International Journal of Digital Crime and Forensics
Volume 14 • Issue 2

A Privacy Protection Scheme for Cross-Chain Transactions Based on Group Signature and Relay Chain

Xiubo Liang, Zhejiang University, China
Yu Zhao, Zhejiang University, China
Junhan Wu, Zhejiang University, China
Keting Yin, Zhejiang University, China*

ABSTRACT

Recently, with the rapid development of blockchain technology, the information interaction and value transfer problems between different blockchains have become the focus of research. The cross-chain technology is to solve the cross-chain operation problems of assets and data between different chains. However, the existing cross-chain technology has the problem of identity privacy leakage. Therefore, this article proposes a cross-chain privacy protection scheme for consortium blockchains based on group signature, certificate authority, and relay chain. The scheme is divided into three cross-chain service layers, called the management layer, the transaction layer, and the group layer. The management layer is responsible for the forwarding of cross-chain transactions, the transaction layer includes the blockchains that actually participate in cross-chain transactions, and the group layer is responsible for group signature related work. Through this scheme, the identity privacy of both parties to the transaction can be protected during the cross-chain transaction process.

KEYWORDS

Anonymity, Blockchain, Certificate Authority, Cross-Chain, Group Signature, Identity Privacy, Relay Chain, Supervisable

INTRODUCTION

The blockchain proposed by Satoshi Nakamoto(Nakamoto, 2008) in 2008 is a distributed chained data structure, which has many advantages such as decentralization, non-tampering and non-forgeability, and is considered to be the future of financial service infrastructure(Huang, Li, Lai, & Chen, 2017). According to the number of central nodes or privileged nodes, the blockchain can be divided into three categories, namely public blockchain, consortium blockchain and private blockchain(Peters, & Panayi, 2016). The public blockchain is completely decentralized, which allows any node to obtain data and process transactions on the blockchain. However, consortium blockchain and private blockchain need to be authorized and verified by at least one organization before nodes can join. The consortium blockchain has the advantage of fast transaction processing, so it is widely used in cultural relics traceability(Liang, Zhang, Gu, Chen, Zhang, & Liu, 2020), medical data sharing(Shahna, Qamar, & Khalid, 2019), educational data sharing(Liang, Zhao, Zhang, Liu, & Zhang, 2020), etc.

However, the blockchain systems and operating mechanisms are various from different application scenarios. This phenomenon leads to the isolation of block information in different blockchains,

DOI: 10.4018/IJDCF.302876 *Corresponding Author

resulting in the islanding effect of the blockchain("Mauve Paper Vitalik", n.d.). Therefore, how to exchange information and value across different blockchains has become the focus of research. In 2012, the InterLedger protocol was proposed to solve the coordination problem between different blockchain systems(Hope-Bailie, & Thomas, 2016). Since then, cross-chain technology has developed rapidly. Cross-chain technology aims to link independent blockchains and carries the value exchange function of different value system blockchains. Herlihy proposed hash-locking mode(Herlihy, 2018) in 2013. BlockStream proposed sidechain (Asgaonkar, & Krishnamachari, 2019) in 2014. In 2016, BTC-Relay proposed a relay-chain solution (Chow, 2016), which has become the mainstream cross-chain technology. In addition, technologies such as the off-chain payment channel of the Lightning Network at the layer-2 level(Poon, & Dryja, 2016) and the decentralized autonomous incentives in Plasma(Poon, & Buterin, 2017) are also worthy of attention. The architecture proposed in this paper uses the relay-chain scheme.

Blockchain ledger is open and transparent, so privacy protection has become a challenge. Unlike within-chain transactions only in one system, cross-chain will inevitably cause two systems to interact and affect each other. According to atomic transfer(Hope-Bailie, & Thomas, 2016), a problem with the cross-chain information of a chain will affect the entire cross-chain network. Recently, there have been many attacks on cross-chain transactions. In July 2021, due to the theft of the administrator's private key, the cross-chain project AnySwap was hacked and lost more than 8 million dollars. In August 2021, Poly Network, a cross-chain interoperability protocol, was attacked by hackers and lost more than 600 million dollars. It can be seen that the cross-chain security situation is very urgent. Therefore, how to ensure system security and protect privacy in the process of cross-chain transactions is a question worth considering.

In the blockchain, privacy issues are mainly divided into two categories: identity privacy and data privacy(Zhu, Gao, Shen, Li, Zheng, Mao, & Wu, 2017). This paper discusses the issue of identity privacy in the cross-chain process, that is, users hope that the public data content stored on the blockchain cannot obtain any useful information related to their identity. The identity privacy of cross-chain transactions is fundamentally different from that of within-chain transactions. Identity privacy refers to the association between user identity information and blockchain addresses. However, different blockchains have their own addresses to represent identity information. Therefore, cross-chain privacy protection must first solve the intercommunication of different blockchains' identity information.

Main contributions of this work are summarized as follows:

1. This paper has unified the identity information of nodes on different blockchains through a centralized CA organization.
2. This paper improves a group signature algorithm, and uses the improved group signature algorithm to realize the concealment of the identity information of both parties in the cross-chain transaction from the nodes that do not participate in the cross-chain transaction, thereby protecting identity privacy.
3. This paper applies the relay chain, the CA and the group signature technology through a three-layer architecture. The three layers are the management layer, the transaction layer, and the group layer.
4. Through the relay chain, a cross-chain transaction process similar to the handshake mechanism is realized in this paper.

The rest of this paper is organized by the following order: Section 2 discusses related work. Section 3 describes three layers, security model, transaction model and the specific process of cross-chain transaction of our system. Section 4 analyzes the safety and the performance evaluation of our system. Section 5 summarizes the whole paper and discusses the future work.

RELATED WORK

Due to the unique multi-level architecture of the relay chain technology, it has shown advantages in cross-chain interoperability. With the development of cross-chain technology, relay chain technology has become the mainstream. The system proposed in this paper also uses relay chain technology, and combines group signatures and certificate authority to ensure privacy protection during the cross-chain process. This section will clarify the definition of identity privacy and describe the technologies mentioned above.

Identity Privacy

Identity privacy is a very important privacy data on the consortium blockchain. Identity privacy refers to the address information of both parties to the transaction, usually called pseudonyms, and its essence is the hash value of the public keys of both parties. In the early blockchain transactions, transactions in this pseudonymous manner can achieve the purpose of anonymity. Since all transaction data in the blockchain is public, with the development of technology, through statistical analysis of public data, the topology of all transaction data on the network can be constructed. Through the topological structure, the relationship between the two parties in the transaction can be analyzed to a certain extent, and the real information corresponding to the sender and the receiver in the transaction can be analyzed(Reid, & Harrigan, 2013). In actual cross-chain transaction scenarios, different blockchains often have different identity systems. This paper proposes an idealized identity model. First, the nodes on each blockchain are formed into a group through group signature technology, and then a centralized CA organization is used to unify the identities of nodes on different groups.

Relay Chain

The relay chain technology aims to construct a third-party blockchain that connects other blockchains in a system through a cross-chain messaging protocol. The other blockchains are called parachain. The relay chain is connected with other blockchains, forwards cross-chain transactions generated by other chains, and records the transaction status, providing a unified consensus and authority guarantee for the entire system. BTC-Relay(Chow, 2016) realizes one-way cross-chain communication from Bitcoin to Ethereum based on the relay-chain scheme, which has aroused attention to relay-chain technology. In 2017, the cross-chain projects Polkadot(Wood, 2016) and Cosmos(Kwon, & Buchman, 2019) proposed a plan to build a cross-chain platform, which can be compatible with all blockchain applications. Polkadot can achieve interoperability, scalability, and shared security heterogeneous cross-chain protocols. The advantage of Cosmos is that through the IBC protocol and Tendermint(Kwon, 2014), the problem of secure and trusted transmission of cross-chain transactions is solved. These two projects are currently under development. The difference between this paper and other cross-chain projects that use relay chain is that it can protect identity privacy during cross-chain transactions, while other projects mostly solve cross-chain asset transfer and interoperability.

Certificate Authority

Certificate Authority (CA) is an organization trusted by both parties to the transaction, and assumes the responsibility of verifying the legitimacy of public keys in PKI (Perlman, 1999). CA issues, manages, and revokes digital certificates, and manages keys. The digital certificate is actually a record stored on the computer and a statement issued by the CA. The function of the digital certificate is to prove that the user listed in the certificate legally owns the public key listed in the certificate. The digital signature of the CA organization makes it impossible for an attacker to forge and tamper with the certificate. If the user has suffered losses due to trust in the certificate, the certificate can be used as valid evidence to pursue the legal responsibility of the CA. The public key is bound to the user's identity information, and everyone can use the CA's public key to verify the signature on the certificate to determine the authenticity of the certificate (Thompson, Essiari, & Mudumbai, 2003).

In recent years, a new digital identity authentication technology called decentralized identity (DID) has emerged ("A Primer for Decentralized Identifiers", n.d.). Unlike CA, there is no centralized organization to manage identities in DID, which facilitates identity intercommunication. However, in systems using group signatures, DID technology is not conducive to key management and identity supervision, so this paper adopts CA technology.

Group Signature

Chaum(Chaum, & Van, 1991) proposed group signature in 1991. A group signature scheme allows group members to sign messages anonymously on behalf of the group. The group manager can use the group private key to track the group signature generated by the group user and expose the identity of the signer. Jan Camenisch et al. (Camenisch, & Stadler, 1997) proposed a famous group signature scheme CS97. CS97 first realized that the group public key and signature length do not depend on the number of group members, and first used knowledge signatures in the group signature scheme. In 2004, Chen Zewen et al. (Chen et al., 2004) first proposed a group signature scheme based on the Chinese Remainder Theorem. This scheme uses the Chinese Remainder Theorem to quickly revoke or join group members without changing the private keys of other group members. In 2016, Huang Conglin et al. (Huang, Zhong, & Wang, 2016) combined the Chinese Remainder Theorem with the complete subtree method, which reduced the cost of group computing congruence, but increased the space complexity. In 2020, Hong Xuan et al. (Hong, & Zhang, 2020)combined the Chinese Remainder Theorem with the Schnorr digital signature system to propose a forward secure group signature scheme. The system proposed in this paper adopts the group signature scheme proposed by Hong Xuan et al and optimized according to the blockchain system.

COMPARISONS OF CROSS-CHAIN TECHNOLOGIES

This section summarizes several cross-chain technologies mentioned in related work, and analyzes their cryptography and security.

Table 1. Comparisons of cross-chain technologies

Cross-chain technology	Solution	Throughput	Security
BlockStream	Sidechain	Low	Weak
Lightning Network	Off-chain Payment Channel	Low	Weak
BTC-Relay	Relay Chain	High	Weak
Polkadot	Relay Chain	Middle	High
Cosmos	Relay Chain	Middle	High

As is shown in Table 1, BlockStream, Lightning Network and BTC-Relay adopt different cross-chain solutions. BTC-Relay using relay chain technology achieves the highest throughput, but these three technologies do not consider the security of cross-chain transactions. Polkadot and Cosmos use relay chain technology and cryptography to protect identity privacy and data privacy in cross-chain transactions, but limit transaction throughput. This paper aims to propose a scheme that balances security and throughput.

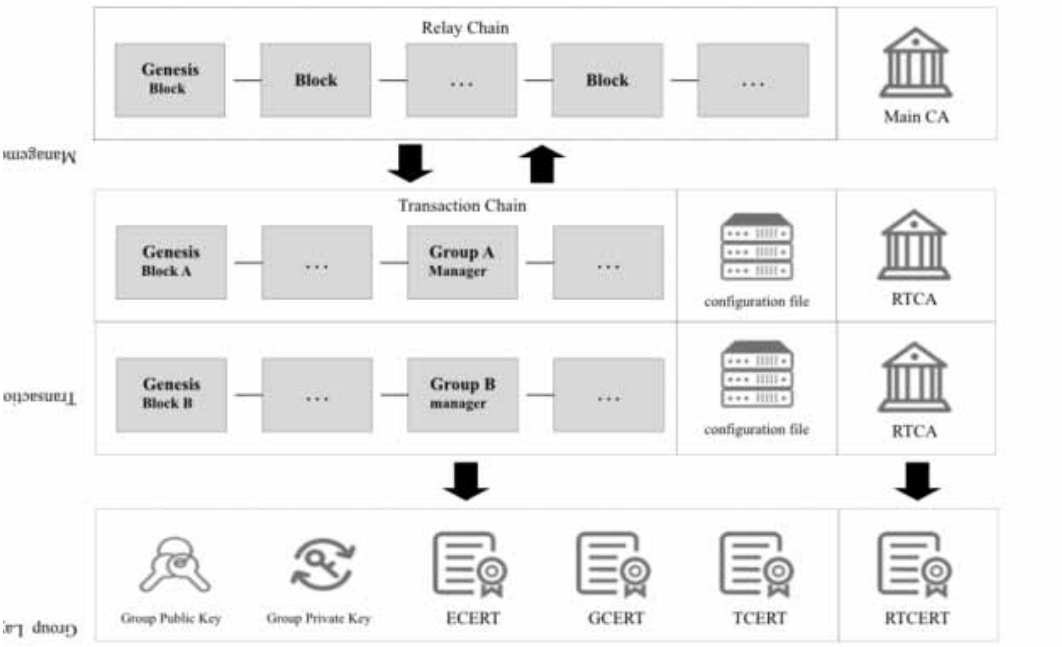
SYSTEM MODEL

This paper proposes a homogeneous blockchain(Shen, Zhu, & Xu, 2020) cross-chain system based on the relay chain. The system is a three-layer hierarchical structure using group signatures and CA, which can effectively protect users' identity privacy when conducting cross-chain transaction. It is worth mentioning that, this paper implements partial identity anonymity, that is, the user identity is anonymous to other nodes but allows the manager node and the RTCA to verify the legality of the transaction.

Layers

As is shown in Figure 1, considering the functions of relay, transaction and group signature, the system proposes a three-layer structure: the management layer, the transaction layer and the group layer. This section will introduce the function of each layer and the role of the entities in each layer.

Figure 1. System model



Management Layer

The management layer is the core of the system, a specific unit that realizes cross-chain data exchange, and has the highest authority to manage parachains participating in cross-chain transactions. The related entities in the management layer include the relay chain and the main CA. The detailed setting of each entity is analyzed below:

The relay chain coordinates the authority and transaction transfer between each chain, and is mainly responsible for the persistence and routing of cross-chain transactions between transaction chains.

The main CA is responsible for unifying the identities of each nodes and managing the access authentication of the transaction chain. By issuing the CA certificate for the transaction chain, the group manager of the transaction chain holds the CA certificate to access the relay chain. The main CA is also responsible for generating and saving configuration files for each transaction chain.

Transaction Layer

The transaction layer is composed of a number of blockchains that require cross-chain transactions. Any two transaction chains are traded through the relay chain. The related entities in each transaction chain mainly include the group manager node, the Root Certificate Authority (RTCA) and the configuration file. The detailed setting of each entity is analyzed below:

The group manager node and the relay chain constitute the bridge of the entire cross-chain transaction. The group manager node is also a certificate authority. In the transaction layer, the group manager node is responsible for applying to the main CA for access to the relay chain, verifying the cross-chain transaction application of other nodes, and selecting a trusted third-party institution as the RTCA.

The RTCA is the Root Certificate Authority, which is selected by the group manager node. The RTCA generates the RTCERT of the transaction chain and issues a sub-RTCERT to each node of the transaction chain according to RTCERT. The RTCERT is the root certificate of a transaction chain, and the sub-RTCERT can indicate which transaction chain the node belongs to. The RTCA writes the RTCERT and sub-RTCERT into the configuration file. At the same time, the RTCA also acts as the supervisory authority of the transaction chain, which will obtain the group private key generated by the group manager node.

The configuration file is generated by the main CA for each transaction chain. When a transaction chain is generated, the main CA selects a trusted institution as the group manager node, and writes the information and address of the group manager node into the initial configuration file. The group signature generation algorithm is also recorded in the initial configuration file. After that, RTCA has the authority to modify the configuration file and send the modified configuration file to the main CA. The RTCA saves the configuration files of its own transaction chain, and the main CA saves the configuration files of all transaction chains.

Group Layer

The group layer is responsible for specific tasks related to group signature and certificate issuance. The related entities in the group layer include the group manager node, the group public and private keys and some digital certificates.

In the group layer, the main function of the group manager node is to generate the group public and private keys of the group signature. The group public key is open to all users in the entire system. The group private key will be sent to RTCA by the group manager node, so that the group manager node and RTCA can verify the signer of the group signature.

The group manager node is also responsible for generating some digital certificates, these certificates include the Transaction Certificate (TCERT), the Enrollment Certificate (ECERT), the Group Certificate (GCERT). The detailed setting of these digital certificates will be introduced below.

Security Model

The security model of this system is mainly embodied at the group level. This security model protects the user's identity privacy by group signature algorithm and using CA to manage authority. This paper adopts the group signature scheme proposed by Hong Xuan et al. (Hong, & Zhang, 2020) and optimizes it according to the cross-chain model. In this part, we introduce some main functionalities of the security model in detail: (i) Root certificate generation, (ii) Group public and private key generation, (iii) The main CA unified identity, (iv) Access certificate issuance, (v) Group signature generation, (vi) Group signature verification and (vii) Group signature supervision.

Root Certificate Generation

When the transaction chain is created, each member in the chain designates a node as the group manager node through a configuration file. Then the group manager node selects a trusted third-party organization as the RTCA, and then RTCA acts as the supervisory authority and root certification authority of the transaction chain.

The group signature algorithm is also recorded in the initial configuration file. Assume that the initial transaction chain has k nodes, that is, there are k group members $U_i\left(i=1,2,\ldots,k\right)$. The group manager node selects a public hash function $H:\left\{0,1\right\}^{*}\rightarrow\left\{0,1\right\}^{k}$. In the literature [26], g is the generator of all large prime number cyclic groups $Z_{p_i}^{*}$ and the structure is complicated. This paper gives a simple scheme. The group manager node selects two large prime numbers p and q, and satisfies $\left(p-1\right)/2$ and $\left(q-1\right)/2$ are also large prime numbers, and calculates $n=pq$. Let g_p and g_q be generators of cyclic groups Z_p^{*} and Z_q^{*}, respectively, and construct the following congruence equations:

$$g\equiv\begin{cases}g_p \bmod p\\ g_q \bmod q\end{cases} \tag{1}$$

The group manager node selects $x\in Z_n^{*}$, and calculates $y\equiv g^x \bmod p$. The group manager node uses $\left(x,p,q\right)$ as the group private key and sends it to RTCA. The RTCA generates the RTCERT of the transaction chain according to the group private key and y. The RTCA organization issues a sub-RTCERT to each member of the transaction chain according to RTCERT, and writes the sub-RTCERT into the configuration file of the transaction chain. The updated configuration file is sent to the main CA by RTCA. The sub-RTCERT generated by the third-party institution RTCA and the information of the group manager node will be packaged into a transaction and broadcast on the whole transaction chain, and finally reach a consensus.

Group Public and Private Key Generation

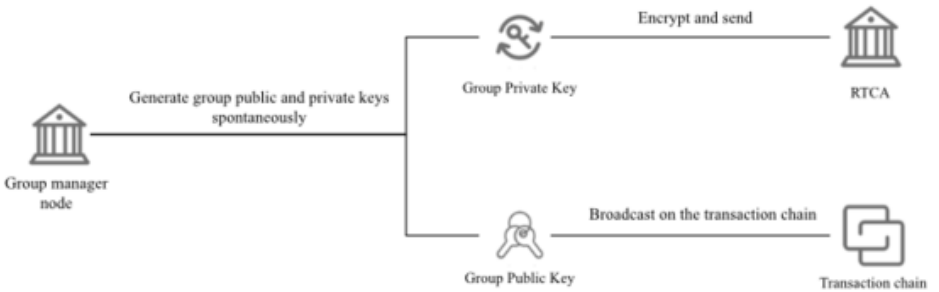
As shown in Figure 2, the group manager node generates the group public key and the group private key of the group signature. The behavior of the group manager node to generate the public and private keys of the group is spontaneous after the transaction chain is created.

From the above content, $\left(x,p,q\right)$ is the group private key. According to the literature [26], the group manager node randomly selects a large prime number $p_i\in Z_P^{*}$ for each group member U_i, and when $i\neq j, pi\neq pj$. Then each group member U_i randomly selects his private key $x_i\in Z_n^{*}$, calculates his public key $y_i\equiv g^{x_i} \bmod p_i$, and sends his identity information and his public key $\left(ID_i,y_i\right)$ to the group manager node on the transaction chain. Then the group manager node saves $\left(ID_i,y_i\right)$ to the configuration file. Using the Chinese Remainder Theorem, the solution of the system of congruence equations $c\equiv y_i \bmod p_i,\left(i=1,2,\ldots,k\right)$ can be found as:

$$c\equiv\ y_1P_1^{'}P_1+\ y_2P_2^{'}P_2+\ldots+\ y_kP_k^{'}P_k\left(mod\ P\right) \tag{2}$$

Where $P = p_1 p_2 \ldots p_k; P_i = \frac{P}{p_i}; P_i P_i^{'} \equiv 1 mod\, p_i, \left(i = 1,2,\ldots,k\right)$. Use $\left(n, y, g, c\right)$ as the group public key. Among them, the group public key is packaged into a transaction, and then the transaction is broadcast in the transaction chain. At the same time, the group private key information is encrypted and packaged into a transaction, and the transaction receiver is the supervisory authority RTCA of the transaction chain, and then the transaction is also broadcast.

Figure 2. Group public and private key generation



The Main CA Unified Identity

In actual cross-chain transaction scenarios, different blockchains usually adopt different identity systems. In this paper, we use the main CA to unify the identity information. We use the same group signature algorithm for each transaction chain, so that each node on each transaction chain has a group public key. However, we cannot use the group public key as the address information of the node.

We use a conventional asymmetric encryption algorithm to generate node address information, that is, identity information. When a new node joins any transaction chain, the main CA will use the asymmetric encryption algorithm to generate a public key and a private key for the node. This pair of public and private keys can be used to encrypt transaction information. The main CA guarantees that the public and private key pairs of each node are different. At this time, the public key of each node can be used as the node's address information, that is, identity information.

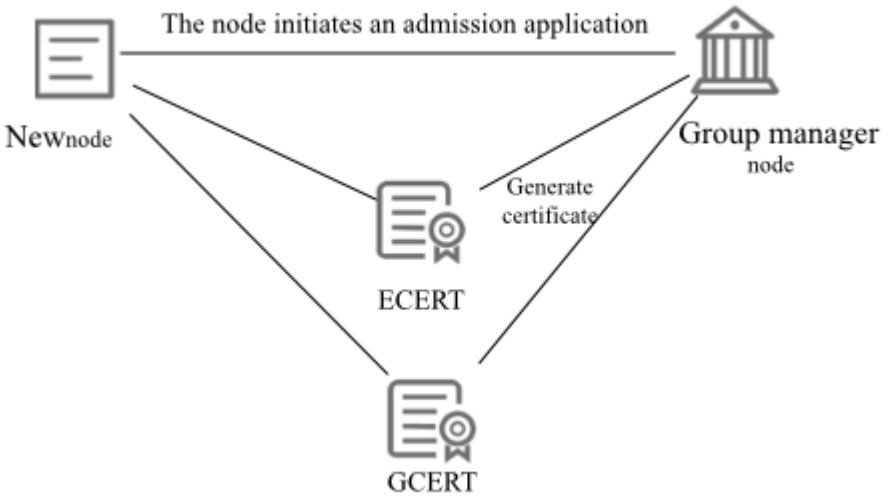
Access Certificate Issuance

As shown in Figure 3, for a node that needs to join a transaction chain, the node initiates an admission transaction to the group manager node of the transaction chain, and the admission transaction contains the necessary identity information ID_{k+1}. After the group manager node verifies the identity information provided by the node, it chooses a new large prime number p_{k+1} and sends it to the node. In Hong Xuan's scheme(Hong, & Zhang, 2020), it is necessary to ensure that g is the generator of $Z_{P_{k+1}}^{*}$, and there is a risk of re-selecting p_{k+1}. In this scheme, it is only necessary to satisfy $p_{k+1} \in Z_p^{*}$. Then the node randomly selects his private key $x_{k+1} \in Z_n^{*}$, calculates his public key $y_{k+1} \equiv g^{x_{k+1}} mod\, p_{k+1}$, and sends his identity information and his public key $\left(ID_i, y_i\right)$. to the group manager node. Then

the group manager node recalculates c and broadcasts it in the blockchain using the Chinese remainder theorem. In this process, the public and private keys of other nodes are not changed.

The group manager node issues an ECERT to the node based on his public and private keys. While dispatching the ECERT, the group manager node issues a GCERT to the node. In this system, all nodes and clients need to apply for a unique identity identification ECERT; all nodes will be required to provide identity information of a specified structure when applying for an access certificate ECERT, and a unified identity verification model is adopted. When the group manager node generates GCERT for the node, it needs to bind the ECERT generated for the node and the group public key to generate it to ensure that the GCERT contains identity information that can be verified by the group private key.

Figure 3. The process of access certificate issuance



Group Signature Generation

Suppose that the node U_i on the transaction chain wants to sign a message m. U_i selects the random number $r \in Z_n^*$ and calculates $s_1 \equiv g^r \bmod p_i$,$s_2 \equiv \left[H\left(m\right)x_i - r\right] mod\left(p_i - 1\right)$, then the effective group signature generated by U_i is $\left(m, p_i, s_1, s_2\right)$.

Group Signature Verification

The steps to verify the group signature $\left(m, p_i, s_1, s_2\right)$ are as follows: First, according to public information, the verifier calculates $y_i \equiv c\left(mod\, p_i\right)$ to get y_i. Second, judge whether the equation $s_1 g^{s_2} \equiv y_i^{2\times H(m)} \bmod p_i$ is correct to verify the validity of the group signature. If it is true, it means that the signature is indeed signed by a legal member of the group; otherwise, the verification fails and the signature is refused to be changed.

Group signature supervision

The group manager node and the RTCA can obtain y_i by calculating $y_i \equiv c\left(mod\, p_i\right)$, and then use the stored node information list $\left(ID_i, y_i\right)$ to obtain the node identity information ID_i, and then determine the specific identity of the signer. At the same time, it is ensured that the identity of the signatory of such message is not known by other members of the system.

Transaction Model

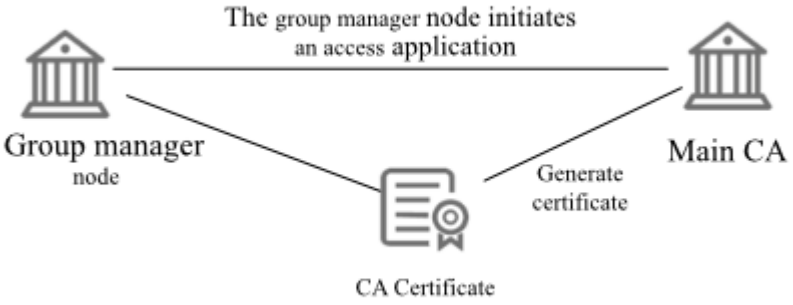
In this part, we introduce some main functionalities of transaction model in detail: (i) Transaction chain access to the relay chain, (ii) Cross-chain transaction application and (iii) Cross-chain transaction processing.

Transaction Chain Access to the Relay Chain

As shown in Figure 4, the group manager node of the transaction chain initiates an access application to the main CA of management layer, and the main CA of management layer determines whether the application access of the transaction chain's group manager node is allowed. After the transaction chain application is approved, the main CA of management layer issues the CA certificate to the group manager node of the transaction chain, and organizes the relevant registration information of the transaction chain into a transaction and publishes it on the relay chain. The transaction includes the address and information of the group manager node of the transaction chain.

In order to achieve a unified consensus among the transaction chains connected to the relay chain, the group manager node of each transaction chain manages the relay chain. Specifically, the manager node of the transaction chain group accesses the relay chain with the obtained CA certificate, and obtains and synchronizes the data of the relay chain. After completion, the group manager node of the transaction chain will share with the relay chain members the data, group public key, public key of each node, the block header information of each node, RTCERT, the address of the group manager node, access requirements, etc. that are permitted to be accessed by the external transaction chains in the blockchain network.

Figure 4. Transaction chain access to the relay chain



Cross-Chain Transaction Application

The node that needs to initiate a transaction in the transaction chain provides the node's ECERT and initiates a TCERT issuance transaction to the group manager node. The group manager node generates the corresponding TCERT by verifying the ECERT and issues the TCERT to the node that wants to initiate a cross-chain transaction. Nodes can apply for TCERT in advance when the transaction is not in progress, and can apply for multiple TCERTs in batches. The node will use the ECERT as the root certificate to issue the TCERT, and the TCERT must contain a certain verifiable identity certificate. After the node applies for TCERT to the group manager node, the group manager node needs to package the application into a transaction and upload the transaction to the relay chain. The process of issuing a certificate on the blockchain does not require the consensus of other nodes, and the group manager node directly uploads the issuance information package transaction on the blockchain.

Cross-Chain Transaction Processing

When a node publishes a cross-chain transaction in the transaction chain, a flag bit must be set in the transaction to identify the cross-chain transaction. At the same time, GCERT is used to sign the transaction and generate a group signature. Finally, the signed transaction is broadcast within the transaction chain. The flag bit of the cross-chain transaction is placed at the head of the transaction as part of the information. It is worth mentioning that when the value of the flag bit is 1, it means that the transaction is a cross-chain transaction, otherwise it is not.

As shown in Figure 6, the group manager node of the transaction chain determines whether it is a legal cross-chain transaction based on the TCERT and the flag bit. If it is, the group private key is used to confirm the identity. After verification, the group manager node will upload the cross-chain transaction to the relay chain.

The group manager node of the transaction acceptor will obtain the transaction on the relay chain and determine whether the transaction is a cross-chain transaction sent to its own transaction chain based on the flag bit and address information. If so, the group manager node will first publish the requested cross-chain transaction information on the transaction chain, and after a node confirms the acceptance of the transaction, the actual cross-chain transaction information will be published on the transaction chain. The specific process of the transaction will be introduced in section 3.4.

Specific Process of Cross-Chain Transaction

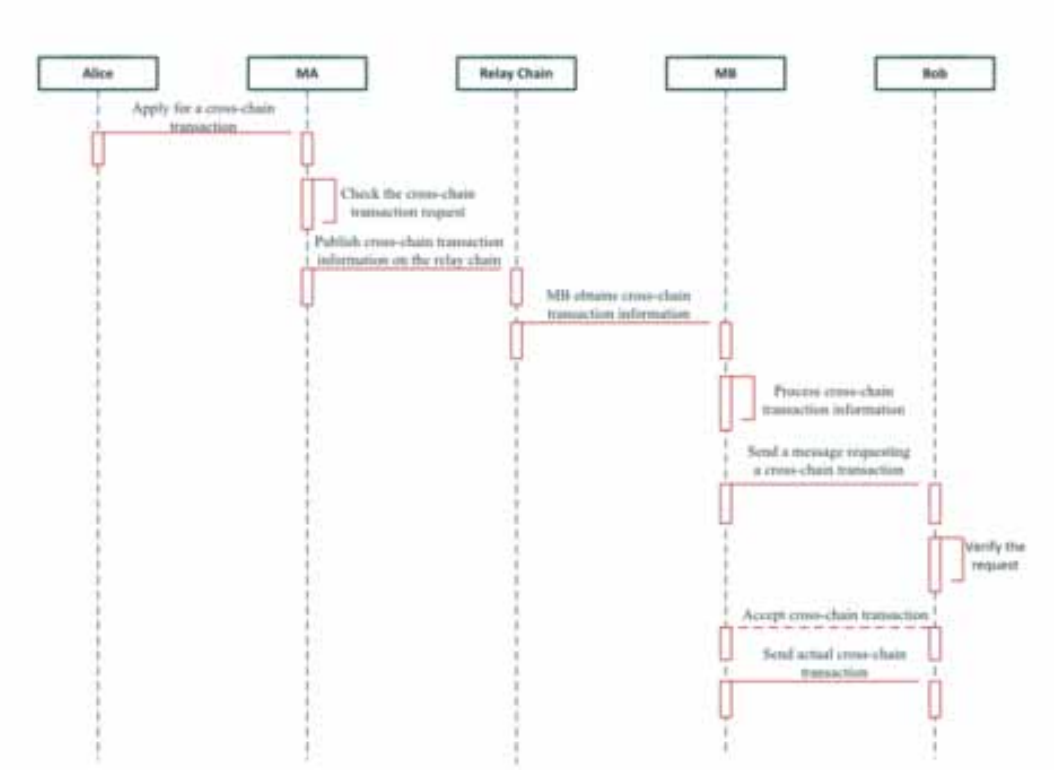
This section will introduce the specific process of cross-chain transactions. For the convenience of description, the steps related to the signature are represented by the symbols in Table 2. In addition, this paper adopts a common asymmetric encryption algorithm for message encryption, which is not explained in this paper.

Table 2. The explanation of some symbols

Symbol	Explanation
Sig	Signature by node using his own public and private keys
Gsig	Group signature by node using group public and private keys
Enc	Encryption by node using its own public and private keys
FlagT	The value is 1, which means a cross-chain transaction
Address	The address of the node on the blockchain
Reqm	Represents a message requesting a cross-chain transaction
Accm	Represents a message accepting a cross-chain transaction
Actm	Actual cross-chain transaction information

Assume that the node that initiates the cross-chain transaction is Alice, the transaction chain where Alice is located is A, and the group manager node of the transaction chain A is MA. Assume that the node that accepts cross-chain transactions is Bob, the transaction chain where Bob is located is B, and the group manager node of transaction chain B is MB. Assume that both Alice and Bob have obtained TCERTs issued by their respective group manager nodes. The cross-chain transaction process is similar to the handshake model in the computer network. The timing diagram of cross-chain transaction is shown in Figure 5:

Figure 5. The timing diagram of cross-chain transaction



Step 1: The node Alice on transaction chain A initiates a cross-chain transaction to Bob on transaction chain B and needs to apply to the group manager node MA. The application information includes the cross-chain transaction flag bit $FlagT$, the group manager node's address of transaction chain B, the request transaction information $Reqm$ and the actual cross-chain transaction information $Actm$ of Alice. First, sign and encrypt $Reqm$ and $Actm$ to get $Enc_{Bob}\left(Sig_{Alice}\left(Reqm\right)\right) || Enc_{Bob}\left(Sig_{Alice}\left(Actm\right)\right)$, and then use GCERT to sign group together with $FlagT$ and $Address_{MB}$ to get:

$$GSig_{Alice}(\mathrm{FlagT}\left\|Address_{MB}\right\| \ Enc_{Bob}\left(Sig_{Alice}\left(Reqm\right)\right) \ || \ Enc_{Bob}\left(Sig_{Alice}\left(Actm\right)\right)) \tag{3}$$

Alice sends Equation (3) to the group manager node MA.

Step 2: After receiving Equation (3), MA uses the group public key to verify the correctness of the group signature and then uses the group private key to know that the signer is Alice, judges that it is a cross-chain transaction through $FlagT$, and then checks the address and transaction information. After all the verifications are passed, MA publishes Equation (3) on the relay chain.

MB receives the relevant information on the relay chain, judges that this is a cross-chain transaction sent from A to B through the group signature and address, and extracts $FlagT$ and the requested cross-chain transaction of Alice, and signs to get:

$$Sig_{MB}(FlagT \,||\, Enc_{Bob}\left(Sig_{Alice}\left(Reqm\right)\right)) \tag{4}$$

MB broadcasts Equation (4) to transaction chain B.

After obtaining Equation (4) on transaction chain B, Bob verifies MB's signature. After verification, Bob uses its private key to decrypt $Enc_{Bob}\left(Sig_{Alice}\left(Reqm\right)\right)$, thus knowing Alice's cross-chain access request and verifying Alice's signature. After confirming that Alice's signature is correct, Bob will sign, encrypt, group signature $FlagT$ and $Accm$ to get:

$$GSig_{Bob}(FlagT \,||\, Enc_{MB}\left(Sig_{Bob}\left(Accm\right)\right)) \tag{5}$$

Bob sends Equation (5) to MB on transaction chain B to indicate that he agrees to accept Alice's cross-chain transaction information.

Step 5: MB receives Equation (5) and uses his private key to decrypt $Enc_{MB}\left(Sig_{Bob}\left(Accm\right)\right)$, thereby verifying Bob's signature and knowing that Bob agrees to accept Alice's cross-chain information, so he signs $FlagT$ and the actual cross-chain transaction of Alice to get:

$$Sig_{MB}(FlagT \,||\, Enc_{Bob}\left(Sig_{Alice}\left(Actm\right)\right)) \tag{6}$$

MB broadcasts Equation (6) to transaction chain B.

Step 6: After obtaining Equation (6) on transaction chain B, Bob verifies MB's signature. After verification, Bob uses its private key to decrypt $Enc_{Bob}\left(Sig_{Alice}\left(Actm\right)\right)$, thus verifying Alice's signature and knowing the actual cross-chain transaction of Alice. This process is regarded as the end of the cross-chain transaction.

SYSTEM ANALYSIS

In this section, to better understand our system, we analyze the safety and the performance evaluation of our system. For security, group signatures and CA are used to protect identity privacy, and relay chains and CAs are used to resist partial attacks during cross-chain. For performance, first analyze and compare the efficiency of group signature algorithms, and then experimentally test the throughput and scalability of cross-chain transactions.

Safety Analysis

The analysis shows that the scheme in this paper satisfies anonymity, unforgeability, and supervisability, and can resist sybil attacks and double-spending attacks. It is worth mentioning that the security of this system depends on the adopted group signature algorithm, but this is the scenario that the system

hopes to meet, that is, by improving the group signature algorithm to improve identity privacy protection in cross-chain transactions. In addition, the use of CA and relay chain also improves the security during the cross-chain process.

Anonymity Analysis

If the group signature is legally generated by the user, it will definitely pass the verification. The verification method is introduced in section 3.2. When other nodes in the system obtain cross-chain transaction information, they can only verify which group formed by the transaction chain the node signing the group signature belongs to in the transaction. Except for the group manager node of the transaction chain and the trusted third-party organization RTCA, no other nodes in the system can verify the identity of the signer. The group signature satisfies non-relevance. For two different group signatures Gsig and Gsig' of the same group, no one can know whether the signature is signed by the same person before the group manager node or RTCA opens it, so anonymity is guaranteed.

Unforgeability Analysis

In this system, if any node on the transaction chain wants to initiate a cross-chain transaction, it needs to apply for TCERT to the group manager node with ECERT, and the node can perform cross-chain transactions with TCERT. The group manager node can verify the true identity of the node that initiated the cross-chain transaction with TCERT. So if an attacker wants to forge a group signature, he can only be a node on the transaction chain where the signer is located.

Consider such an attack model. Suppose there is an attacker who forges the group signatures $\left(m,r_i,h_i,s_i\right)$ and $\left(m,r_i,h_i^{'},s_i^{'}\right)$ of a certain group member to the message m, where h_i, $h_i^{'}$ are the random response of the random oracle to $\left(m,r_i\right)$. And we know:

$$g_i^{s_i^{'}} = r_i \times y_i^{2h_i^{'}} \ mod \ p_i, \ g_i^{s_i} = r_i \times y_i^{2h_i} \ mod \ p_i \tag{7}$$

That is $x_i\left(h_i - h_i^{'}\right) = \left(s_i - s_i^{'}\right) \ mod \ p$. Because $\left(h_i - h_i^{'}\right)$ and q are relatively prime, so we can calculate $x_i = \left(s_i - s_i^{'}\right)\left(h_i - h_i^{'}\right)^{-1} \ mod \ q$. So the attacker needs to calculate the discrete logarithm x of y to make $g_i^x = y \ mod \ p_i$. However, the discrete logarithm problem is currently a difficult problem, so such an attacker does not exist.

Supervisability Analysis

The identity information $\left(ID_i, y_i\right)\left(i = 1,2,\ldots,k\right)$ of each node is stored in the configuration file. When a dispute occurs, the group administrator node can calculate y_i according to the group public key, and the signer's identity can be traced according to the saved member information list $\left(ID_i, y_i\right)$.

Resist Sybil Attacks

Sybil attack(Douceur, 2002) means that the attacker uses a single node to forge multiple identities to exist in the P2P network, so as to achieve the purpose of weakening the redundancy of the network, reducing the robustness of the network, and monitoring or interfering with the normal activities of the network.

In this system, each node has been authenticated. In addition, the relay chain is run by the group manager node of each transaction chain and the main CA, and each group manager node is responsible for the maintenance of at least one node on the relay chain. Nodes on the relay chain will perform

redundant calculations and store data in real time, so a sybil attack disguised as a large number of nodes of relay chain and transaction chain is unlikely to happen.

Resist Double-Spend Attacks

In this system, the relay chain scheme is adopted for cross-chain, and the block header information on each transaction chain is stored in the blocks of the relay chain, which can avoid double-spend attacks.

Performance Analysis

We evaluate the experiment result of main operations such as group signature and cross-chain transaction in our proposed system. We ran the evaluation in the following environment. We used Hyperledger Fabric2.3.0 and its BaaS service as the blockchain infrastructure and used CouchDB as the state database. The operating system is Ubuntu20.04.

Group Signature Efficiency Analysis

This system adopts the group signature scheme based on the Chinese remainder theorem proposed by Hong Xuan et al, and improves the scheme. Table 3 below is a comparison of the calculation amount of this scheme and the representative group signature scheme in recent years. The main operations in the system proposed by this paper are modular exponentiation, modular multiplication and squaring operations, denoted by E, M and S respectively. The operations in other systems are bilinear pairing calculation, hash operation and exponential calculation, denoted by e, H and A respectively.

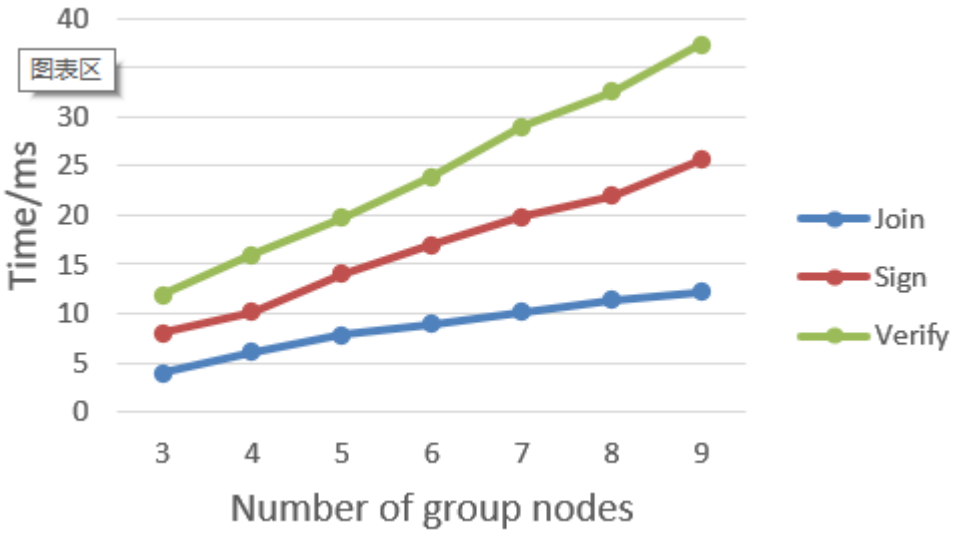
Table 3. Comparisons of computational complexity

Scheme	Join	Signature	Verification
(Hong, & Zhang, 2020)	kM	E + M	2E + M
(Zhang, Li, & Li, 2019)	-	9E + 9e	7E + 11e
(Wang, Liu, & Zhang, 2018)	-	H	12A + 4E + 2e +2H
This scheme	kM	E + M	2E + M

It can be seen from Table 3 that the calculation amount of the main operation of the group signature scheme adopted by this system is the same as the scheme proposed by Hong Xuan. But in the scheme of Hong Xuan et al., the system initialization needs to solve at least k generators of large prime numbers. The complexity of solving a generator of a large prime number P can be estimated as $\left(P-1\right)^2 E$. It can be seen that the scheme of Hong Xuan et al. has a higher initialization complexity. This scheme achieves substantial optimization at the constant level in system initialization. Compared with other studies, this scheme has certain advantages in the calculation of main operations. In general, the solution in this paper has a better overall overhead.

We experimentally tested the time of main operations such as joining, signing, and verifying when the number of group nodes is 3 to 9. As the result shown in Figure 6, the time it takes for a new node to join the group increases as the number of group nodes increases, but the increase in time is not much because it mainly performs modular multiplication operations. The verification operation is one more modular exponentiation than the signature operation, but the overall time taken is satisfactory.

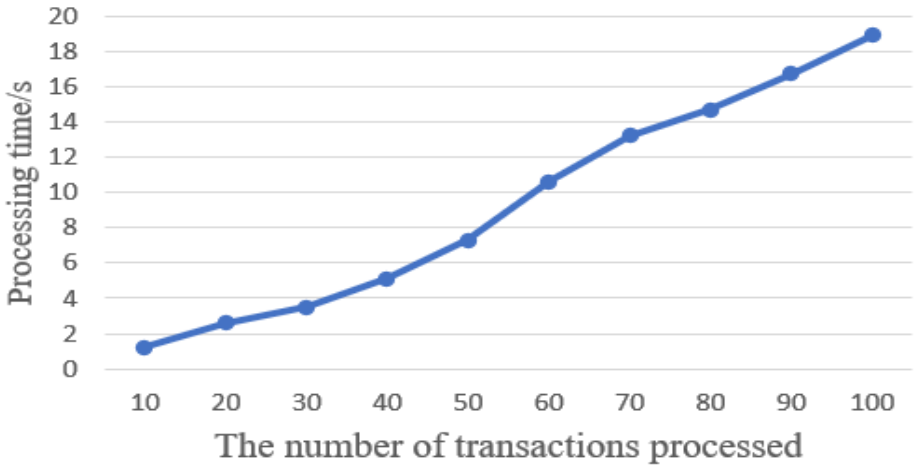
Figure 6. The influence of the number of group nodes on time



Throughput Test

The throughput of this system can be measured by counting the number of simple cross-chain transactions processed by the system every second. First simulate a simple cross-chain transaction scenario: There are only two transaction chains in the initial system, and the group manager nodes of these transaction chains upload relevant information to the relay chain. The simple cross-chain transaction sent is only 10 bytes of actual transaction information sent by the transaction initiator each time. The processing time of a transaction is the time spent in the entire process in Figure 5. During the test, the step length is increased by 10 times to determine the time required for the cross-chain transaction, that is, the number of transactions initiated each time is a multiple of 10. The experimental results are shown in Figure 7:

Figure 7. Cross-chain transaction processing time



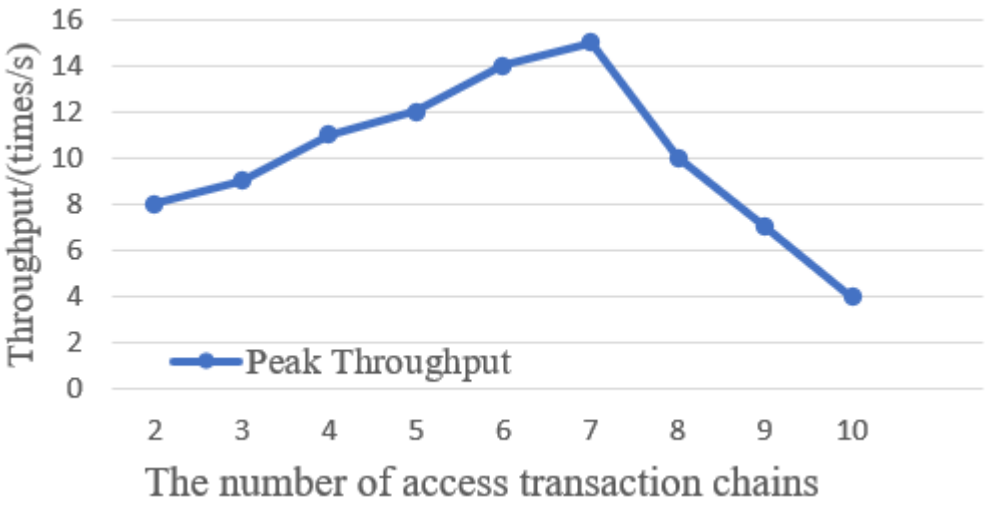
It can be seen from Figure 7 that the system's limit for processing cross-chain transactions is roughly 8 times/s. After analysis, it is found that the performance of the system is mainly affected by the group signature algorithm and the transaction transfer between the transaction chain and the relay chain. Since the entire system is simulated on a computer, the network conditions are good, and the impact of network congestion on the throughput rate of the system is not involved. At the same time, the utilization rate of CPU during simulation may have a greater impact on the processing efficiency of the system.

Scalability Test

With the access of various transaction chains, the network topology of the system will become more and more complicated. The scalability of the system is manifested in the changes in the throughput of the system as the number of access transaction chains increases.

The experiment process is as follows: The initial system has only two transaction chains, and the number of transaction chains is constantly increasing. The system guarantees that only half of the transaction chains will initiate simple cross-chain transactions every time, and the recipient of the transaction is arbitrary. The sum of transactions initiated by all transaction chains still maintains a step length of 10 times. Test the peak throughput of the system for a certain number of transaction chains. The experimental results are shown in Figure 8:

Figure 8. Peak throughput changes as number of access transaction chains increases



It can be seen that when the number of access transaction chains is less than 7, the peak throughput gradually rises from $8 times / s$ to $15 times / s$. This is because the processing of cross-chain transactions on the initiator and receiver can be performed in parallel. After there are 8 transaction chains, the peak throughput gradually decreases, indicating that there is a performance bottleneck on the relay chain. When trying to access 23 transaction chains, the system does not respond, but the final consistency of cross-chain transactions can still be maintained after a long wait.

CONCLUSION

This paper constructs a three-layers cross-chain model that supports identity privacy protection by introducing a relay chain in the blockchain network, and using group signatures and certificate authority. The three layers are the management layer, the transaction layer and the group layer. The management layer has the highest authority to unify the identities of each node and manage parachains participating in cross-chain transactions. The transaction layer contains specific units for cross-chain transactions. The group layer is responsible for specific tasks related to group signature and certificate issuance.

In the group layer, we improved a group signature scheme (Hong, & Zhang, 2020). Analysis shows that the group signature scheme has high security and performance. It is worth mentioning that we aim to propose a cross-chain transaction model that can adopt any group signature scheme, which means that the system security can be improved by improving the group signature scheme.

The specific cross-chain transaction process of the system is similar to the handshake model of a computer network. Experimental analysis shows that the system can effectively complete cross-chain transactions and protect identity privacy. But the system is still in the preliminary exploration stage, and the efficiency and throughput of the model in processing cross-chain transactions need to be further optimized in the follow-up work.

ACKNOWLEDGMENT AND FUNDING AGENCY

This work is supported by the National Key R&D Program of China 2019YFB1404903.

REFERENCES

A Primer for Decentralized Identifiers. (n.d.). https://w3c-ccg.github.io/did-primer/

Asgaonkar, A., & Krishnamachari, B. (2019). Solving the buyer and seller's dilemma: A dual-deposit escrow smart contract for provably cheat-proof delivery and payment for a digital good without a trusted mediator. In *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. (pp. 262–267). IEEE. doi:10.1109/BLOC.2019.8751482

Camenisch, J., & Stadler, M. (1997). Efficient group signature schemes for large groups. In *Annual International Cryptology Conference*. (pp. 410–424). Springer. doi:10.1007/BFb0052252

Chaum, D., & Van Heyst, E. (1991). Group signatures. In *Workshop on the Theory and Application of Cryptographic Techniques*. (pp. 257–265). Springer.

Chen, W., Zhang, L., & Wang, Y. (2004). A group signature scheme based on Chinese remainder theorem. *Tien Tzu Hsueh Pao*, *32*(7), 1062–1065.

Chow, J. (2016). Btc relay. Academic Press.

Douceur, J. R. (2002). The sybil attack. In *International workshop on peer-to-peer systems* (pp. 251-260). doi:10.1007/3-540-45748-8_24

Herlihy, M. (2018). Atomic cross-chain swaps. In *Proceedings of the 2018 ACM symposium on principles of distributed computing* (pp. 245–254). doi:10.1145/3212734.3212736

Hong, X., & Zhang, X. (2020). Forward secure group signature scheme based on Chinese remainder theorem. *Jisuanji Yingyong Yanjiu*, *37*(09), 2806–2810.

Hope-Bailie, A., & Thomas, S. (2016). Interledger: Creating a standard for payments. In *Proceedings of the 25th International Conference Companion on World Wide Web* (pp. 281–282). doi:10.1145/2872518.2889307

Huang, C., Zhong, H., & Wang, Y. (2016). Improved group signature scheme based on Chinese remainder theorem. *Computer Science*, *43*(3), 174–178.

Huang, Z., Li, X., Lai, X., & Chen, K. (2017). Blockchain technology and its applications. *Journal of Information Security Research.*, *3*, 237–278.

Kwon, J. (2014). Tendermint: Consensus without mining. *Draft*, *6*(Fall), 1.

Kwon, J., Buchman, E. (2019). *Cosmos whitepaper*. Academic Press.

Liang, X., Zhang, Q., Gu, J., Chen, S., Zhang, Y., & Liu, C. (2020). Blockchain-Based Traceable Management System for Entry and Exit of Cultural Relics. In *2020 International Conference on High Performance Big Data and Intelligent Systems (HPBD&IS)* (pp. 1–6). IEEE. doi:10.1109/HPBDIS49115.2020.9130590

Liang, X., Zhao, Q., Zhang, Y., Liu, H., & Zhang, Q. (2020). EduChain: A highly available education consortium blockchain platform based on Hyperledger Fabric. *Concurr. Comput. Pract.* https://cdn.hackaday.io/files/10879465447136/Mauve%20Paper%20Vitalik.pdf

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Bus. Rev.* 21260.

Perlman, R. (1999). An overview of PKI trust models. *IEEE Network*, *13*(6), 38–43. doi:10.1109/65.806987

Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In *Banking beyond banks and money* (pp. 239–278). Springer. doi:10.1007/978-3-319-42448-4_13

Poon, J., Buterin, V. (2017). Plasma: Scalable autonomous smart contracts. *White Pap.* 1–47.

Poon, J., & Dryja, T. (2016). *The bitcoin lightning network: Scalable off-chain instant payments*. Academic Press.

Reid, F., & Harrigan, M. (2013). An analysis of anonymity in the bitcoin system. In Security and privacy in social networks. (pp. 197-223). doi:10.1007/978-1-4614-4139-7_10

Shahnaz, A., Qamar, U., & Khalid, A. (2019). Using blockchain for electronic health records. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 147782–147795. doi:10.1109/ACCESS.2019.2946373

Shen, M., Zhu, L., & Xu, K. (2020). Secure Homogeneous Data Sharing Using Blockchain. In Blockchain: Empowering Secure Data Sharing. (pp. 39–59). Springer. doi:10.1007/978-981-15-5939-6_4

Thompson, M. R., Essiari, A., & Mudumbai, S. (2003). Certificate-based authorization policy in a PKI environment. *ACM Trans. Inf. Syst. Secur. TISSEC.*, *6*(4), 566–588. doi:10.1145/950191.950196

Wang, Z., Liu, J., Zhang, Z. (2018). Full anonymous blockchain based on aggregate signature and confidential transaction. *Journal of Computer Research and Development.*, *55*(10), 2185–2198.

Wood, G. (2016). Polkadot: Vision for a heterogeneous multi-chain framework. *White Pap.* 21.

Zhang, L., Li, H., Li, Y., Yu, Y., Au, M. H., & Wang, B. (2019). An efficient linkable group signature for payer tracing in anonymous cryptocurrencies. *Future Generation Computer Systems*, *101*, 29–38. doi:10.1016/j.future.2019.05.081

Zhu, L., Gao, F., Shen, M., Li, Y., Zheng, B., Mao, H., & Wu, Z. (2017). Survey on privacy preserving techniques for blockchain technology. *J. Comput. Res. Dev.,* 2170.

Xiubo Liang is an associate researcher in School of Software, Zhejiang University, PhD. His research interests include artificial intelligence, natural human-computer interaction, digital entertainment, big data and blockchain.

Yu Zhao is a master student in School of Software, Zhejiang University. His research interests include blockchain and privacy protection.

Junhan Wu is a master student in School of Software, Zhejiang University. His research interests include blockchain and privacy protection.

Keting Yin (Corresponding Author) is associate researcher in School of Software, Zhejiang University, PhD. His research interests include blockchain and big data. Email: yinkt@zju.edu.cn.