform through multiple parties to check in real time to ensure information transmission, and help the logistics industry from the production to transportation of the entire link is fully controllable, traceable, and identifiable. The blockchain can accommodate all users in the logistics service process. In the whole process of information transmission, the logistics block chain is formed by consensus verification through data encryption, so as to ensure the authenticity, transparency, non-tampering and traceability of logistics service transaction information [2].

Blockchain technology effectively solves the pain points of traditional traceability systems by using its distributed storage, encryption algorithms, and time stamps. At present, the types of blockchain can be divided into Public chains, Consortium chains, and Private chains. The Consortium Chain refers to a blockchain network that only allows

The associate editor coordinating the review of this manuscript and approving it for publication was Wenbing Zhao .

members of a specific group and a limited number of third parties to access [3]. Due to the access mechanism of the Consortium Chain and the use of high-performance consensus algorithms, the Consortium chain usually has higher transaction performance than the Public chain, while the demand and background of traceability chain are consistent with Consortium chain, and logistics information chain needs faster speed and lower cost. Therefore, the Consortium chain technology is suitable for the traceability system, so this paper chooses the Consortium chain as the basic network for logistics information traceability.

The problem of consensus is one of the main problems of distributed computing in blockchain. The Practical Byzantine Fault Tolerant (PBFT) [4] consensus algorithm is widely used in the Consortium chain system because of its good fault-tolerant rate and consensus efficiency. Because the number of nodes involved in the logistics information traceability process is very large, the PBFT algorithm has a lower consensus efficiency in the case of larger node sizes. In addition, although the blockchain technology can ensure that the data on the chain cannot be tampered with, it cannot be guaranteed that the data will not be tampered with before it is recorded on the chain, that is, the authenticity of the updated logistics information cannot be guaranteed during the update of the logistics information.

From what has been discussed above, this paper uses the three major characteristics of blockchain technology: decentralization, data cannot be tampered with, and data can be traced to source. This paper proposes a logistics information traceability model based on Consortium chain. The logistics information that wants to trace to the source in this paper means that the seller sends the goods to the buyer by express delivery when shopping online, thereby generating logistics information. First of all, a logistics information traceability architecture is proposed. The architecture is divided into three layers: the basic layer, the core technology layer, and the interaction layer. The key technologies involved in each layer are summarized, and the two key technologies in the architecture are emphatically analyzed. Aiming at the consensus algorithm and the characteristics of the logistics information traceability chain, the PBFT consensus algorithm was improved and the Multi-center Practical Byzantine Fault Tolerance (MCPBFT) consensus algorithm was proposed. The algorithm divides the nodes into multiple consensus sets, each of which has a "center", the consistency protocol in the MCPBFT algorithm was improved to two phases to reduce the number of communications, thereby improving the efficiency of consensus. An information matching mechanism is proposed for the authenticity of logistics information. By matching the updated logistics information with the logistics information that should be stored in the data layer in advance, false information cannot be uploaded.

In addition to the advantages of the decentralization, immutability, and trust of the blockchain, the proposed solution also has the following advantages:

(1) Adopting the Consortium chain instead of the unlimited public chain can maximize the protection of user privacy and corporate secrets on the basis of ensuring decentralized operation.

(2) The adopted MCPBFT algorithm is suitable for the large scale of logistics information nodes in this paper, and can improve the efficiency of consensus and the speed of logistics update.

(3) By proposing an information matching mechanism, logistics information can be prevented from being tampered with before being uploaded.

II. RELATED WORK

Traceability information generally refers to any information describing the production process of a product, including various metadata about entities, data, processing, activities, etc. in the production process [5]. In order to ensure that the origin of the goods is regular, it can be verified by querying the logistics information. However, the logistics information can be easily tampered with and forged. In recent years, many scholars have begun to study the "traceability mechanism", especially in the supply chain traceability including agricultural products and food traceability. In [6], A complete meat food traceability system was designed using RFID technology. By affixing RFID tags to each newborn animal, the entire process monitoring from source, circulation and sales was realized. However, the content in RFID tags is easily tampered with, and in modern logistics information networks, the traceability process is time-consuming and complex. The advent of blockchain technology has made the need for information tracing more and more satisfied. In [7], A supply chain information platform is built based on blockchain technology. Blockchain technology can make the entire supply chain transparent, and does not require a centralized organization, and does not need to trust institutions in advance. This enables subsequent traceability information to be true and effective. In [8], [9], It is the combination of blockchain and the Internet of Things to achieve data traceability. In [10], [11], Combining RFID technology with blockchain technology effectively utilizes the advantages of blockchain technology's immutability, data sharing, RFID technology's high security, and anti-copying advantages. Establish a blockchain ledger in the production, processing, and sales of RFID traceable items. In [12], A food traceability system based on the blockchain is designed to store the data of food manufacturing and transportation in the blockchain, but the capacity of the system is limited and cannot store a large amount of data.

Because most of the consensus mechanisms and smart contracts in the blockchain are developed for cryptocurrencies, not for information traceability. Therefore, in order to apply to the logistics information platform, the technology in the blockchain needs to be improved. In [13], Ethereum blockchain and smart contracts are used to effectively execute commercial transactions to track and trace soybeans throughout the agricultural supply chain., the proposal focuses on

using smart contracts to manage and control transactions between all participants in all interactive supply chain ecosystems. In [14], A food safety traceability system based on blockchain and EPC information services was proposed, and a prototype system was developed. An on-chain and off-chain data management architecture is proposed. Through this architecture, the traceability system can alleviate the data explosion problem of the IoT blockchain. In [15], In order to prevent drug counterfeiting, the blockchain technology is applied to drug traceability, and a traceability framework is proposed, starting from the production of the drug and including the formula for full traceability. In [16], [17], Based on the blockchain, a food traceability system is proposed to query the source of food and the manufacturing process. Consumers can query all participants involved in food manufacturing and transportation. In [18], Trustchain was proposed on the basis of the paper [17]. In order to prevent information from being tampered with before being uploaded, a three-tier architecture was defined to “monitor” key institutions and personnel involved in the food chain, and proposed a reward and punishment mechanism to ensure information Authenticity. In [19], A traceability model in the permission chain is defined and the traceability of the model is proved by the zero-knowledge proof method. However, this model does not take into account the problem of information authenticity. In [20], A kind of anti-counterfeiting traceability system using public chain and private chain double block chain is proposed. This traceability system can ensure the authenticity and reliability of the obtained traceability information and cannot be tampered with. It also solves the problem of product label duplication, spam and product quality in traditional product traceability systems. The problem-related responsible person and the problem link are difficult to locate.

As for the key technologies involved in the “traceability mechanism”, consensus algorithm is also a research hotspot. Different system functions have different requirements. This requires a suitable consensus algorithm to achieve good results. BFT algorithms are currently widely used. In [21], A resource efficient Byzantine fault tolerance (REBFT) mechanism is proposed. This method keeps the replicas in passive mode, thereby reducing the resource usage of the BFT system under normal circumstances and improving system flexibility. In [22], The Honey Badger of BFT [23] algorithm is improved, and a BEAT protocol with higher consensus efficiency is proposed. As the scope of application of the PBFT protocol is limited to models such as client-server nodes, In [24], an Aegen model is proposed, which can implement fault-tolerant protocols outside the scope of the client-server model, and considers the existence of interactions between services In this case, the correctness of the system can be ensured.

The current improved algorithms for PBFT take into account a variety of situations in the actual scene. These improved methods have improved the consensus efficiency of the PBFT algorithm to a certain extent. However, these improved algorithms are still not applicable to the case of

large node size such as transportation of goods, and the communication time is still very high. Therefore, this paper proposes MCPBFT consensus algorithm based on the improvement of PBFT algorithm. In addition, in view of the authenticity of information recorded on the chain, this paper was inspired by the paper [17], [18] to propose an information matching mechanism to prevent criminals from updating the wrong logistics information to the blockchain.

III. MODEL DESCRIPTION

A. MODEL ARCHITECTURE

The model in this paper uses an architecture based on the Consortium chain. Throughout the model, all technologies are used to achieve the purpose that users can quickly and accurately trace information. The architecture diagram is shown in Figure 1. The overall architecture is divided into three parts from bottom to top: the first layer is the bottom layer, which is composed of the infrastructure layer and the data layer; The second layer is the core technology layer, which is composed of network layer, consensus layer and contract layer. The third layer is mainly the interaction layer, in which the participants of each link interact with the logistics information traceability platform.

1) BASIC LAYER

The infrastructure layer collects basic data generated by various links of logistics activities through RFID, barcode and other data collection equipment. Basic data includes logistics information, goods, storage, etc. It also includes some information from third-party logistics companies. After uploading basic data to the data layer through the transmission mechanism, it is asymmetrically encrypted and time stamped to generate data blocks, which are then linked to the blockchain.

2) CORE TECHNOLOGY LAYER

The network layer propagates and stores data blocks to each node through specific network transmission protocols and authentication mechanisms, and allows authenticated nodes to participate in the consensus and recording of data blocks. Among them, consensus algorithms and smart contracts are the key technologies of the blockchain.

3) INTERACTION LAYER

The application layer is mainly an application scenario of the logistics service information traceability chain, an interface for members of the traceability chain to conduct business operations, and a carrier of information interaction.

This paper assumes that each participating subject in the architecture is a trusted subject certified by the Trusted Certificate Authority (CA). The subjects of the traceability model include:

(1) System user. It can be a consignor, a logistics carrier (acquisition party), a transit station (a transit consignor), a person in charge of the cargo storage office, a consignee, etc. Each system user has a unique identifier.

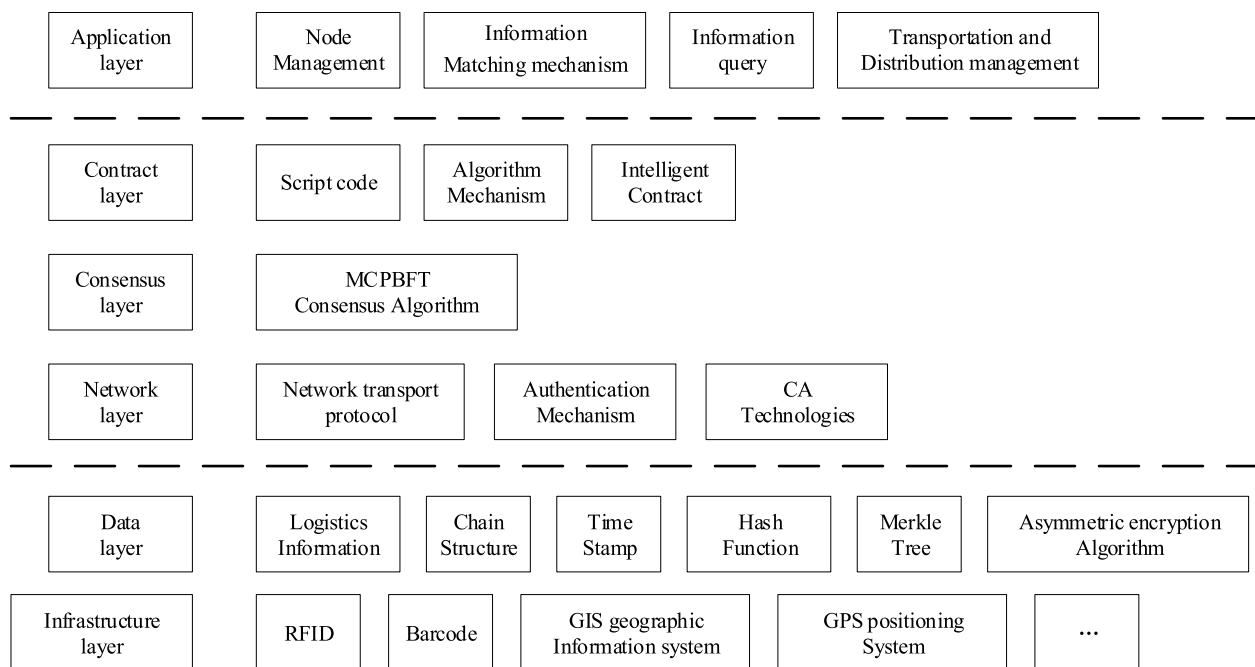


FIGURE 1. Architecture of logistics information traceability model based on Consortium chain.

(2) Data platform. Provide big data storage and transaction services, and store copyright information and historical transaction records in the blockchain.

(3) Key Center. Generate unique signatures for users and assign public and private keys.

(4) Blockchain network. It is composed of various verification nodes and is responsible for storing copyright information and data transaction records. The transaction information on the chain must be subjected to attribute encryption verification processing.

Assuming that each logistics company has its own complete blockchain, the model described in this article is a company's complete blockchain traceability system.

B. MCPBFT

MCPBFT is a multi-center consensus algorithm. This consensus algorithm is based on the PBFT consensus algorithm.

In MCPBFT, nodes are divided into multiple parts, and each part is called a consensus set. Each consensus set has a primary node and the remaining nodes called replicas. The distribution of nodes is shown in Figure 2. In this paper, each cargo is taken as the primary node, and the entities related to the cargo such as the consigner, the contractor, the carrier of the transit station, the person in charge of the storage office, and the consignee are the replicas. The primary and the replicas form a consensus set. Assuming that each consensus set has the same number of nodes, each consensus set has its own chain and stores the logistics information of this consensus set. After the information is reached in the consensus set, it will eventually enter the global consensus, that is, the same batch of goods (primary node) will start global consensus. At this time, the information matching mechanism will be

started (described in section C). The global consensus set is composed of the primary in each consensus set. After the updated information is consistent with the global consensus, the system considers that the logistics information is complete and the logistics information of the goods is true and correct.

(1) Let the number of consensus sets in the system be K , represent each Consensus Set as CS_i , then $CS_i \in \{CS_1, CS_2, \dots, CS_K\}$.

(2) Represent all primary nodes in the sets as N_P , $N_P = K$, replicas are represented as N_R , then the total number of nodes N in the sets is:

$$N = N_P + N_R \tag{1}$$

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

$$N \geq \frac{(3f + 1)}{K} \tag{2}$$

(4) This paper uses the 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, that is, entities participating in logistics transportation, must register identity information in the MSP, such as node ID, phone, etc.

(b) Suppose the node wants to join the system, first register in the MSP, and then join the system after passing the MSP audit. Suppose node wants to quit the system, apply to the MSP, and the MSP agrees to quit.

In the Consortium chain, consensus nodes usually do not fail, and Byzantine nodes usually appear when the network is down and communication is disconnected. In this era of

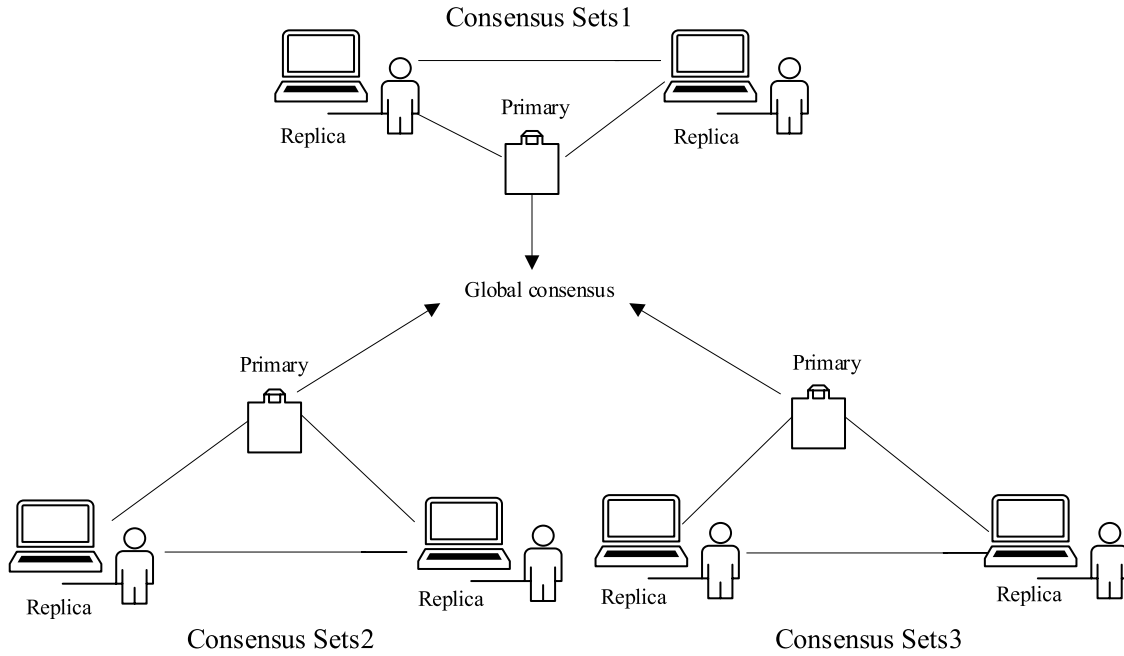


FIGURE 2. Schematic diagram of node division.

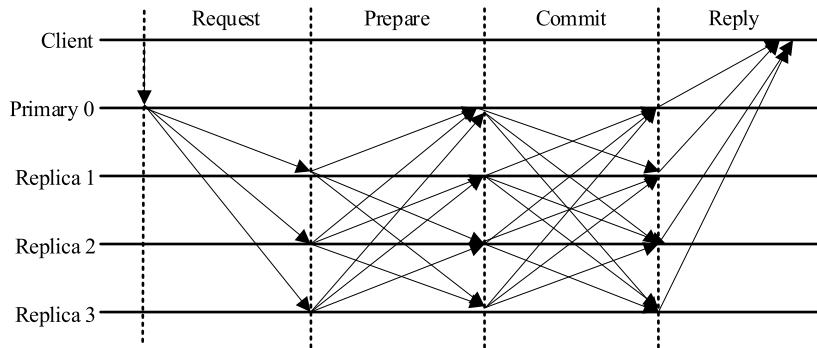


FIGURE 3. Two phases of the consistency protocol.

increasingly developed networks, these situations generally do not occur. Therefore, in order to reduce the number of communications, the three-phase broadcast consensus of the consistency protocol in the PBFT algorithm is improved to two phases, and the pre-preparation phase is removed. Figure 3 is a process diagram of the two phases of a consistency protocol within a consensus set.

(1) Prepare phase: After the primary receives the request message (the cargo receives the logistics update information), it immediately assigns a serial number f to the request, and then broadcasts the message to the replica, and the replica sends the preparation message $\langle PREPARE, m, v, n, t, i \rangle$ to all replicas. Among them, m is the summary of the message, v is the number of the current view, t is the time stamp of the request n , and i is the node number.

(2) Commit phase: When the replicas verifies that the message is true, it will broadcast a confirmation message $\langle COMMIT, m, v, n, t, i \rangle$ to other nodes.

(3) After verifying the confirmation message, the replicas can perform the operation and return the result to the client. The format of the result is $\langle REPLY, m, v, n, t, i, r \rangle$, where r is the result of the returned message. For example, the updated logistics information is consistent with the information stored in the data layer, the result of r is *TRUE*.

C. INFORMATION MATCHING MECHANISM

We can use the non-tampering of the blockchain to ensure that the information is not maliciously tampered with, but there is a point that must be paid attention to: we cannot guarantee the authenticity of the information recorded on the chain, that is, the information registered on the chain may be false. In other words, the logistics information we query may have been tampered with before being recorded on the blockchain. Therefore, in order to avoid this situation, an information matching mechanism is proposed for the logistics information source tracing scheme in this paper. Firstly, the route that

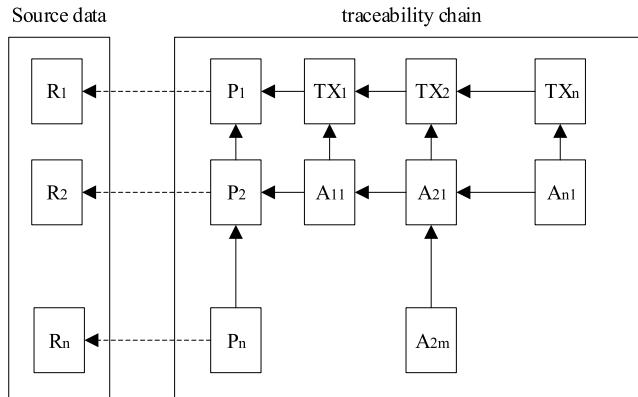


FIGURE 4. Traceability chain.

each cargo should take, that is, the predetermined logistics information, is recorded in the block chain data layer. When the cargo is sent out, the logistics information is updated on the chain in real time. If the updated logistics information does not match the corresponding information uploaded to the data layer in advance, an error warning is issued. The specific implementation method is as follows:

The information block R_i of each piece of goods in this article has a unique corresponding block P_i in the Consortium chain. During the logistics update process, this model encrypts the information of each piece of goods to be chained to form a ciphertext structure $CT = \{C, C_\delta, (C_i, D_i)_{i \in [1, 2, \dots, l]}\}$ (l represents the number of goods), all consensus nodes complete the information chaining, query and dynamic update through the process shown in Figure 4.

When goods need to be sent out, the consignor (logistics company’s consignee) first creates the logistics chain of the goods, which is marked as TX_{cr} , and the content of TX_{cr} is as follows:

$$TX_{cr} = [CID | CT_{data} | ID_o | Log_{contract} | Sig_o | PU_o] \quad (3)$$

Among them, CID is the tag of the goods, CT_{data} is the ciphertext structure data of the goods, similar to the hash value. ID_o is the identifier of the person in charge of the goods, $Log_{contract}$ is the interface used to connect to the predetermined logistics information stored in the blockchain data layer in advance, Sig_o and PU_o is the signature and public key of the acquirer.

When the goods arrive at the transit station, the goods are transferred to the transit party, and the information in the logistics chain TX_{cr} changes, which is recorded as TX_{tr} :

$$TX_{tr} = [CID | CT_{data} | ID_o | Sig_o | PU_o | Sig_s | PU_s] \quad (4)$$

Among them, CID , CT_{data} and ID_o are the same as those defined in TX_{cr} . In addition to the signature Sig_o and public key PU_o of the acquirer, the signature Sig_s and public key PU_s of the transfer station need to be added in TX_{tr} . If there are multiple transit stations, the signature and public key corresponding to each transit station are added in turn.

When the logistics information at the transit station needs to be updated, the consensus node first generates an information block TX with (C, C_δ) , and generates a block A with $(C_i, D_i)_{i \in [1, 2, \dots, l]}$ to get a new logistics information block group $\{TX, A\}$; Then find the last information block group $\{TX_j, A_j\}$ of the information chain P_i according R_i , append $\{TX, A\}$ to the chain to form a new information record $\{TX_{j+1}, A_{j+1}\}$. When the updated logistics information is uploaded to the blockchain, the smart contract is immediately started to match the logistics information stored in the chain in advance, that is, the logistics chain information is verified by the consensus node. If the verification is consistent, the blockchain does not react. In addition, the identity of the person who updates the information needs to be verified to determine whether the identity of the updater is authentic. This operation can ensure the security of the goods and prevent the goods from being “taken” by malicious people. Then, by judging whether the equation $C_\delta = C'_\delta$ is valid, it can be used to determine whether the updator has the right to update the cargo information and whether the Shared key s used before and after the update is consistent. Finally, the information block A' generated by $(C'_i, D'_i)_{i \in [1, 2, \dots, l]}$ is added to the last information block of TX , the block group $\{TX, A'\}$ containing the updated logistics information is obtained to complete the logistics update.

After the transit is completed, the goods are sent to the cargo storage place, such as Cainiao Post Station, so the information in the logistics chain TX_{tr} changes and is marked as TX_{ar} :

$$TX_{ar} = [CID | CT_{data} | ID_o | Sig_o | PU_o \times | Sig_s | PU_s | Sig_b | PU_b | GI_{tx}] \quad (5)$$

Among them, the newly added information Sig_b and PU_b are the signature and public key of the person in charge of the cargo storage office, and GI_{tx} is the pickup information of the cargo.

When the consignee picks up the goods at the cargo storage place, the logistics chain enters the last link, and the logistics information will be finally updated, recorded as TX_{vr} :

$$TX_{vr} = [CID | CT_{data} | ID_o | Sig_o | PU_o | Sig_s \times | PU_s | Sig_b | PU_b | GI_{tx} | Sig_d | PU_d] \quad (6)$$

It can be seen from the above formula that the consignee’s signature Sig_d and public key PU_d are finally recorded in the logistics chain. This pickup process also prevents the goods from being picked up by mistake.

During the traceability information query process, the consensus node obtains the logistics information from TX , and obtains the corresponding updated information $(C_i, D_i)_{i \in [1, 2, \dots, l]}$ from the last information block A corresponding to TX . The complete ciphertext $CT = \{C, C_\delta, (C_i, D_i)_{i \in [1, 2, \dots, l]}\}$ of the information record formed by $\{TX, A\}$ is returned to the source-tracking user, and the user decrypts CT to obtain the logistics information through the attribute private key.

IV. ANALYSIS AND PROOF OF KEY TECHNOLOGIES

This section analyzes and proves two key technologies. It analyzes the MCPBFT algorithm from three aspects: security, communication times, and fault tolerance. The information matching mechanism is mainly analyzed from the aspect of liveness.

A. SECURITY ANALYSIS OF MCPBFT

First of all, the security of MCPBFT algorithm is analyzed. For the sake of proof, this paper assumes that the total number of nodes in the system is $N = 3f + 1$, and no-fault nodes are called benign nodes.

Theorem 1: There are at least $\frac{(2f+1)}{K}$ benign nodes in each round of consensus of each consensus set, so the consensus result of each consensus set CS_i is valid.

Proof: The consensus nodes of each round of the consensus set CS_i are divided into K consensus sets from the $3f + 1$ nodes in the system to synchronize the consensus. Byzantine theorem, there are fault nodes in the system, then there are f benign nodes in the system, that is, each The number of benign nodes in the consensus set is $2f + 1$. Because there are at most $\frac{f}{K}$ fault nodes in K consensus set, each round of consensus in the consensus set is valid.

Theorem 2: In this paper, there is no cross-problem between each consensus set and there is no cross-problem between the global consensus set and the remaining consensus sets.

Proof: $\frac{N}{K}$ nodes in each consensus set use the MCPBFT algorithm to reach consensus on logistics information, and each consensus set synchronizes consensus to achieve the purpose of improving consensus efficiency. The primary of each consensus set records the node number in its own consensus set. Each primary only broadcasts messages to the replicas in its own consensus set, so there is no crossover problem in the transactions of each consensus set. The global consensus set also uses MCPBFT algorithm to make the final consensus on the logistics information and build the block. Once the final consensus is reached, a block is generated and added to the chain. Because the global consensus set is composed of all the primary nodes, and the global consensus set is the final consensus on the current information, there is no crossover problem between the global consensus set and the rest of the consensus set.

B. ANALYSIS OF COMMUNICATION TIMES OF MCPBFT

This section will analyze the communication times of the classic PBFT algorithm and MCPBFT algorithm in the consensus process to verify that the communication times of the MCPBFT algorithm is less than the classic PBFT consensus algorithm.

Since the MCPBFT algorithm needs to divide the nodes in the system into K consensus sets, it is assumed that the number of nodes in each replica consensus set is the same, and the number of nodes in each replica consensus set and the primary consensus set should be no less than 3.

Therefore, the number of consensus sets should be no less than 3, so this paper assumes that the number of nodes in the system is N ($N \geq 9$).

There are three phases in the PBFT that need to send messages for communication. First, the client sends the request to the primary, and the primary sends the request (pre-prepared message) to all the replicas, so the number of communications in the pre-prepared phase is $(N - 1)$. Then enter the prepared phase. After receiving the pre-prepared message from the primary, the replicas verifies the message and sends the prepared message to the primary and other replicas. The number of communications in this phase is $(N - 1)^2$. Finally, it enters the committed phase. All nodes verify the received prepared message. When the verification results of all nodes are consistent, the committed message is sent to all other nodes. The number of communications in this phase is $N(N - 1)$. Adding the communication times of the above three phases to get $(N - 1) + (N - 1)^2 + N(N - 1)$, simplifying can get the classical PBFT algorithm to complete a consensus communication times T_1 is:

$$T_1 = 2N(N - 1) \quad (7)$$

In the MCPBFT, there are two phases in each consensus set that need to send messages for communication, and each replicas consensus set has $\frac{N}{K}$ nodes. The number of communications in the prepared phase is $(\frac{N}{K} - 1)$, and the number of communications in the committed phase is $\frac{N}{K}(\frac{N}{K} - 1)$. Since there are a total of replicas consensus sets that need to communicate, the number of communications T_2 in the MCPBFT is:

$$T_2 = \left(\frac{N}{K} + 1\right)(N - K) \quad (8)$$

Because when $N \geq 9$, there is $T_2 < T_1$, so the communication times of this scheme are less.

C. ANALYSIS OF FAULT TOLERANCE RATE OF MCPBFT

This section compares the fault tolerance rates of the MCPBFT and the PBFT. The maximum number of error nodes f_1 that the system can tolerate is:

$$f_1 = \frac{(N - 1)}{3} \quad (9)$$

In MCPBFT, the number of error nodes f_2 that the system can tolerate is obtained by formula (2):

$$f_2 = \frac{(N \cdot K - 1)}{3} \quad (10)$$

Since K is the number of consensus sets, the result of $N \cdot K$ is greater than N , that is, $f_2 > f_1$. Therefore, the fault tolerance rate of the MCPBFT algorithm proposed in this paper is higher than that of the PBFT algorithm.

D. LIVENESS ANALYSIS OF INFORMATION MATCHING MECHANISM

Liveness means that a certain system or mechanism, algorithm, etc. can be continuously carried out without being

stuck due to various faults. The liveness of the information matching mechanism means that the mechanism can be effectively continued, Cargo traceability data is guaranteed to be accurate..

(1) First, when a logistics company collects the goods, it prints the shipping order and creates the logistics chain TX_{cr} of the goods. It is connected through the $Log_{contract}$ and the logistics information stored in the data layer. The label on the shipping order is the unique physical identifier of the goods.

(2) After TX_{cr} is successfully created, it will be automatically submitted to the chain. In addition to recording some necessary information, the most important thing is the information matching process and results. If the information matches, the goods can continue to be transported normally. If there is a problem with the matching, an alert is generated and the logistics of this cargo is suspended, at which time the background staff needs to investigate.

(3) After receiving the goods, the consignee can scan the label or APP to view the detailed logistics information.

Since the transit logistics information of the goods are recorded in the blockchain, product tracing can be performed directly by querying the blockchain transactions. Assuming the current cargo P_j is located at a transit station x , according to the information matching mechanism described above, the traceability process of the cargo is:

```

transaction trans = Sigx → SigN1&SigN2&...
//Ni is the signature of the subsequent entity
while trans.input is not None
//Query preorder transactions
while Cδ = C'δ
//Determine if the information matches,
currently hypothetical match
trans = lastTransaction (Sigx → SigN1&SigN2&...)
//Output traceability information
print extravtPubKey(trans.input)
print trans.time

```

In the process of obtaining the traceability information m , in order to ensure the traceability efficiency and the accuracy of the traceability results, the results need to be decrypted in the blockchain to obtain m . According to $Decrypt(CT, SK) \rightarrow m$, enter the ciphertext $CT = \{C, C_\delta, (C_i, D_i)_{i \in [1, 2, \dots, l]}\}$ and the private key SK of the user attribute set S in the decryption algorithm, and set the index set to $I = \{i : \rho(i) \in S\}$, then the decryption calculation formula is:

$$\frac{e(C_\delta, K)}{\prod_{i \in I} (e(C_i, L) e(D_i, K_{\rho(i)}))} = \frac{e(g, g)^{as\delta} e(g, g)^{\delta\beta t}}{\prod_{i \in I} e(g, g)^{\delta\beta t \lambda_i}} = e(g, g)^{as\delta} \quad (11)$$

Finally get the ciphertext information $m = \frac{C}{e(g, g)^{as\delta}}$.

The above process can ensure the liveness of the logistics information traceability mechanism.

The fourth section analyzes and proves the MCPBFT consensus algorithm and information matching mechanism.

The problems that need to be considered in the MCPBFT algorithm are guaranteed by the theorem and proof. The MCPBFT divides the system nodes into multiple consensus sets for synchronous consensus, which reduces the consensus time to a certain extent and improves the efficiency of the consensus, Especially when the scale of nodes in this system is large, the performance of the model can be effectively improved. The theoretical analysis of the matching mechanism of logistics information is carried out from the aspect of liveness to ensure that the mechanism can be successfully applied to the logistics information traceability model.

V. CONCLUSION

Aiming at the problem that the current logistics information may be falsely updated, combined with the advantages and characteristics of the Consortium chain technology, a logistics source tracing model based on the Consortium chain is proposed. This model provides a new method for logistics information that cannot upload false information and that cannot be tampered with after being recorded on the chain. Detailed analysis of two key technologies in the model, the first is to propose the MCPBFT algorithm. This paper describes the algorithm's consensus process and how to apply it to the logistics information traceability model. The analysis shows that the algorithm reduces the number of communications to a certain extent and improves the efficiency of the consensus; the second is to propose an information matching mechanism. The main idea of the mechanism is explained. The liveness analysis is performed to ensure that the mechanism can effectively and continuously verify the updated information to ensure the authenticity of the logistics information. The next research direction is to research and improve other key technologies in the model to design a better logistics information traceability model.

REFERENCES

- [1] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
- [2] Q.-F. Shao, C.-Q. Jin, Z. Zhang, W.-N. Qian, and A. Zhou "Blockchain: Architecture and research progress," *Chin. J. Comput.*, vol. 41, no. 5, pp. 969–988, 2018.
- [3] Y. Yuan, X. Ni, S. Zeng, and F. Wang, "Blockchain consensus algorithms: The state of the art and future trends," *Acta Automat. Sinica*, vol. 44, no. 11, pp. 2011–2022, 2008.
- [4] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. Symp. Oper. Syst. Des. Implement.*, Feb. 1999, pp. 173–186.
- [5] Y. Minghe, N. Tiezheng, and L. Guoliang, "Data curation technologies and applications," *Big Data Res.*, vol. 5, no. 6, pp. 1–17, 2019.
- [6] Z. Yiying, R. Yuanlong, L. Fei, S. Jing, and L. Song, "Research on meat food traceability system based on RFID technology," in *Proc. IEEE 3rd Inf. Technol., Netw., Electron. Automat. Control Conf. (ITNEC)*, Chengdu, China, Mar. 2019, pp. 2172–2175.
- [7] Y. Cui and H. Idota, "Improving supply chain resilience with establishing a decentralized information sharing mechanism," in *Proc. 5th Multidisciplinary Int. Social Netw. Conf. (MISNC)*, New York, NY, USA, 2018, pp. 1–7.
- [8] Y. P. Tsang, K. L. Choy, C. H. Wu, G. T. S. Ho, and H. Y. Lam, "Blockchain-driven IoT for food traceability with an integrated consensus mechanism," *IEEE Access*, vol. 7, pp. 129000–129017, 2019.

- [9] Q. Rui, C. Yan, and W. Qingxian, "Traceability mechanism of dynamic data in Internet of Things based on consortium blockchain," *J. Softw.*, vol. 30, no. 06, pp. 1614–1631, 2019.
- [10] W. Yu and S. Huang, "Traceability of food safety based on block chain and RFID technology," in *Proc. 11th Int. Symp. Comput. Intell. Design (ISCID)*, Hangzhou, China, Dec. 2018, pp. 339–342.
- [11] Y. Liu and Y. Liu, "Security provenance model for RFID big data based on blockchain," *Comput. Sci.*, vol. 45, no. S2, pp. 367–368 and 381, 2018.
- [12] H. Hayati and I. G. B. B. Nugraha, "Blockchain based traceability system in food supply chain," in *Proc. Int. Seminar Res. Inf. Technol. Intell. Syst. (ISRITI)*, Yogyakarta, Indonesia, Nov. 2018, pp. 120–125.
- [13] K. Salah, N. Nizamuddin, R. Jayaraman, and M. Omar, "Blockchain-based soybean traceability in agricultural supply chain," *IEEE Access*, vol. 7, pp. 73295–73305, 2019.
- [14] Q. Lin, H. Wang, X. Pei, and J. Wang, "Food safety traceability system based on blockchain and EPCIS," *IEEE Access*, vol. 7, pp. 20698–20707, 2019.
- [15] R. Kumar and R. Tripathi, "Traceability of counterfeit medicine supply chain through blockchain," in *Proc. 11th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Bengaluru, India, Jan. 2019, pp. 568–570.
- [16] G. Baralla, A. Pinna, and G. Corrias, "Ensure traceability in European food supply chain by using a blockchain system," in *Proc. IEEE/ACM 2nd Int. Workshop Emerg. Trends Softw. Eng. Blockchain (WETSEB)*, Montreal, QC, Canada, May 2019, pp. 40–47.
- [17] S. Malik, S. S. Kanhere, and R. Jurdak, "ProductChain: Scalable blockchain framework to support provenance in supply chains," in *Proc. IEEE 17th Int. Symp. Netw. Comput. Appl. (NCA)*, Cambridge, MA, USA, Nov. 2018, pp. 1–10.
- [18] S. Malik, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "TrustChain: Trust management in blockchain and IoT supported supply chains," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Atlanta, GA, USA, Jul. 2019, pp. 184–193.
- [19] T. Mitani and A. Otsuka, "Traceability in permissioned blockchain," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Atlanta, GA, USA, 2019, pp. 286–293.
- [20] L. Jiaji, Y. Ting, and W. Wenyong, "Traceability system using public and private blockchain," *J. Cyber Secur.*, vol. 3, no. 3, pp. 17–29, 2018.
- [21] T. Distler, C. Cachin, and R. Kapitza, "Resource-efficient byzantine fault tolerance," *IEEE Trans. Comput.*, vol. 65, no. 9, pp. 2807–2819, Sep. 2016.
- [22] S. S. Duan, M. Reiter, and H. B. Zhang, "BEAT: Asynchronous BFT made practical," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, 2018, pp. 2028–2041.
- [23] A. Miller, Y. Xia, K. Croman, E. Shi, and D. Song, "The honey badger of BFT protocols," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, 2016, pp. 31–42.
- [24] R. C. Aksoy and M. Kapritsos, "Aegean: Replication beyond the client-server model," in *Proc. 27th ACM Symp. Oper. Syst. Princ. (SOSP)*, New York, NY, USA, 2019, pp. 385–398.



XIAOFANG LI received the B.Sc. degree in computer science and technology, the M.Sc. degree in power system automation, and the Ph.D. degree in hydro informatics from Hohai University, in 1995, 2004, and 2011, respectively. She is currently a Professor with the Changzhou Institute of Technology, Changzhou, China. Her research areas include information acquisition, wireless sensor networks, and blockchain. She is a Senior Member of the China Computer Federation.



FURU LV was born in Jiangsu, China. She is currently pursuing the master's degree with the College of Modern Posts and Institute of Modern Posts, Nanjing University of Posts and Telecommunications. Her current research interest is blockchain technology and its applications.



FENG XIANG received the B.A. degree from the Nanjing University and Master of Public Administration, and the JFK School of Government, Harvard University. He is currently the CEO of YTO Express Company, Ltd., and the Director of the National Engineering Laboratory of Information Technology in Logistics. His research interests include logistics engineering and strategic management of business.



ZHE SUN received the Ph.D. degree from Zhejiang University, in 2015. He is currently working at the Nanjing University of Posts and Telecommunications. His research interests include evolution computation, differential evolution algorithm, fuzzy logic systems, neural networks, and blockchain.



ZHIXIN SUN was born in Xuancheng, China, in 1964. He received the Ph.D. degree from the Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 1998. From 2001 to 2002, he held a postdoctoral position at the School of Engineering, Seoul National University, South Korea. He is currently a Professor and the Dean of the School of Modern Posts, Nanjing University of Posts and Telecommunications. His research interests are in cloud computing, traffic identification, and blockchain.

...