PTLchain: Privacy and Traceability Enhanced Scheme for Logistics by using Consortium Blockchain

Xiaoguo LIN[1], Xunbing Wang[1]
[1]School of computer science and communication engineering, Jiangsu University, Zhenjiang, Jiangsu ,212013, China

In digital intelligence era, the authenticity , privacy and traceability of data are key factors in building a good logistics information system. However, current logistics system does not pay attention to protecting user's privacy information, once the user's privacy is leaked, it will seriously damage the interests of the user. Besides, when there is a logistics dispute, the logistics system cannot ensure the credibility of the traceable process, which reduces the security and availability of the system. Compared with the traditional logistics system, the blockchain-based logistics scheme ensures the security of users' personal privacy, the authenticity and traceability of logistics information to a certain extent. However, most of the existing blockchain-based privacy-preserving logistics schemes only propose corresponding system models, which cannot be directly applied. Therefore, to address the leaking problems of logistics information in today's logistics system and inefficiency in tracing the logistics delivery process, we propose a privacy and traceability enhanced scheme for logistics based on consortium blockchain. The blockchain guarantees the authenticity of logistics data through tamper-resistance and traceability, it avoids logistics information and transportation process tampering and supports efficient logistics traceability. Furthermore, we utilize asymmetric encryption and attribute-based encryption to encrypt users' privacy and logistics information, to protect the private information and realize fine-grained access control. Finally, we implement the prototype system by Hyperledger Fabric platform, and give the performance evaluation to verify the feasibility and practical significance of our scheme.

Index Terms—**Consortium blockchain, Logistics scheme, CP-ABE, Privacy-preserving, Traceability**

I. Introduction

The rapid development of logistics industry has brought great convenience to people's life and greatly improved people's living conditions. However, the expansion of the scale of the logistics industry has brought many security problems, especially the security of user's privacy and logistics information in the logistics process. For example, logistics data is stored in a third-party logistics company, which is easy to be tampered with and illegally stolen by logistics staffs, or during the delivery process of the package, the user's personal privacy and logistics information are presented in plaintext, and anyone can obtain a large amount of logistics information. Therefore, a good logistics information system must ensure the privacy of users and the security of logistics information, and realize the effective tracing of logistics information on the basis of ensuring the privacy and security of logistics information.

The realization of privacy preservation in the logistics system is still an urgent problem to be solved. The existing logistics privacy-preserving schemes have the following shortcomings: 1) Logistics data is stored in a centralized system and is vulnerable to tampering by illegal users; 2) There is no effective solution to protect the user's personal privacy and logistics information; 3) When a logistics dispute occurs, the logistics information cannot be traced effectively; 4) The sender can deny sending a package, and the receiver can deny accepting a package.

At present, most logistics companies have their own logistics systems, although some existing logistics systems preserve the privacy, most of them either are centralized storage of logistics information or do not support fine-grained access control. Centralized storage is easily attacked by illegal users, resulting in the leakage of user privacy information and logistics information. Secondly, users' privacy and logistics information are stored in untrusted third-party logistics companies, data owners cannot control their own information, logistics staff can tamper and steal users' personal privacy to carry out illegal activities, making users' privacy information accessible not guaranteed. Furthermore, under the current logistics system, the sender is required to disclose a significant quantity of personal privacy and logistics information in order for logistics companies to enable transmitting, transporting, and receiving. For example, when sending a package, users are required to fill in personal information such as their name, telephone number and address on the logistics delivery form. The logistics privacy information mentioned above is presented in plaintext, which is easily resulting in leaking privacy information or be used by illegal users, thus this will bring great disadvantages to users and damage the interests of users. Already, certain solutions exist to secure logistics privacy data directly through technical means, such as keeping customers' personal privacy and logistical information in a QR code. However, due to the QR code data remains in plaintext, the issue of privacy information leakage has not been resolved properly. Additionally, when a logistics dispute occurs or a package is lost or damaged, the logistics data is centrally stored in the logistics company, and the user cannot reliably trace the logistics data, resulting in the user's interests not being guarantee. Also, the sender can deny having sent an illegal package, the receiver can deny receiving a package,which reduces the security and availability of the system.

Manuscript received Nov 5, 2021; revised Jan 21, 2022. Corresponding author: Xiaoguo LIN (email: GuoCheng1016@gmail.com). Portions of this work were presented at the Nerwork and Network Application in 2021, TPLI:A Traceable Privacy-preserving Logistics Information Scheme via Blockchain.

In recent years, blockchain technology has attracted wide attention worldwide. As a key underlying technology, blockchain is one of the important supports of component logistics system, it guarantees the authenticity of logistics data through tamper resistance and traceability. Many researchers at home and abroad are committed to the integration of blockchain technology into the logistics supply chain industry. The combination of blockchain technology with the logistics supply chain industry has gradually become the standard of the industry. The application of blockchain technology to the logistics industry can effectively solve the problem of data traceability in the logistics industry.

Compared with the traditional logistics system, the blockchain-based logistics scheme ensures the security of users' personal privacy, the authenticity and traceability of logistics information to a certain extent. However, most of the existing blockchain-based privacy preservation logistics schemes only propose corresponding system models, which cannot be directly applied. As a result of the leaking of logistical information in the current logistics system and the problems associated with tracing the package delivery process, we developed a privacy and traceability enhanced blockchain-based scheme for logistics that is both private and efficient. The following are the major contributions:

- On the basis of consortium blockchain, we offer a privacy-preserving architecture for logistics platforms. It enables effective auditing and tracing of logistical privacy and process information. Users may simply search for logistics information while maintaining their privacy.
- To safeguard the personal privacy and logistics route information of users, We offer an attribute-based encryption approach and fine-grained access control for logistics stations and users, guaranteeing that logistics stations can only get logistical information based on their attributes, enabling the security and control of privacy rights and logistics route information.
- Finally, we built a prototype system using the Hyperledger Fabric blockchain technology and validated the scheme's practicality.

The remainder of this essay is organized in the following manner. The section II work will discuss related work. In section III, we will discuss the strategies that were used in this paper. The section IV contains the system model, threat model, design objectives, and specific algorithm. In section V, we discussed the development environment and the prototype's implementation. In section VI, we discussed the development environment and the prototype's implementation.

Compared to our conference version [1], we have made great enhancements. We gave a more detailed traceable privacy-preserving logistics information scheme, Firstly, the introduction is further expanded, and the research background of the logistics system is introduced in more detail.Secondly, In related work, we have supplemented the current domestic and foreign research status of blockchain-based privacy-preserving logistics system, and added the comparison between the existing schemes and our scheme, highlighting the advantages of our scheme. Then, we conducted a more detailed analysis and design on the complexity and practicality of the algorithm, and provided more figures in the performance analysis to illustrate the effectiveness of the scheme, which proved the efficiency and privacy performance of the proposed scheme.

II. Related work

In this section, we mainly carry out two parts of work, one is to introduce and summarize the logistics privacy-preserving scheme in recent years, and to make a detailed comparison with our scheme; the second is to study and discuss the blockchain technology combining the current logistics system's status of domestic and foreign research and the application in the logistics industry.

A. Logistics privacy-preserving schemes

In a typical logistics information system, information is kept in the logistics company's central database, as seen in Fig. 1, and its security is entirely dependent on the logistics company's trustworthiness. However, once the centralized logistics management is attacked by illegal users, it will lead to the leakage of a large number of logistics data, damage the company's property and can not guarantee the interests of customers. Then the centralized storage is straightforward to tamper with and subject to single-point attacks [2]. With the increasing expansion of modern logistics, users face a significant threat to their privacy. In a conventional logistics information system, a package's information should be divided into two sections: personal and logistical. Personal information typically contains the sender's and receiver's identities. By contrast, logistics information primarily comprises of the start and finish points of the logistics process, as well as the delivery path. [3]. As a result, logistics system's security and privacy are primarily concerned with two forms of privacy information. [4] proposed a two-dimensional code-based privacy protection system for logistics information. In this paper, the method of segmented encryption of logistics information is adopted, the two-dimensional code is used to store the encrypted logistics information and the authority classification mechanism is designed, which solves the problem of privacy leakage in logistics transport process and data storage. However, each logistics station needs to continuously update the QR code, and repeat encryption and decryption, which reduces efficiency. In 2014, Wei et al. [5] presented a symmetric encryption-based logistics privacy-preserving system. While this approach does present a way for encrypting personal information, it does not adhere to real-world applications and is not easily adaptable to the existing LIP system. Protective techniques for private information in logistics delivery are presented in the preceding ways, however, no practical privacy preservation schemes for logistics information are proposed. In [6], this scheme achieves the confidentiality of logistics information, but it is inefficient to encrypt and decrypt logistics information repeatedly in the logistics process. In [7], while the ABE algorithm provides fine-grained access control for logistics service providers, which effectively ensures the security of customers' privacy information, it does not distinguish between personal information and logistical data, which allows logistics personnel to readily gain personal privacy. PriExpress has been presented as an attribute-based encrypted privacy-preserving logistics system that enables fine-grained access control to logistics data. By encrypting order information with CP-ABE, the sender can set an access strategy for orders containing sensitive information [8]. However, the approach does not distinguish between customers' private information and logistical data. When logistics company staffs deal with logistics delivery services, they require strong and complicates computing abilities to process delivery information, which is not convenient for the availability and implementation of the system.

Satoshi Nakamoto first proposed the notion of blockchain in 2008 [9]. After three generations of development, blockchain 3.0 has penetrated into the real economy. In 2018, Dobrovnik et al. [10] presented a framework description of the development of blockchain in the logistics industry. Subsequently, Gao et al. [11] developed a technique for protecting the privacy of logistics information based on attribute encryption and location, guaranteeing that different couriers can access just the logistics information for the next station. All logistics transaction data is maintained on the blockchain under this system, assuring its safety and traceability [12]. However, this scheme relies on location cryptography to facilitate package delivery, which necessitates the use of numerous parcel devices. As a result, there may be difficulties in implementing this system. The comparison between the above scheme and the proposed scheme is shown in Table 1.

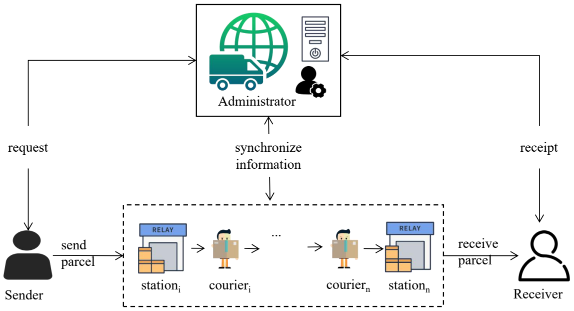


Fig. 1. Traditional Logistics System.

B. Logistics schemes based on blockchain

In recent years, blockchain technology has received extensive attention and rapid development worldwide [13]. As an underlying technology, blockchain is one of the important supports for the component logistics system. First of all, the open and consensus features of the blockchain can enable participants such as logistics stations and front-line logistics service staff to act as nodes in the network to achieve the transparency, openness and authenticity of customers' privacy and logistics information in the package delivery process. Secondly, a centralized logistics system can easily lead to single-point failures, resulting in the loss and leakage of users' private information. Blockchain, as a distributed shared ledger [14], can avoid system paralysis caused by network attacks. Then, the decentralization, trustlessness, and non-tamperability of the blockchain can ensure the authenticity, integrity, and validity verification of users' privacy and logistics information. Many researchers at home and abroad are committed to incorporating blockchain technology into the supply chain logistics business. The combination of blockchain technology and the logistics supply chain industry has gradually become a standard in the industry. The application of blockchain technology [15] to the logistics industry can effectively solve the problem of data leakage and tampering of users' privacy and logistics information in the logistics industry, and the traceability of logistics information.

Aiming at how to better integrate the blockchain into the logistics industry to ensure the privacy of logistics data, domestic and foreign researchers have proposed many solutions. In 2018, JD.com took the lead in establishing the country's first "logistics + blockchain" technology alliance, incorporating blockchain technology into the supply chain logistics business, and promoting the upgrade and reform of the logistics industry. Traditional logistics systems based on the Internet of Things (IOT) usually store users' sensitive information in a centralized cloud center, which is likely to cause the leakage of logistics information. [16] proposed a blockchain-based data security storage scheme, it uses the distributed characteristics of the blockchain network to securely store logistics data. Combining attribute-based encryption and blockchain technology, a new access control strategy based on blockchain and trusted and secure ciphertext strategy is proposed to achieve access control, thereby achieving data sharing safely [17]. Ar, Ilker Murat, et al [18] used a quantitative method to study the feasibility of blockchain technology in the logistics system. This paper proposed a decision-making framework based on a multi-criteria decision-making structure to realize the interoperability and availability of logistics data in the logistics operation process. In addition to auditability and security, the decision-making framework allows decision makers to evaluate the practicality of blockchain in the logistics industry, which is currently one of the key research topics of blockchain in the logistics field.

Blockchain is a key technology to acheive traceability in the logistics system, and it plays a vital role in improving the auditability and traceability of logistics information. The decentralization and non-tamperable of the blockchain, as well as the corresponding encryption algorithm and timestamp, can effectively solve the pain points that are difficult to trace in traditional logistics system. In order to solve the problem of traceability of logistics data when logistics disputes occur in the logistics process, and to improve the internal operation performance of the logistics system, many solutions have been proposed at home and abroad. In 2017, JD.com joined forces with strategic parties such as Walmart and IBM to form a food safety blockchain traceability alliance, using blockchain technology to achieve end-to-end traceability of food [19]. In [20] describes how to use blockchain to improve traceability and transparency for fourth-party logistics companies, but to achieve this goal, three conditions must be met: mutual cooperation between logistics users, integration between different IT systems, and users' smartphones motivation of the application. In [21] researched the current impact of blockchain on trace-

TABLE I
THE SCHEME COMPARISON OF LOGISTICS

Logistics privacy preservation schemes	DS	ABAC	LIP	CPP	VR	VP	NRC	NRS	Security	Traceability
Wei et al.[3]	×	×	×	✓	×	×	×	×	×	×
Qi et al.[4]	×	×	×	×	×	×	×	×	✓	×
Li et al.[6]	×	✓	✓	×	×	×	✓	×	×	×
Gao et al.[8]	×	✓	✓	✓	✓	✓	✓	✓	✓	×
Our scheme	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

- DS-distributed storage ● ABAC-attribute based access control ● LIP-logistics information protection
- CPP-confidentiality of customers' privacy ● VR-verifiability of the receiver ● VP-verifiability of packages
- NRC-the non-repudiation of the couriers ● NRS-the non-repudiation of the logistics station

ability in the logistics industry. Based on the characteristics of consortium blockchain, a logistics information traceability model is established [22], which can effectively prevent the logistics information on the chain from being tampered with, and the information matching mechanism is applied to the traceability model to improve the practicality of the model. [23] using the publicly verifiable and non-tamperable features of the blockchain to achieve trust between multiple entities in the logistics system, and in order to trace logistics information, the paper proposes a blockchain-based intelligent anti-switch package in the logistics system, which provides traditional logistics system that difficult to be traceable with a brand-new solution.

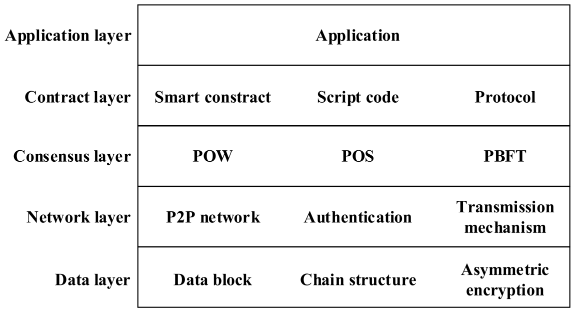
III. PRELIMINAIES

In this section, we will introduce some essential technologies used in our scheme and review the applications of mentioned technologies.

A. *Blockchain Technology*

Blockchain technology is a distributed storage ledger that is decentralized. [9], the chain structure is the most critical characteristic of the blockchain. In general, the blockchain architecture is composed of five layers: data, network, consensus, contact, and application [2]. Blockchain technology is to use the block chain data structure to verify and store data, use distributed node consensus algorithm to generate and update data, use cryptography to ensure the security of data transmission and access, and use the intelligence composed of automated script codes. A new distributed infrastructure and computing paradigm that uses contracts to program and manipulate data.

The data layer is identical to the data structure used by the blockchain's four fundamental technologies, namely the ”block + chain” structure. Typically, a block consists of a block header and a block body, and all blocks are connected chronologically via a hash function, the network layer is primarily suggested to employ a P2P mechanism of communication. The consistency of data across the blockchain network is ensured by the consensus layer. Currently, the most often used consensus algorithms are PoW, PoS, and PBFT. After the corresponding program code is written into the smart contract, the system can customize the constraints, without the need for an untrusted third party to endorse, and it will operate in real time immediately when the time is up. Of course, in the contract layer, in addition to smart contracts, there are some other script codes, side chain applications, etc. This article discusses a privacy-preserving and traceable logistics scheme at the application layer. At the moment, blockchain technology is classified as public blockchain, consortium blockchain, and private blockchain. Public blockchain are considered fully decentralized and are widely used in digital currencies such as Bitcoin. However, the low efficiency of public blockchain is difficult to meet the complex application scenarios. In the case of weak centralization, consortium blockchain can maintain high efficiency, and it can better meet the complex logic operation. Therefore, we chose to use consortium blockchain to build our application. As shown in the Fig. 2.



Application layer	Application		
Contract layer	Smart constract	Script code	Protocol
Consensus layer	POW	POS	PBFT
Network layer	P2P network	Authentication	Transmission mechanism
Data layer	Data block	Chain structure	Asymmetric encryption

Fig. 2. The architecture of Blockchain.

B. *Attribute encryption algorithm based on ciphertext strategy*

J. Bethencourt introduced an attribute-based encryption (ABE) technique in 2007 [7]. Later, A. Sahai, and B. Waters et al. described two types of ABE schemes [24], that is, ciphertext-based policy attribute encryption (CP-ABE) and key-based policy attribute encryption (KP-ABE). The purpose of ABE is to augment the identity-based encryption system with an access structure [25]. The term ciphertext policy attribute-based encryption system (CP-ABE) refers to an encryption system in which the ciphertext corresponds to an access structure and the key to an attribute set. Decryption is possible only if the attributes contained in the attribute set conform to the access strategy. CP-ABE deploys the access policy in the ciphertext. The ciphertext can be decrypted only when the stations' attribute set matches the access strategy. In this way, the data owner can decide what type of users can access the logistics data, thus achieving fine-grained access control.

IV. System model

This section describes the system model for this logistics system, briefly describes the types of entities included in the model, and describes the model's workflow. As shown in Fig. 3, this system includes four types of entities.

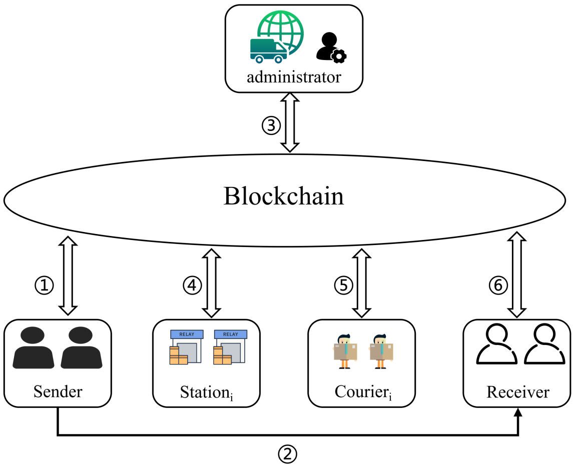


Fig. 3. The System Model for this scheme.

- **Customers.** Customers who may be involved in the logistics process consist of senders and receivers. They are capable of encrypting, uploading, downloading, and decrypting personal private information, as well as querying logistics information based on the logistics ID order(ID_{order}). To receive logistics services, they must not reveal personal information or logistical route information.
- **Logistics Administrator.** Being the logistics company's leader, the administrator is forthright but inquisitive. He gives convincing and dependable package transmit service to consumers and oversees the whole logistical transport process. Simultaneously, he attempts to decode the customers' personal information.The administrator can build the logistics distribution route and complete the ABE of the logistics delivery path based on the customer's address in order to accomplish access control to each logistics station.
- **Logistics station.** The major role of the logistics station is to manage the station's following details. After the courier sends the parcel to next logistics station, the logistics station can decrypt the next station destination and allocate a courier to deliver it using their own properties.
- **Couriers.** Couriers are engaged by logistics companies to deliver packages. A courier is only responsible for transporting packages between logistics stations. He receives packages from the same logistics station, takes them to the next station or receiver, and then delivers them. When the courier receives the package, he or she simply has to be aware of the following station information in order to complete the delivery.

We created a threat model for each entity as follows:

We presume that all parties to this scheme adhere to cryptographic primitives; we do not address network security risks (such as DDoS attacks), computer virus attacks, or hardware attacks.

We suppose that the sender is interested in other users' logistics information or is attempting to send out some contraband, and the receiver is feigning to receive other people's parcels. For the administrator of a logistics company, he is straightforward but inquisitive. On the one hand, the administrator is able to develop logistical routes and encrypting transport data using a variety of access mechanisms to guarantee the data's privacy. On the other hand, administrators are also concerned about their customers' privacy and will attempt to collect personal information about them unlawfully. Package management is the responsibility of each logistics delivery point. They are inquisitive about the privacy information of their consumers. Certain logistic stations with unique characteristics may collaborate to decrypt personal information. As the courier's executor, he or she may not take the item to the next logistics station or to the intended receiver during the distribution process and may dispute his or her actions, resulting in the package's lost.

A. Design goals

- **Privacy preservation.** Personal information and logistics data should not be exposed or tampered with in the normal logistics processes. Personal information can be used by related senders and receivers only for the purpose of package delivery and authentication. No logistics companies or courier service can guarantee the privacy of their customers. Additionally, the logistics is private for different logistics stations and couriers, and logistics organizations can implement access control based on the characteristics of stations.
- **Efficient traceability.** All logistics activities can be saved to the blockchain depending the logistics process's ID_{order}. Based on the ID_{order}, users and auditors may swiftly trace logistical information and identify anomalous occurrences.
- **Non-repudiation.** Using blockchain to record logistics information, customers cannot deny that they receive or send a package. The logistics station and courier cannot deny the authenticity of their actions to complete the delivery of the package.
- **non-tamperability.** Based on the non-tampering feature of the blockchain, once the user's privacy and logistics information are stored on the chain, no one can modify the information on the chain, so as to achieve the integrity of users' privacy and logistics information.

B. The workflow of logistics system

1) Key initialization

To guarantee privacy rights and logistical information in the process of logistics, this method requires numerous parties to encrypt data on the blockchain, which requires us to initialize multiple entities' keys. Starting the actual the logistical process, a secure and trustworthy KDC must execute the key generation and distribution.

Firstly, it is important to deliver key pairs to the receiver in order for the receiver to retain the security of his or her personal data: the receiver's public key and private key (Pub_{Rec}, Pri_{Rec}). Second, in order to maintain the security of logistical data, It is essential for the administrator to release asymmetric key pairs: the administrator's public key and private key(Pub_{Adm}, Pri_{Adm}). Most significantly, it is essential to collect the attributes of multi logistics stations to spread the attribute base through the use of key pairs: the logistics station's public key and its private key(Pk_{s_t}, Sk_{s_t}), to prevent the logistics station from receiving logistic path information in an unauthorized manner while still allowing the logistics station to obtain the associated route.

2) Order initialization

This part will discuss the logistics data that is generated during the logistics process. Logistics order information consists of three parts: *logistics information*, *personal information* and *goods information*.

Include the sender's address (Sen_{Add}), the receiver's address (Rec_{Add}), etc, in the logistics information. It uses Pub_{Adm} to ensure that only the logistics company has access to the logistical information.

Personal information contains the sender's name (Sen_{Name}), the sender's telephone number (Sen_{Tel}), the receiver's name (Rec_{Name}), the receiver's telephone number (Rec_{Tel}), etc.; using Pub_{Rec} to encrypt personal information to ensure absolute confidentiality in the entire logistics transaction process.

Goods information contains goods name ($Goods_{Name}$) and goods quality ($Goods_{Qua}$), which is convenient for the administrator to check the package.

The logistics order information is divided into two sections, $section_1$ and $section_2$. The content of the $section_1$ is the logistics information, goods information, and ID_{order}. $section_1$ is logistics information in deliver process. Using Pub_{Adm} to encrypt the $section_1$ to get the logistics information ciphertext $Cipher_{section_1}$. $section_2$ contains the sender and receiver information, logistics information, goods information, ID_{order}, and random number RN, etc. All information should be kept in ciphertext throughout the logistical process and should only be retrieved and verified by the receiver. Therefore, the component of the $section_2$ should be encrypted with Pub_{Rec} to obtain the ciphertext $Cipher_{section_2}$ of personal information. The sender combine $Cipher_{section_1}$ with $Cipher_{section_2}$ as $Cipher_{order}$ and saves it to the blockchain to finish the logistical information's initialization. The Fig. 4 depicts the logistics order details.

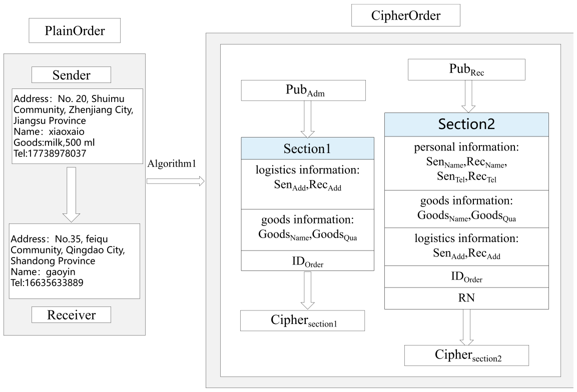


Fig. 4. The data structure of ID_{order}.

3) Workflow

① The sender initiates communication with the logistics station by submitting a shipment request. When the logistics station gets the shipping request, which generates a ID_{order} and sends it to the sender as the package's unique number. After obtaining the ID_{order}, the sender encrypts the logistical data. This logistics ciphertext is divided into two parts. First, the sender stores Sen_{Add}, Rec_{Add}, $Goods_{Name}$, $Goods_{Qua}$ and ID_{order} in $section_1$, and encrypts the $Cipher_{section_1}$ with Pub_{Adm}. Hereafter, the sender creates a random number RN, and calculates the hash value of RN, $HN = Hash(RN)$, and saves the random number RN, ID_{order}, Sen_{Name}, Rec_{Name}, Sen_{Add}, Rec_{Add}, Sen_{Tel}, Rec_{Tel}, $Goods_{Name}$, and $Goods_{Qua}$ in $section_2$, and encrypt the $Cipher_{section_2}$ with Pub_{Rec}. The sender stores $Cipher_{section_1}$ and $Cipher_{section_2}$ in $Cipher_{order}$ and uploads the ciphertext information to the blockchain.

② The sender uses Pub_{Rec} to encrypt the unique ID_{order} and random number RN and transmits them to the receiver.

③ After obtaining the $Cipher_{order}$ from the blockchain, the administrator may use his private key to decrypt the $Cipher_{section_1}$, therefore obtaining the starting and ending logistics information. The administrator can split the logistics transportation path, and the result is encrypted based on an attribute; lastly, a series of ciphertext information $CT_1, CT_2, ...CT_n$ is obtained, and the data about the path is recorded to the blockchain.

④ The logistics station can get the ciphertext from the blockchain and decrypt it using an attribute-based decryption key depending on their characteristics. The station may decrypt the address of the following station based on their attributes. After determining the courier, the logistics station uploads to the blockchain the current station address associated with the ID_{order}, the courier's name, and the delivery package's timestamp.

⑤ After delivering the package to the next station, the courier adds the ID_{order}, the station's current arrival address, his name, and the delivery package's timestamp to the blockchain.

Rep the first two phases ④⑤ until the logistics $station_n$. After arriving at the logistics $station_n$, the logistics $station_n$ will complete the arrival state modification according to the ID_{order}.

⑥ Following the receiver's verification of the chain and receipt of the logistics arrival sign, he may engage with the logistics $station_n$ to pick up the goods. The logistics $station_n$ asks the receiver's verified identity information and requests the receiver's RN. The last station calculates HN_1 = $Hash(RN)$, then he needs to determine whether HN_1 is equal to HN, so that the identity of the receiver can be determined. The station can change and upload the logistics receiving state to true, and the receiver may query the chain for $Cipher_{section_2}$. So far, the receiver could get and decrypt the whole logistical information using his private key.

C. Algorithm

To protect the confidentiality of personal and logistical processes, we keep all private data on the blockchain in ciphertext form. We explained the encryption and chaining processes in depth in the preceding section. This section will cover the logistics station's ABE algorithm and the function algorithm used in the chaincode.

`Setup(`k`)` $\rightarrow$ (GP, Mk): The initialization algorithm defines the variables of the algorithm. `Setup()` takes the parameter k to compute global parameter GP and master key Mk, select a group G with prime number p as the order, in this group the generator is g. Besides, select two random numbers α,β from Z_p^*, then suppose the global parameters GP= G, g, h=(g^{β}, $e(g,g)^{\alpha}$), the mater key Mk=(β,g^{α}).

$Key\_Gen(Pk, Mk, A)$ $\rightarrow$ `(`Sk`)`: This method is primarily responsible for generating attribute-based-decryption keys. Take the public key Pk and master key Mk as input variables, and a set of logistics stations' identity attributes A. Select a random number r from Z_p, for each attribute φ_i from A, it can output the logistics stations' private key Sk.

$$Sk = (B = g^{(\alpha+r)/\beta}, \forall \varphi_i \in S : B_{\varphi_i} = g^r \cdot H(j)^{r\varphi_i}, \\ B'_{\varphi_i} = g^{r\varphi_i}) \tag{1}$$

`Encryption Algorithm` Encrypt(M, Pk, A_{cp}) $\rightarrow$ CT: the logistic information (M), public key Pk, and the access control policy(ACP) A_{cp} as input, get the logistic information ciphertext CT. In this algorithm, we use a access control tree T as ACP. First, we select a polynomial q_x for each attributes x in T. For tree node x , define the degree d_x of the polynomial q_x be one node less than the threshold k_x, and $d_x = k_x - 1$. The algorithm selects random value s from Z_p as the root node $Root$, and sets $q_{Root(0)}$ = s. Then randomly select the d_{Root} point in the polynomial q_{Root} and fully describe it. Therefore, from $Root$ down. For any node x, it sets $q_x(0)$ =$q_{parent(x)}(index(x))$. Randomly select d_x and other nodes to completely set q_x. Define L be the set of leaf nodes in T, using this access control tree, we can get the logistic information ciphertext CT. In this algorithm, the access control tree can be designed as Fig. 5.

$$\begin{gathered} CT = \Big(T, \tilde{C} = M(g,g)^{\alpha s}, C = h^s \\ \forall l \in L : C_l = g^{q_l}(0), C'_l = H(\mathrm{att}(l))^{q_l(0)}\Big) \end{gathered} \tag{2}$$

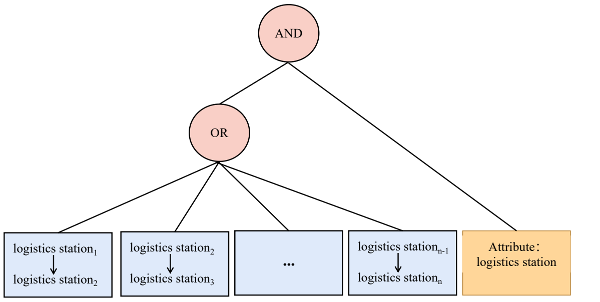

AND
OR
logistics station$_1$ ↓ logistics station$_2$
logistics station$_2$ ↓ logistics station$_3$
...
logistics station$_{n-1}$ ↓ logistics station$_n$
Attribute: logistics station

Fig. 5. Access control policy

`Decryption Algorithm` Decryption(CT, Sk, x) $\rightarrow$ CT: The ciphertext CT = $\Big(T, \tilde{C}, C, \forall l \in L : C_l, C'_l\Big)$ and the logistics station's key Sk corresponds to a set of attributes, and a node x from access control tree as input. if x is leaf node ,we define the i=att(x)(x $\in$ {logistics phase, logistics station and so on}). We can decrypt it as follow algorithm:

$$\begin{aligned} \mathrm{DecryptNode}(CT, Sk, x) &= \frac{e\left(D_i, C_x\right)}{e\left(D'_i, C'_x\right)} \\ &= \frac{e\left(g^r \cdot H(i)_i^r, h^{q_x(0)}\right)}{e\left(g^{r_i}, H(i)^{q_x(0)}\right)} \\ &= e(g,g)^{r q_x(0)} \end{aligned} \tag{3}$$

and then it can decrypt the corresponding next station M.

Thus, it enables fine-grained access control for logistics stations with distinct characteristics and assures that various stations may decrypt only the plaintext of the logistical path specified by their attributes A_{cp}.

Additionally, the chaincode contains a sequence of functional algorithms.

- `Logistics_CreatTx(Transaction information)`: Using theID_{order} and transaction information from $section_1$ and $section_2$ as input parameters, this method may be used to create orders and upload logistical transactions. The detail of this algorithm as algorithm 1.
- `Route_DecideTx(starting station, ending station)`: The administrator may employ the algorithm to ascertain the logistical delivery path, and then acquire information about the stations ST_1, ST_2,...ST_n involved in the logistics process. The detail of this algorithm as algorithm 2.
- `Package_DeliverTx(`ST_i`,name,timestamp)`: This algorithm can be used by the logistics station or courier to submit the logistics transportation record to the blockchain. The detail of this algorithm as algorithm 3.

V. Deployment and Implementation

We constructed a simulation of the logistics system in this research on the Hyperledger Fabric platform. We construct the experimental environment as follows: PC (Intel(R)Core(TM) i7-10750, 8GB RAM, Ubuntu 20.04). Docker is used to manage the chaincode, while Docker-compose is used to built the Docker container. Hyperledger Fabric v2.x is responsible

Algorithm 1 `Logistics_CreatTx`

```
Input: A set of Transaction information, sender, receiver,
    $Sen_{Add}$, $Rec_{Add}$, $Sen_{Tel}$; The public key of administrator
    $Pub_{Adm}$
Output: A transaction ID $ID_{order}$, and a logistics information ciphertext $Cipher_{order}$
Initialization:
    Declare the $Txinfo$ format
Variable Assignment:
    Assign the input parameters $ID_{order}$, $Sender$,
    $Receiver$, $Sen_{Add}$, $Rec_{Add}$ to $Txinfo$
Encryption:
    do the encryption with $Pub_{Adm}$ and logistics transaction $Txinfo$
    Enc( $Pub_{Adm}$,$Txinfo$) $\rightarrow$ $Cipher_{order}$
```

Algorithm 2 `Route_DecideTx`

```
Input: Logistics transaction ciphertext $Cipher_{order}$
Output: Decision route: obtaining the station information
    $CT_1$, $CT_2$,...$CT_n$
Decryption:
    Decrypt the $Cipher_{order}$ with $Pri_{Adm}$
    Dec($Pri_{Adm}$,$Cipher_{order}$) $\rightarrow$ (starting station, ending station)
Decision:
    Decision(starting station, ending station) $\rightarrow$ ($ST_1$, $ST_2$,...$ST_n$)
Storage:
    Performed attribute-based encryption on route station
    ($ST_1$, $ST_2$,...$ST_n$) $\rightarrow$ ($CT_1$, $CT_2$,...$CT_n$)
```

for the development of the blockchain. As shown in Fig. 6, a consortium blockchain network built on the HLF platform is being constructed to emulate the logistics prototype system. Just like the HLF network architecture in Fig. 6 and system's deployment environment, the logistics prototype system is implemented. We add customers who demand to get logistics services, administrators of logistics companies, stations responsible for sorting out package information, and couriers who are responsible for delivering packages as an organization to join the above consortium blockchain network.

Install chaincode (including `Logistics_CreatTx`, `Route_decideTx()`, `Package_DeliverTx() functions`), etc. into peer and initialize. Following startup, various peers will utilize chaincode to perform logistics tasks.

Finally, we invoke the chaincode Logistics_CreatTx() method to create logistical transactions on the chain, as the picture shown in Fig. 7; by using the chaincode Route_decideTx() function and completing the chaining of the logistics decision path's ciphertext, as shown in Fig. 8; the chaincode Package_DeliverTx() function is called to realize the on-chain of the logistics delivery process, as shown in Fig. 9. Lastly, the entire logistics information process will be chained together, ensuring the protection of both personal and logistical information, as well as the traceability of the package delivery process.

Algorithm 3 `Package_DeliverTx`

```
Input: Logistics transaction ID $ID_{order}$, Deliver attributes
Output: Delivery confirmation
if Deliver attributes satisfy access control policy then
        Obtain station and complete delivery
        Assign middle delivery information
```

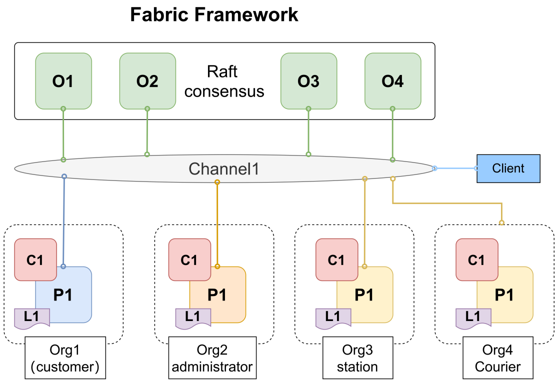
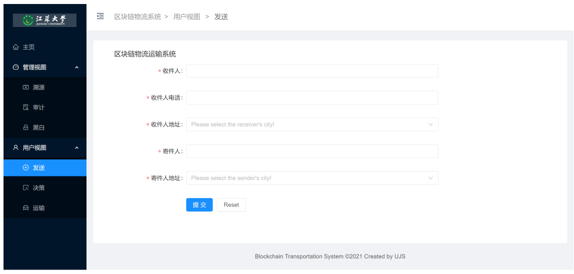


Fig. 6. The HLF network architecture.



区块链物流运输系统

* 收件人：

* 收件人电话：

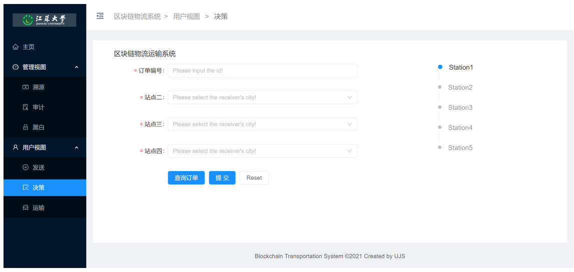
* 收件人地址： Please select the receiver's city!

* 寄件人：

* 寄件人地址： Please select the sender's city!

Blockchain Transportation System ©2021 Created by UJS

Fig. 7. The Screenshots of Logistics_CreatTx.



区块链物流运输系统

* 订单编号： Please input the id!

* 站点二： Please select the receiver's city!

* 站点三： Please select the receiver's city!

* 站点四： Please select the receiver's city!

● Station1

● Station2

● Station3

● Station4

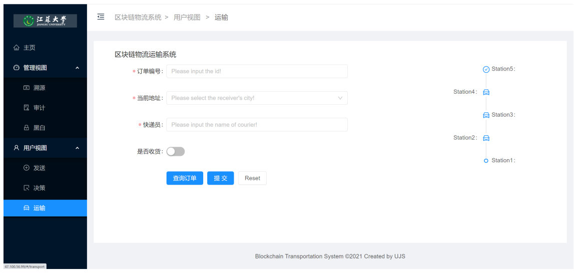
● Station5

Blockchain Transportation System ©2021 Created by UJS

Fig. 8. The Screenshots of Route_decideTx.

VI. PERFORMANCE EVALUTION

In this paper, PBC (pair-based cryptography) [26] is used to generate the key. The HLF blockchain platform tests the scheme, and uses 1024-bit discrete logarithmic difficulty for the test. We assume that the experimental test data is: secure and trustable key distribution center contains 500 senders, 300 receivers, 10 administrators, 80 logistics stations and 350 couriers. When the sender uploads personal information and



区块链物流运输系统

* 订单编号 : Please input the id!

* 当前地址 : Please select the receiver's city!

* 快递员 : Please input the name of courier!

是否收货 :

Blockchain Transportation System ©2021 Created by UJS

Fig. 9. The Screenshots of Package_DeliverTx.

logistics information, KDC needs to generate 5000 key pairs , The key is updated every day. In the calculation cost analysis of Fig. 10, the main calculation cost is the process of attribute-based key generation, encryption and decryption. In this paper, it is assumed that each data owner contains 8 attributes and 9 leaf nodes in the access control tree. Under this assumption, the system initialized time we can calculate is about 1200 milliseconds on average, and the time for attribute-based encryption is about 30 ms, and the attribute-base decryption time is about 12 ms. In addition, only the ABE encryption procedure is subject to tight time constraints in this system, and other processes have no strict requirements on timeliness. Therefore, the solution is considered feasible in terms of time complexity.

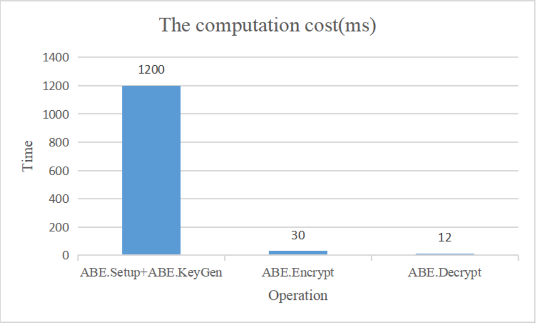


Fig. 10. Computation cost

Fig. 11 shows the operation of the sender to create a transaction and the receiver to query the transaction in HLF. The sender encrypts the corresponding logistics information and personal privacy and uploads them to the blockchain, and the administrator of the logistics company obtains it. The logistics request information is encrypted in segments, and then the logistics station and the courier decrypt the logistics information according to their attributes and deliver the corresponding packages. The receiver can query the corresponding logistics information according to their own needs.

As clearly given in Fig. 12 that when the sender sends 500 transaction requests, the transaction throughput rate can reach 83 tps. When the sender sends 5000 sending requests, the transaction throughput rate can still be maintained at about 80 tps. But when the sending request reaches 10000tx, the transaction throughput rate drops to about 58tps. When the sending request is 20000tx, the transaction throughput rate remains at 58tps. It shows that when the number of transactions reaches 10000tx, the system throughput rate reaches saturation. Since the query does not need to be sorted and endorsed, that is, the query transaction does not go through a consistent agreement, its processing speed is much faster. And it is not affected by the number of transactions, and its transaction throughput rate remains at about 40 tps. The results show that this experiment did not reach the process limit of QueryTx.

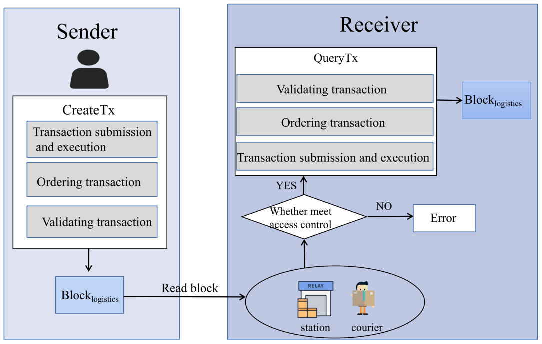

Sender
CreateTx
Transaction submission and execution
Ordering transaction
Validating transaction
$\text{Block}_{\text{logistics}}$
Read block
Receiver
QueryTx
Validating transaction
Ordering transaction
Transaction submission and execution
$\text{Block}_{\text{logistics}}$
YES
Whether meet access control
NO
Error
RELAY
station
courier

Fig. 11. Logistics transaction process on the blockchain network

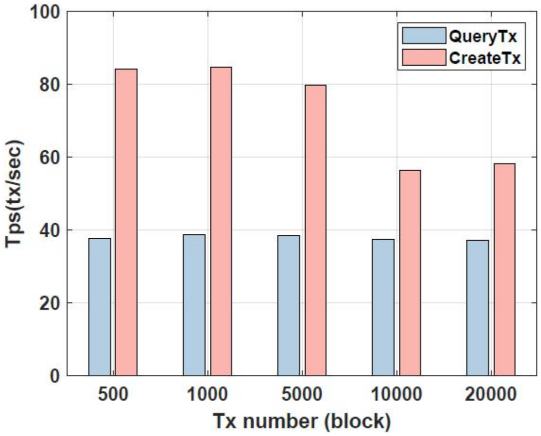


Fig. 12. Transaction throughput on the blockchain

VII. Conclusion

The consortium blockchain is applied to the logistics information system in this article. We proposed PTLchain, a logistics information system by using consortium blockchain and attribute-based encryption, as a mechanism that protects users' privacy, provides fine-grained access control, is auditable and traceable. We have altered the typical centralized logistics information scheme, assuring the validity and security of customers' private information and logistics data throughout the logistical process. And unlike existing blockchain-based logistics system, our proposal pays more attention to privacy preservation and traceability. Customers may validate the veracity of logistics data and obtain effective traceability; administrators can establish access control to logistics stations to secure the confidentiality of logistics delivery routes. More importantly, we built a prototype system using the Hyperledger Fabric blockchain technology and evaluated the scheme's practicality using performance evaluation.

Acknowledgment

This paper was supported by National Key R&D Program of China(2020YFB1005500), the Natural Science Foundation of the Jiangsu Higher Education Institutions under (No.20KJB520031), the Natural Science Foundation of Jiangsu Province under(No.BK20200888), and Jiangsu Province Higher Education Teaching Reform Research Project under (No.2021JSJG403).

References

[1] X. Lin, P. Jing, C. Yu, and X. Feng, "Tpli: A traceable privacy-preserving logistics information scheme via blockchain," in *2021 International Conference on Networking and Network Applications (NaNA)*. IEEE, 2021, pp. 345–350.

[2] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE international congress on big data (BigData congress)*. IEEE, 2017, pp. 557–564.

[3] J. Yu, H. Xue, B. Liu, Y. Wang, S. Zhu, and M. Ding, "Gan-based differential private image privacy protection framework for the internet of multimedia things," *Sensors*, vol. 21, no. 1, p. 58, 2021.

[4] X. Zhang, H. Li, Y. Yang, G. Sun, and G. Chen, "Lipps: logistics information privacy protection system based on encrypted qr code," in *2016 IEEE Trustcom/BigDataSE/ISPA*. IEEE, 2016, pp. 996–1000.

[5] W. Qian, W. Chen, and L. Xingyi, "Express information privacy protection application based on rsa," *Appl. Electron. Tech*, vol. 40, no. 7, pp. 58–60, 2014.

[6] H. Qi, D. Chenjie, Y. Yingbiao, and L. Lei, "A new express management system based on encrypted qr code," in *2015 8th International Conference on Intelligent Computation Technology and Automation (ICICTA)*. IEEE, 2015, pp. 53–56.

[7] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *2007 IEEE symposium on security and privacy (SP'07)*. IEEE, 2007, pp. 321–334.

[8] T. Li, R. Zhang, and Y. Zhang, "Priexpress: Privacy-preserving express delivery with fine-grained attribute-based access control," in *2016 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2016, pp. 333–341.

[9] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.

[10] M. Dobrovnik, D. M. Herold, E. Fürst, and S. Kummer, "Blockchain for and in logistics: What to adopt and where to start," *Logistics*, vol. 2, no. 3, p. 18, 2018.

[11] Q. Gao, J. Zhang, J. Ma, C. Yang, J. Guo, and Y. Miao, "Lip-pa: A logistics information privacy protection scheme with position and attribute-based access control on mobile devices," *Wireless Communications and Mobile Computing*, vol. 2018, 2018.

[12] C. YU, Z. HAN, zhiyuan LI, and L. WANG, "Blockchain-based hierarchical and multi-level smart service transaction supervision framework for crowdsourcing logistics," *Chinese Journal of Network and Information Security*, vol. 6, no. 3, pp. 50–58, 2020.

[13] W. Yang, S. Garg, A. Raza, D. Herbert, and B. Kang, "Blockchain: trends and future," in *Pacific Rim Knowledge Acquisition Workshop*. Springer, 2018, pp. 201–210.

[14] X. Fu, H. Wang, and P. Shi, "A survey of blockchain consensus algorithms: Mechanism, design and applications," *Science China Information Sciences*, vol. 64, no. 2, pp. 1–15, 2021.

[15] Z. Zheng, S. Xie, H. Dai, , and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE International Congress on Big Data (BigData Congress)*, 2017, pp. 557–564.

[16] H. Li, D. Han, and M. Tang, "A privacy-preserving storage scheme for logistics data with assistance of blockchain," *IEEE Internet of Things Journal*, 2021.

[17] S. Gao, G. Piao, J. Zhu, X. Ma, and J. Ma, "Trustaccess: A trustworthy secure ciphertext-policy and attribute hiding access control scheme based on blockchain," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5784–5798, 2020.

[18] I. M. Ar, I. Erol, I. Peker, A. I. Ozdemir, T. D. Medeni, and I. T. Medeni, "Evaluating the feasibility of blockchain in logistics operations: A decision framework," *Expert Systems with Applications*, vol. 158, p. 113543, 2020.

[19] R. Kamath, "Food traceability on blockchain: Walmart's pork and mango pilots with ibm," *The Journal of the British Blockchain Association*, vol. 1, no. 1, p. 3712, 2018.

[20] A. Jeppsson and O. Olsson, "Blockchains as a solution for traceability and transparency," 2017.

[21] J. M. Song, J. Sung, and T. Park, "Applications of blockchain to improve supply chain traceability," *Procedia Computer Science*, vol. 162, pp. 119–122, 2019.

[22] X. Li, F. Lv, F. Xiang, Z. Sun, and Z. Sun, "Research on key technologies of logistics information traceability model based on consortium chain," *IEEE Access*, vol. 8, pp. 69 754–69 762, 2020.

[23] C.-L. Chen, Y.-Y. Deng, W. Weng, M. Zhou, and H. Sun, "A blockchain-based intelligent anti-switch package in tracing logistics system," *The Journal of Supercomputing*, vol. 77, no. 7, pp. 7791–7832, 2021.

[24] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM conference on Computer and communications security*, 2006, pp. 89–98.

[25] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Annual international cryptology conference*. Springer, 2001, pp. 213–229.

[26] B. Lynn, "The pairing-based cryptography (pbc) library," 2010.

Xiaoguo LIN received the BS degree from Jinagsu University, in 2020. She is currently a master student of Jiangsu University, her main research direction is blockchain and data privacy.

Xunbing WANG received the MS degree from Jinagsu University, in 2008. He is currently an associate professor of Jiangsu University, his main research interests include blockchain, data privacy, and modern educational technology.