Journal of Cases on Information Technology
Volume 24 • Issue 5

A Blockchain-Based Privacy Protection Application for Logistics Big Data

Huabin Duan, College of Information Engineerin, Hunan University of Science and Engineering, China*

Jie Yang, College of Information Engineering, Hunan University of Science and Engineering, China

Huanjun Yang, College of Information Engineering, Hunan University of Science and Engineering, China

ABSTRACT

Logistics business is generally managed by logistics orders in plain text, and there is a risk of disclosure of customer privacy information in every business link. In order to solve the problem of privacy protection in logistics big data systems, a new kind of logistics user privacy data protection scheme is proposed. First of all, an access rights management mechanism is designed by combining blockchain and anonymous authentication to realize the control and management of users' access rights to private data. Then, the privacy and confidentiality protection between different services is realized by dividing and storing the data of different services. Finally, the participants of the intra-chain private data are specified by embedding fields in the logistics information. The blockchain node receiving the transaction is used as the transit node to synchronize the intra-chain privacy data, so as to improve the intra-chain privacy protection within the business. Experimental results show that the proposed method can satisfy the privacy requirements and ensure considerable performance.

KEYWORDS

Big Data, Blockchain, Logistics, Privacy Protection

1 INTRODUCTION

In order to facilitate the receiving, distribution and delivery of goods by logistics enterprises, the senders need to fill in a lot of logistics privacy data on the logistics bill. In the whole process of logistics, these logistics privacy data are visible in plain text, which will cause the leakage of logistics privacy data (Rivero-García et al., 2019)(Ahmad et al., 2021)(Li et al., 2016)(Liu et al., 2016). Some websites clearly list the price of logistics order information and provide the service of "generating the back order". In the process of using logistics services, senders are also passive in preventing the leakage of logistics privacy data. While senders can protect their names by filling in pseudonyms, other logistics privacy data cannot be protected, such as telephone information and address information. The countermeasures for the logistics privacy data leakage in the logistics industry are as follows. On the one hand, try to deal with it at the level of management system. On the other hand, the privacy data of logistics users can be protected through technology, such as the application of two-dimensional code technology in information packaging. In the process of logistics transfer, the staff of logistics enterprises can scan the QR code through a special QR code scanner to obtain the logistics privacy data (Zhang et al., 2016)(Zhao & Zhang, 2019). However, the scanned data is still the plaintext information on the logistics bill, and the problem of leakage of logistics privacy data has not been completely solved (Chen et al., 2019). There are two main reasons. (1) Logistics enterprises do not pay

DOI: 10.4018/JCIT.295249

*Corresponding Author

attention to the protection of users' logistics privacy data. (2) In the process of logistics transfer, it is also necessary to complete the transfer process by manpower, so that the staff of logistics enterprises can still get all the plaintext information. Therefore, it is very important to study the privacy data protection technology in logistics

In the field of data protection of logistics privacy, literature (Qian et al., 2014) proposes a form that does not use logistics orders in the logistics process. Imagine encrypting and storing the addressee information that the deliveryman needs to deliver the parcels on that day in the Android phone, and using the home address as the file name of the encrypted information to deliver to the addressee address. However, this scheme has some limitations in practical application, as follows. (1) Give up the use of logistics bill, unable to realize the logistics transfer function. (2) The recipient's information is encrypted and stored in the mobile phone, which still fails to fully realize the hidden encryption of logistics privacy. Literature (Feng, 2021) proposed a logistics information privacy protection system based on QR code technology. The system uses segmented encryption technology to encrypt the logistics user's private data, and stores the encrypted cipher text in the two-dimensional code. It designs different levels of authorization mechanism to decrypt the corresponding information, so as to complete the logistics business operation. But the system does not give the concrete implementation and the implementation details of the hierarchical encryption technology. As can be seen from the above studies, existing researches still have the following shortcomings in the protection of logistics users' privacy. (1) User privacy data is still stored in the third party that is not fully trusted, and user privacy cannot be guaranteed. (2) Users cannot control and manage the access rights of logistics privacy data, and their control process lacks transparency and traceability, and they cannot control the partial reading of private data by third parties.

In the field of blockchain access control research, literature (Mohammadinejad & Mohammadhoseini, 2020) has solved the privacy problem when using third-party application services. It proposed a decentralized personal data management system to ensure that users own and control their own private data. Literature (Fan et al., 2018) proposed a medical data sharing system to solve the access control management problems existing in the process of medical data sharing. In this system, an application framework based on block chain is proposed. Users can easily and securely own, control and share their own medical data while ensuring that their privacy is not violated. Literature (Zyskind & Nathan, 2015) proposed a distributed personal data management system and an automated access control protocol based on blockchain to address the problem of privacy leakage caused by third-party collection of personal data. This protocol ensures that users own and control private data. However, it lacks support for multi-party fusion sharing scenarios. Literature (Feng et al., 2019) proposed a Hawk protocol that encrypts the communication between the two parties of the contract, aiming at the problem of transaction privacy leakage caused by blockchain transactions on the public network. This agreement mainly focuses on the transaction data, and does not have an advantage in the processing capacity of business data. Literature (Bünz et al., 2020) used an encrypted smart contract to protect public privacy files by means of public and private keys, and provides auditing and tracking. Literature (Patel, 2019) proposed a decentralized data sharing framework. User access requested to shared medical data are realized in a decentralized manner by verifying the user's cryptographic key. The above studies all solve the access rights control and management problems in different fields through blockchain, but there are still some problems: (1) Risk of disclosure of user privacy. (2) Access management based on Ethereum or Bitcoin network has the disadvantages of small throughput and slow transaction verification.

In order to solve the shortcomings of the current privacy protection technology and methods in the field of blockchain, this paper proposes a blockchain-based logistics big data privacy data protection method. A logistics prototype verification system is designed and implemented, and the security of the system is evaluated. The main work of this paper is as follows. (1) To solve the problem of users' lack of control over logistics privacy data, an access rights management mechanism based on the combination of blockchain and direct anonymous attestation (DAA) technology is proposed.

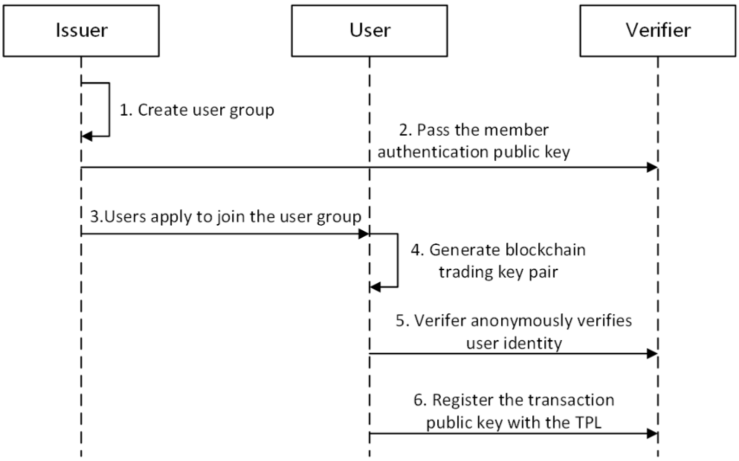
This mechanism implements membership management based on DAA anonymous authentication and provides anonymous and verifiable identity for entities on the blockchain. Access control of blockchain nodes is achieved by maintaining a transaction public key list (TPL), which solves the risk of privacy leakage existing in current blockchain technology. (2) The privacy and confidentiality protection between different businesses is realized by dividing the data of different businesses and storing them in partitions. (3) By embedding fields in the transaction body, the participants of the intra-chain privacy data are designated, and the blockchain node receiving the transaction is used as the transit node to synchronize the intra-chain privacy data, so as to improve the intra-chain privacy protection within the service.

2. THE METHODS

2.1 Permission Control of Private Data

The membership management module provides anonymous and verifiable identity for users who want to join the blockchain network according to the anonymous authentication scheme of DAA. A user in a DAA scenario is composed of a TPM and the corresponding Host. Users first obtain an identity certificate from Issuer and then use this certificate to prove to the Verifier that they are a legitimate user authenticated by Issuer. Finally, the transaction public key, which is tran_pub, is registered in the list of transaction public keys maintained by the Verifier. During this process, the Verifier does not have access to any information about the user's identity because the user is anonymous to the Verifier. So the Verifier does not know the real user identity of the tran_pub for each of the transaction public keys in the TPL. A user can anonymously authenticate multiple tran_pubs with the Verifier and register multiple tran_pub with the TPL, which are unrelated to each other. Therefore, it can solve the problem of privacy leakage risk existing in blockchain technology, that is, it is impossible for an attacker to analyze the association between blockchain trading address and node identity according to the association relationship existing in blockchain transactions. The specific process of the membership management module is shown in Figure 1.

Figure 1. The workflow chart of membership management module


Issuer
User
Verifier
1. Create user group
2. Pass the member authentication public key
3.Users apply to join the user group
4. Generate blockchain trading key pair
5. Verifer anonymously verifies user identity
6. Register the transaction public key with the TPL

Issuer creates a user group whose members are also physical nodes in the blockchain network. This step will generate the member authenticated public key K_{PG} KPC and the member issued private key K_{MIPK}. The steps are as follows.

Step1 Issuer selects an RSA modulus $n = pq$, where $p = 2p' + 1, q = 2q' + 1$. $p,\ q, p', q'$ are prime numbers, and *p* and *q* are prime numbers of the same length. The length of *n* is l_n.

Step2 Issuer selects a random born member g' of QR_N.

Step3 Issuer selects random integers: $z_0, z_1, z_y, z_s, z_h, z_g \in \left[1, p'q'\right]$, and use the following random integers to calculate.

$$g := g^{'z_g} modn \tag{1}$$

$$h := g^{'z_h} modn \tag{2}$$

$$S := h^{z_s}\ \ mod\ \ n \tag{3}$$

$$Y := h^{z_y} modn \tag{4}$$

$$R_0 := S^{z_0} modn \tag{5}$$

$$R_1 := S^{z_1} modn \tag{6}$$

Step4 Provides a non-interactive zero-knowledge proof that g, h, S, Y, R_0, R_1 produced by the publisher are all correctly calculated.

Step5 Issuer select a prime number plant of length $l_{\text{“}}$ and a prime number ρ of length l_ρ. Where, $\text{“} = r\rho + 1$. Randomly select a number $\gamma' \in_R \mathrm{Z}^*_{\text{“}}$, then $\gamma^{'(\text{“}-1)/\rho} \neq 1\mathrm{mod}\text{“}$. Where

$$\gamma := \gamma^{'(\text{“}-1)/\rho}\mathrm{mod}\text{“} \tag{7}$$

Step6 Issuer put $\left(n, g', g, h, S, Y, R_0, R, \gamma, \text{“}, \rho\right)$ as the member authentication public key K_{PG} and keep $p'q'$ as the member issuing private key K_{MIPK} secret.

Issuer sends the member authentication public key K_{PG} to the Verifier. The Verifier will use K_{PG} to authenticate the anonymous user's identity in subsequent steps. Users join the user group created by Issuer. Members of the group created by Issuer are also physical nodes in the blockchain network. In order to join the blockchain network, users must register with Issuer to obtain an identity certificate. In order to join the user group created by Issuer, the user first sends a request to Issuer that contains some identity information about the user. If Issuer verifies the user's information and determines that the user is ready to join the user group, then the following steps will be taken to issue the user with an identity certificate.

After obtaining the DAA certificate, the user joins the blockchain network, and then the user generates the user's blockchain transaction key pair (tran_pub, tran_pri). Users anonymously prove their membership to Verifer. Users have joined the cluster created by Issuer in the steps above, which means joining the blockchain network and becoming a node in the blockchain network. The user then needs to prove to the Verifier that he or she is a legitimate member of the group and remains anonymous to the Verifer during the authentication process. The specific steps are as follows.

Step 1 First, the user makes an anonymous authentication request to the Verifier.

Step 2Verifer receives an anonymous authentication request from the user and returns a response to the user. The response contains the Verifier's base name bsn_V and a message *m*.

Step 3 User uses 2. 1. The identity certificate $\left(A, e, v''\right)$ obtained in section 3 generates the knowledge signature σ for the message *m*

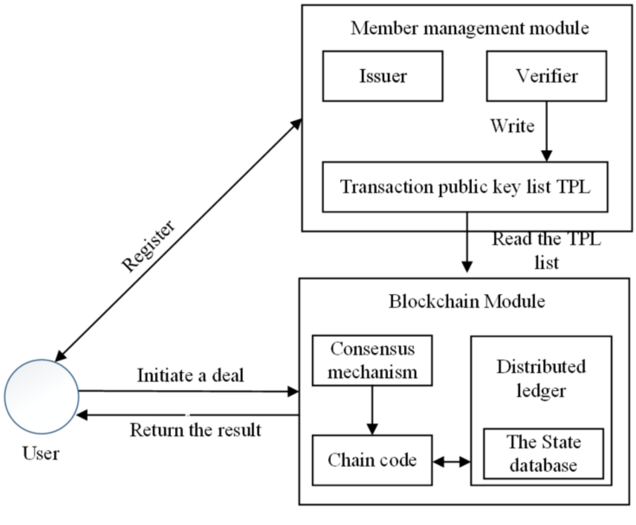
Step 4 Verifer verifies that signature σ is valid, if Verifier verifies it. If it is valid, a symmetric key PSK that is shared with the user will be generated and transmitted to the user who initiated the anonymous authentication request in a secure manner.

The user registers the trading public key tran_pub in the trading public key list TPL. After anonymously proving to the Verifier that he is a valid member of the group, the user must add his trade public key, tran_pub, to the list of trade public keys maintained by the Verifier, TPL. Only then can the consensus mechanism treat the user-generated transaction as legitimate when it is processed. Only through this transaction can the user complete the reading or updating of the distributed ledger.

The data owner generates a corresponding data permission state for each logistics user's privacy data in the distributed ledger according to its own will, and the data permission state determines the access authority of each data accessor. The data accessor must construct a transaction to access the distributed ledger through the application program to determine whether he has the right to access the corresponding logistics user privacy data. If you have access, you can obtain the corresponding ESK storage path and the cloud storage path corresponding to the private data ciphertext through the distributed ledger. At the same time, the traceability of privacy data access records can be realized by recording the data accessor's access records of the logistics user's privacy data on the blockchain. The specific framework is shown in Figure 2.

Among them, the block chain module is established based on Hyperledger Fabric and consists of consensus mechanism, distributed ledger and chain code. Consensus mechanism is responsible for verifying the sequence and legality of a batch of unconfirmed transactions. The consensus mechanism will control the access rights of the blockchain nodes according to the TPL maintained by the Verifier in the member management module. The distributed ledger records information about all transactions in the blockchain network. The state database holds the latest State of ledger data. The chain code encapsulates the business logic between the data owner, the data accessor and the logistics user's private data.

Figure 2. The overall architecture of access rights management mechanism



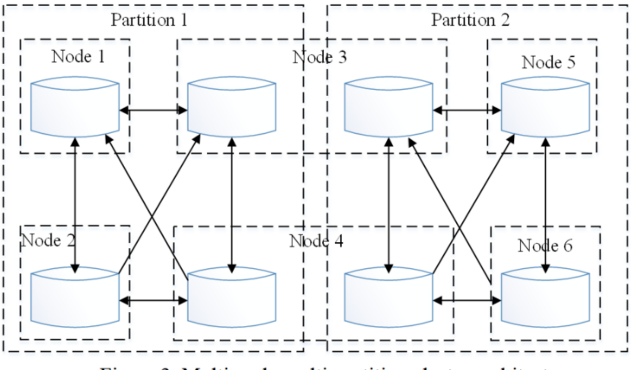
Blockchain modules handle user-generated transactions in the blockchain network. The consensus mechanism in the node determines whether an unprocessed transaction is valid or not. And determine whether the transaction public key tran_pub corresponding to the unprocessed transaction exists in the TPL of the transaction public key list maintained by the Verifier. If the transaction is valid, then the transaction interacts with the distributed ledger by calling the appropriate method in the chain code.

2.2. Inter-chain Privacy Protection

2.2.1 Frame Design

In order to solve the problems of low efficiency of privacy protection and complex authority control in the alliance chain, an inter-chain privacy protection method based on data isolation is proposed in this paper. This method realizes the business-level privacy protection by partitioning and isolating the different business flows of nodes, and eliminates the time-consuming data encryption and decryption process. Through the partition manager NSM (Namespace Manager) to achieve strict partition rights management. The proposed partition isolation method greatly improves the speed of parallel processing of multiple business flows, greatly reduces the deployment difficulty of multi-business flow scenarios, and improves the scalability of the blockchain platform. The following diagram shows the architecture of multi-node multi-partition cluster with inter-chain privacy protection.

Figure 3. Multi-node multi-partition cluster architecture



This article refers to a business flow network as a partition. Each partition is jointly maintained by a variable set of namespace participants. Every time a node participates in a new business, a new partition needs to be created. All nodes participate in global partitions by default at the initial startup for the management of the whole node and the extension of blockchain functionality. Figure 1 shows an architectural diagram of a node cluster with multiple partitions.

2.2.2 Partition Management

The partition manager NSM is the core of inter-chain privacy protection, which ensures the split execution and isolated storage of data between different partitions, and realizes the parallel processing of single node and multiple services. A blockchain node usually consists of a network layer, a consensus layer, an execution layer and a storage layer, before the introduction of NSM. Since a single node only needs to process the transaction request of one business partition, a high degree of coupling between each layer does not affect the distribution and processing of transactions. After the introduction of

NSM, in order to achieve the shunt processing of transactions, each module needs to be decoupled, and the main module is transformed from node level to partition level. A partition can be thought of as a virtual blockchain network, so a partition consists of the four modules described above. All partitions can handle the transaction requests within their own partitions separately, have their own transaction sequencing mechanism and execution engine, and distribute the transaction requests uniformly by NSM. At the same time, in order to improve the reuse of the underlying network, the same set of physical network is shared between different partitions.

The transaction processing process of partitioned consensus has two more steps than the traditional transaction processing process. First, the RPC interface layer resolves the partition ID, and second, the partition manager NSM transacts according to the partition ID. After NSM has shunted the transaction, the processing logic inside the partition is the same as the original solution and does not change. Because these two steps can ignore the time difference, the time complexity of the whole partition consensus transaction processing process is almost the same as that of the traditional transaction processing process. At the same time, in the reconstruction process of partitioning consensus scheme, each module in the system needs to be decoupled, so that the call logic between modules becomes clearer. Therefore, compared with the traditional solution, the reconstructed partition consensus scheme has a certain optimization in processing logic, and the system performance will also be improved to a certain extent.

2.3 Intra-chain Privacy Protection

2.3.1 Framework Settings

Inter-chain privacy protection is usually applicable to the scenarios where each participant in the alliance chain has multiple complex business flows, but not all privacy data requests need to be completed by creating new partitions. On the one hand, simple privacy requirements, such as multiple privacy certificates, only need one or several privacy transaction requests to be completed. Creating a separate partition for each of these small data volumes and small transaction frequency privacy requirements would be a more resource-intensive approach. On the other hand, there are many privacy requirements within a business partition.

In order to solve the above problems, this section proposes the intra-chain privacy protection methods. All blockchain nodes need to maintain two ledger information in each partition, namely the public data ledger and the private data ledger. This method realizes the privacy protection of intra-partition transaction level and contract level. By specifying the participant information (collection) of the privacy transaction inside the transaction body, the user can select any legal subset of the partitioned participant as the participant of the privacy certificate or privacy contract, and initiate the privacy transaction to the blockchain platform through the construction of a double-signed transaction by the client. The blockchain node receiving the privacy transaction acts as the transit node, synchronizes the privacy data to all the privacy participants, constructs the public transaction and carries out the whole network consensus within the partition. After the public transaction is finally synchronized to the partitioned participant node, the privacy participant node updates the privacy ledger separately. The method ensures the synchronization of private data through transit nodes, prevents the leakage of private data, and achieves a more flexible transaction level privacy protection.

2.3.2 List of Privacy Participants

In order to achieve fine-grained privacy protection at the transaction level, a private transaction must support a flexible collection of information from the list of private participants. Therefore, the collection field can be embedded in the extra field as additional information of the privacy transaction, which will eventually be included in the calculation of the signature of the privacy transaction. It should be noted that for the privacy depository scenario, each privacy depository may have a different list of participants, that is, each privacy depository transaction request must specify the privacy participant information. For the privacy contract scenario, each privacy contract determines the list of participants in the privacy contract when the contract is deployed. Therefore, the client does not need to specify the participant information of the privacy contract again in the subsequent contract invocation, upgrade and other operations.

For both the privacy transaction deposit scenario and the privacy contract scenario, the privacy data required to be protected is recorded in the payload field of the transaction. Therefore, the main purpose of transaction-level privacy is the protection of the Payload field. In this paper, the SHA3 encrypted hash function is selected to calculate the hash value of Payload raw data, and the hash value is used to replace Payload raw data to construct a public transaction to avoid the leakage of privacy raw data. The payload field is also embedded in the Extra field to integrate the privacy-related data segments. In the privacy transaction, the portion of the original Payload field is always empty.

2.3.3 Transfer Node

In this paper, the block chain node directly connected with the client is defined as a transit node, which is also the first block chain node to receive privacy transactions and is responsible for the synchronization of privacy transactions. The specific workflow of the transit node is as follows. After receiving a privacy transaction request from the client, the transit node first checks whether the signature information of the privacy transaction is legal, and rejects the transaction with illegal signature. For legally signed transactions, the transit node needs to check whether it belongs to the list of privacy participants specified by the transaction, and the transit node only accepts the privacy transactions that it participates in. For the privacy transaction passed by the authority check, the transit node will send it to the privacy transaction manager PTM for privacy data synchronization. After confirming the completion of private data synchronization, the transit node notifies the client of the successful synchronization result, and the client constructs a new public transaction, which is sent to the current partition of the consensus network to carry out the on-chain process of normal public transaction.

In the inter-chain privacy design approach, each partition has a separate partition ledger. Therefore, each node maintains multiple partition ledgers, each of which records the block information and status information of its respective partition. Similarly, privacy transaction will also cause the change of privacy state, and each privacy contract also has its corresponding privacy state to be maintained. Therefore, each partition also needs to maintain a privacy ledger, which records the privacy block information and privacy status information.

3. EXPERIMENT

3.1 Experimental Environment

In this experiment, 6 machines deployed with Hyperchain nodes are used as servers to simulate 6 institutions participating in multiple businesses, and a test machine is used as a client to send simulated transactions to blockchain nodes. Accordingly, as a contrast, each server is also prepared to add privacy protection features of the transformation of Hyperchain nodes. For simplicity, network partitioning scenarios are not simulated between the client and the blockchain node. The test machine can connect all nodes at the same time. The configuration of all machines is consistent, as shown in Table 1.

3.2 Safety Analysis

In the member identity management module, DAA is mainly used for anonymous authentication, and its security mainly includes the confidentiality of privacy key, anonymity, and unforgability of signature. In the whole scheme, TPM always proves that TPM has the privacy key in the form of zero-knowledge proof, which ensures the absolute privacy of the privacy key. In the signature protocol phase, the Host first blindes the trust certificate $\left(A, e, v''\right)$ sent by Issuer. It then uses the message M to generate a knowledge signature σ to send to the Verifier, so that no identical messages exist

Table 1. The configuration table of test machine

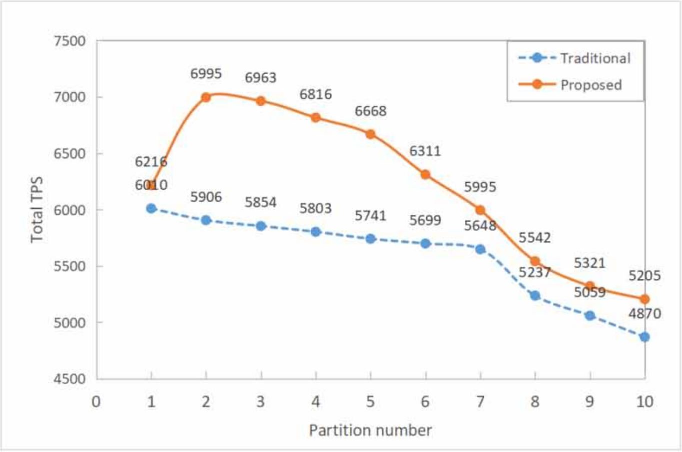
Configure	Specific information
OS	CentOS 8.3.2011
CPU	Intel(R) Core i7 @ 3.06GHz
Network card	Intel Corporation Intel(R) Ethernet Connection (7) I219-V
Memory	32G
The hard disk	256G SSD, 1024G HDD

between the Verifer and Issuer. Even if the Verifer and Issuer colluded, they were unable to identify the specific TPM, preventing the Verifier and Issuer from colluding. Therefore, the anonymity of the platform can be realized to ensure the privacy of the platform.

3.3 Inter-chain Privacy Protection Test

Figure 4 shows the comparison of total performance values of single node processing from the point of view of blockchain nodes. As can be seen from Figure 4, the total processing performance of proposed approach is about 10% to 15% better than traditional approach. After using the partitioning consensus feature, the performance of two partitions is significantly better than that of one partition. The main reason is that in the multi-platform deployment approach, each additional service requires an additional set of blockchain platforms to be deployed, for which several network port resources need to be enabled separately. In the partitioning consensus approach, the underlying network resources are shared between all partitions. Therefore, no matter how many partitions a single node participates in, it only needs to start one network port resource, which greatly reduces the consumption of network resources. Compared to traditional approach, the proposed partitioned consensus approach provides significant performance improvements while ensuring correctness and integrity.

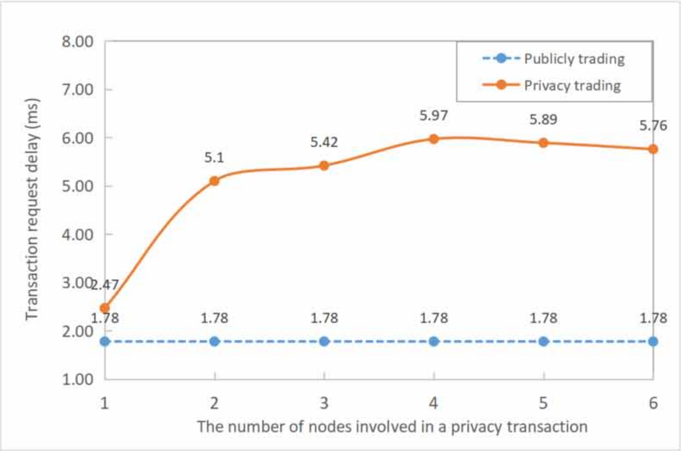
Figure 4. Performance comparison of single node



3.4 Intra-chain Privacy Protection Test

Because the intra-chain privacy protection method mainly faces the privacy protection requirements of small data volume and small groups, the method focuses on the delay of privacy transaction rather than the throughput. In the case of 6 nodes, this paper sets 1 to 6 nodes as privacy participants respectively, and tests the delay of privacy transaction request and privacy transaction receipt query under different number of participants. Figure 10 shows a comparison graph of privacy request latency.

Figure 5. Comparison of transaction request latency



As you can see from Figure 5, the request latency for all private transactions increased slightly compared to the 1.78ms request latency for normal public transactions. When there is only one participant, the local duration of the private transaction and the private transaction in this scenario is only one more than that in the public transaction scenario. The delay was increased by about 0.69ms. When there are two participants, the transit node needs to synchronize the privacy transaction to the remaining one privacy participant node in addition to its own privacy transaction verification and local persistence. The time spent waiting for the privacy participant node to check, persist locally, and return an acknowledgement message, so the latency increases by about 3.32ms. Subsequently, with the increase of participants, the total time of privacy synchronization was basically stabilized between 5ms and 6ms, and the overall delay time was within the acceptable range of users.

4 CONCLUSION

In order to solve the problem of privacy protection in logistics big data system, a logistics big data privacy protection scheme based on block chain is proposed. The concrete work of this paper includes the following three points. (1) An access rights management mechanism based on the combination of block chain and direct anonymous proof technology is proposed, to solve the problem of users' lack of control over logistics privacy data. Access control of blockchain nodes is realized by maintaining a list of transaction public keys, which solves the risk of privacy leakage existing in the current blockchain technology. (2) The privacy and confidentiality protection between different businesses is realized by dividing the data of different businesses and storing them in partitions. (3) Specify participants of the intra-chain private data by embedding fields in the transaction body. The blockchain node receiving the transaction is used as the transmission node to synchronize the intra-chain privacy data, thus improving the in-chain privacy protection within the service. The experimental results show that the proposed method not only meets the privacy requirements, but also ensures considerable performance, which makes a contribution to the privacy and security of the blockchain platform.

DATA AVAILABILITY STATEMENT

The labeled dataset used to support the findings of this study are available from the corresponding author upon request.

CONFLICT OF INTEREST

The author declares no competing interests.

REFERENCES

Ahmad, R. W., Hasan, H., Jayaraman, R., Salah, K., & Omar, M. (2021). Blockchain applications and architectures for port operations and logistics management. *Research in Transportation Business & Management*, *41*, 100620. doi:10.1016/j.rtbm.2021.100620

Bünz, B., Agrawal, S., & Zamani, M. (2020). Zether: Towards privacy in a smart contract world. In *International Conference on Financial Cryptography and Data Security*. Springer.

Chen, E., Ye, A., & Miao, F. (2019). Design of Secure Enhanced Privacy Protection Electronic Hotel-card Based on QR Code. *IOP Conference Series: Materials Science and Engineering, 565*(1), 012006.

Fan, K., Wang, S., Ren, Y., Li, H., & Yang, Y. (2018). Medblock: Efficient and secure medical data sharing via blockchain. *Journal of Medical Systems*, *42*(8), 1–11. doi:10.1007/s10916-018-0993-7 PMID:29931655

Feng, H. (2021). Application of QR Code Technology in the Design of User Information Privacy Protection Logistics System. *International Journal of Frontiers in Engineering Technology*, *3*(3).

Feng, Q., He, D., Zeadally, S., Khan, M. K., & Kumar, N. (2019). A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications*, *126*, 45–58. doi:10.1016/j.jnca.2018.10.020

Li, T., Zhang, R., & Zhang, Y. (2016). Priexpress: Privacy-preserving express delivery with fine-grained attribute-based access control. In *2016 IEEE Conference on Communications and Network Security (CNS).* IEEE.

Liu, X., Hu, B., & Zhou, Q. (2016). A Logistics Privacy Protection System Based on Cloud Computing. In *International Conference on Frontier Computing*. Springer.

Mohammadinejad, H., & Mohammadhoseini, F. (2020). Privacy Protection in Smart Cities by a Personal Data Management Protocol in Blockchain. *International Journal of Computer Network & Information Security*, *12*(3), 44–52. doi:10.5815/ijcnis.2020.03.05

Patel, V. (2019). A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Informatics Journal*, *25*(4), 1398–1411. doi:10.1177/1460458218769699 PMID:29692204

Qian, W., Chen, W., & Xingyi, L. (2014). Express information privacy protection application based on RSA. *Dianzi Jishu Yingyong*, *40*(7), 58–60.

Rivero-García, A., Santos-González, I., Caballero-Gil, C., Molina-Gil, J., Hernández-Goya, C., & Caballero-Gil, P. (2019). Blockchain-based ubiquitous transport and logistics monitoring system. *Multidisciplinary Digital Publishing Institute Proceedings.*, *31*(1), 9. doi:10.3390/proceedings2019031009

Zhang, X., Li, H., & Yang, Y. (2016). LIPPS: Logistics information privacy protection system based on encrypted QR code. In 2016 IEEE Trustcom/BigDataSE/ISPA. IEEE.

Zhao, Y., & Zhang, Y. (2019). Safety Protection of E-Commerce Logistics Information Data Under The Background Of Big Data. *International Journal of Network Security*, *21*(1), 160–165.

Zyskind, G., & Nathan, O. (2015). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops. IEEE.

Huabin Duan received the B.S. degrees at the school of Computer Science and Technology, Central China Normal University, Wuhan, China, in 2003, and the M.S. degree in computer application from Central South University, Changsha, China, in 2008. She worked in Hunan University of science and technology in 2003. Her research interests include network security, database application and big data analysis.

Yang Jie was born in 1976. He is a professorat Hunan University of Science and Engineering. His research interests include network security and artificial intelligence.

Huanjun Yang was born in 1979. He is an experimentalist at Hunan University of Science and Engineering. His research interests include network security and artificial intelligence.