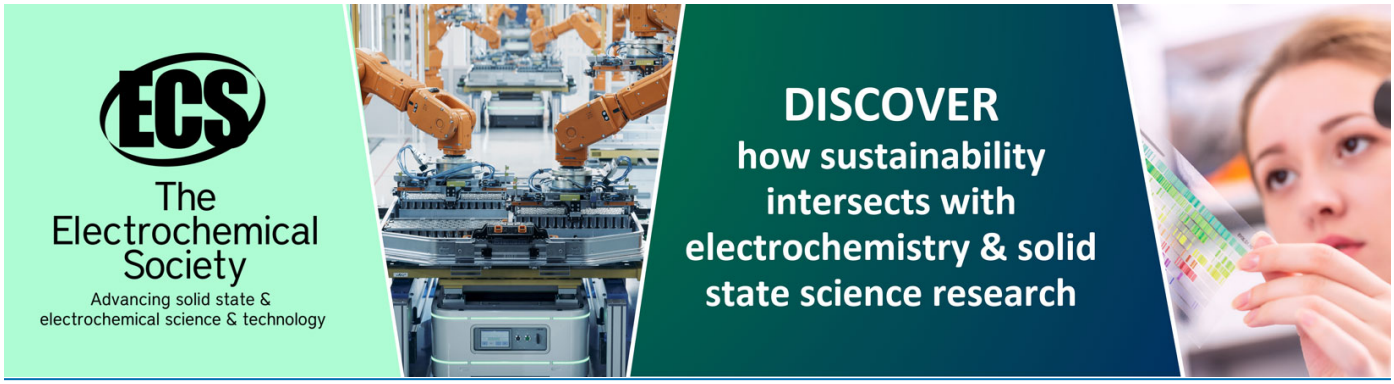
A New Privacy Protection Security Scheme for Blockchain



IOP Conf. Series: Journal of Physics: Conf. Series **1237** (2019) 022025 doi:10.1088/1742-6596/1237/2/022025

A New Privacy Protection Security Scheme for Blockchain

Kang Qiao, Wei You, Hongbo Tang

National Digital Switching System Engineering & Technology R&D Center, ZhengZhou 450001, China

773441271@qq.com

Abstract. The strong security and strong privacy protection features of the blockchain are important aspects of the development of the blockchain, but the security and privacy protection features of the blockchain are not perfect. With the continuous development and wide application of blockchain technology, the problem of privacy leakage is becoming more and more prominent and must be fully taken seriously. This paper proposes a new blockchain signature scheme based on the combination of aggregate signature and ring signature for the privacy protection of transaction addresses in blockchain. This scheme uses a ring signature as the basis for the signature algorithm. On the basis of this, it combines the aggregate signature, which hides the address information of the signer on the one hand and fixes the signature length on the other hand. This enhances the privacy protection capability of the transaction address in the blockchain, and also effectively reduces the signature space of the blockchain system, and solves the problem of capacity expansion to some extent.

1. Introduction

The blockchain is the underlying technology born in Bitcoin. The earliest definition comes from the article published by Nakamoto in 2008 [1]. Blockchain technology is a distributed Internet database technology. Its decentralization, trustworthiness, transparency and other characteristics enable strange nodes to establish a point-to-point relationship without relying on third-party trusted organizations. The main advantage of trusted value delivery is the ability to significantly reduce trust costs and improve interaction efficiency. There is no central server in the blockchain network. Each participating node in the system holds a complete copy of the data. Together, they maintain the integrity of the data and can effectively avoid the risk of single-point crash and data leakage of the centralized server.

However, the global ledger that records transaction data in the blockchain is public in the network, and any attacker can obtain all transaction information, leaving the trader's privacy risk of disclosure. For example, the Bitcoin system currently has approximately 155 GB of transaction data, including all transactions from 2009 to the current time. The data in the book is analyzed. The attacker can obtain all the transactions corresponding to any account, and can also analyze the trading relationship map between different accounts. Even if the user uses different accounts for trading, the attacker can use the address clustering. The technology analyzes different accounts belonging to the same user [2-6].

The ring signature[7] has the function of protecting the subject account information signed by the participants. Therefore, the ring signature has its own advantages in terms of privacy protection in the blockchain, especially the protection of the user address information involved in the transaction. Among the currently developed cryptocurrencies with privacy-protected stomach characteristics, Monroe[8] is mainly based on ring signature as its innovation point. However, when a transaction

contains multiple input addresses, multiple signed messages will be generated. In the blockchain, this can seriously affect the performance of the system. In order to reduce the signature space of the transaction, this paper combines the aggregate signature[9] and the ring signature to obtain an aggregate ring signature scheme.

The remainder of this paper is organized as follows. This paper present the background information on the privacy preserving on blockchain in section 2.Section3 introduces the ring signature and the aggregate signature scheme. Section 4 describes the core of our signature scheme on blockchain based on ring and aggregate signature. Section 5 summarizes our contributions.

2. Privacy Preserving on Blockchain

In traditional information systems, privacy protection usually refers to the original data or the attributes behind the data that the data owner is not willing to disclose. In the blockchain, in order to reach a consensus between different nodes, a lot of information must be disclosed to synchronize the nodes. However, on the other hand, there is also a requirement for privacy protection in the blockchain system. For some sensitive information, the data owner needs to encrypt or otherwise process it to reduce the risk of privacy leakage. Based on these, this paper divides the privacy in the blockchain into identity privacy and transaction privacy.

2.1. Identity privacy

User identity privacy mainly refers to the correspondence between the address information on the blockchain and the identity of the user in real life. The identity information of the user in the blockchain is usually not related to the identity information of the user in reality. In the blockchain, the address is generally used to represent the identity of the user, and the address is generally cryptographically selected by the user. The method is generated and has strong privacy. Although the identity information in the blockchain itself is private, when the same user generates a large number of transactions in the blockchain, through the analysis of the user transaction information, and through the collection of the user transaction network information, combined with other technologies. Means, it is very possible to achieve the correspondence between the user's real identity information and the blockchain identity information.

2.2. Transaction privacy

Transaction privacy mainly refers to the judgment of transaction association through public transaction information, including transaction sending address, transaction receiving address and transaction amount. In a cryptocurrency system such as Bitcoin, all transaction information is public to all users. In this case, the user can easily obtain the transaction information of the entire network. Through the open transaction information, combined with network technology and big data analysis technology, the relevant information of the user can be analyzed. The user's identity information and transaction information are much more important in the blockchain than the traditional centralized system. Because the blockchain system is not tamperable and decentralized, the user's private information can not be recovered once it is leaked. In the centralized system, it can also complete the tampering behavior through the center. In the blockchain system, once the user's identity information or transaction information is leaked, it will be a permanent behavior.

3. Two Important Signature Scheme

3.1. Ring signature

The ring signature is a special group signature [10]. In this group signature technology, there is no trusted third party. The signer randomly selects multiple other public keys when signing, combining their own public and private keys and random numbers. And other technical means to complete the signature. For the signature verifier, he only knows that the signer is from this signature set, and cannot determine which signer is the specific one. Especially for some information that requires long-

term protection, ring signature technology with unconditional anonymity will play an important role. Since the first signing of the ring signature, it has developed rapidly, and more and more new ring signature technologies have been proposed. In 2001, Rivest et al. proposed the first ring signature party [11]. In 2002, Fangguo Zhang et al. proposed an identity-based ring signature scheme through identity-based cryptosystem and bilinear pairing technique [12]. In 2006, Fangguo Zhang et al. proposed an identity-based ring signature scheme in P2P networks [13].

The definition of the ring signature. Assume that there are *n* users $\{u_1, u_2, ..., u_n\}$ in the system, one for each u_i has public-private key pair (pk_i, sk_i). The most important feature of ring signature is unconditional anonymity, which is applicable in many scenarios. The main algorithms are key generation Gen, signature Sign, and Verify. The following are introduced separately:

Key generation Gen. This is a probability polynomial time algorithm. For each user u_i, enter the security parameters k_i and output the corresponding public-private key pair (pk_i, sk_i).

Signature Sign. Enter the message *m* and *n* public key sets $\{pk_1, pk_2, ..., pk_n\}$ of the users participating in the ring signature and some other parameters, the most important is the private signer's private key sk_i, and the output signature *R*.

Verify. The input message and the corresponding signature information pair (*m, R*) are output if the signature *R* satisfies the signature change requirement of the message *m*, otherwise the output is false.

3.2. Aggregate Signature

Aggregated signature is a digital signature technique mainly used to compress and aggregate multiple digital signatures, and compresses any number of signatures {σ} into a signature σ. This can greatly reduce the storage requirements for signatures, and at the same time reduce the network bandwidth requirements, which is very useful in distributed systems such as blockchains. It can effectively solve the storage performance problem of blockchain. Simplifying the verification of any number of signatures to one verification can also reduce the work of signature verification in the blockchain system and further improve the performance of the blockchain system. Therefore, It's a good role of the aggregation signature technology has the signature and verification signature for the blockchain system.

The definition of the aggregate signature. Aggregated signature is a signature scheme used to aggregate any number of signatures into one signature. It is assumed that *n* messages $\{m_1, m_2, ..., m_n\}$ in the system have *n* message signatures $\{\sigma_1, \sigma_2, ..., \sigma_n\}$, *n* users $\{u_1, u_2, ..., u_n\}$ have *n* public keys $\{pk_1, pk_2, ..., pk_n\}$, and producers of aggregated signatures $\{\sigma_1, \sigma_2, ..., \sigma_n\}$ can aggregate into unique signatures σ. Given the aggregate signature σ, the generated public key set $\{pk_1, pk_2, ..., pk_n\}$, and the message set $\{m_1, m_2, ..., m_n\}$, it is possible to verify σ_i that the user u_i has signed the message m_i separately. The implementation of the aggregate signature is described in detail below.

$AS = \{Gen, Sign, Verify, AggS, AggV\}$ is a polynomial time algorithm quintuple, which is described as follows:

$DS = (Gen, Sign, Verify)$ is a common signature scheme, also known as the base signature of an aggregated signature.

Aggregate signatures generate AggS. Based on Gen and Sign, it implements the common signature function, and realizes the aggregation function of message vector $(m_1, m_2, ..., m_n)$, user vector $(u_1, u_2, ..., u_n)$, and individual signature vector $(\sigma_1, \sigma_2, ..., \sigma_n)$, and can aggregate new signatures σ_{n+1}.

Aggregate signature verification AggV. Suppose each one u_i corresponds to a public-private key pair (pk_i, sk_i). If :

$AggV(pk_1,...,pk_n,m_1,...,m_n,AggS(pk_1,...pk_n,Sign(sk_1,m_1),...,Sign(sk_n,m_n)))=1$, output true, otherwise output false.

4. The Core of Our Signature Scheme

4.1. Ring Signature Scheme

Firstly, a ring signature scheme based on Schnorr signature idea proposed by Zhaoxia Wu et al. Participants in this ring signature scheme include users and one verifier. The specific algorithm of the scheme is as follows:

Initialization: Given a security parameter k, the algorithm outputs (F_1, q, P, H). The definition F_1 is a large prime q -order cyclic addition group. Define P as the generator of F_1. The definition $H:\{0,1\}^*\times\mathrm{F}_1\rightarrow\mathbf{Z}_q^*$ is a secure password hash function.

User key generation Gen. The signer randomly select $x_i\in\mathbf{Z}_q^*$ as the private key and calculates the corresponding public key $Y_i=x_iP$.

The ring signature generates RingS. Given a message m , n user's identity set $W=\{ID_1,ID_2,...,ID_n\}$, an actual signer u_s can generate a ring signature σ for the message m anonymously. The actual signer u does the following:

1.The signer u_s randomly selects $t\in\mathbf{Z}_q^*$ and randomly selects $\sigma_i\in\mathbf{Z}_q^*$ for all $i\in(1,2,...,n)$, $i\neq s$;

2. Calculating $h=H(m,tP+\sum_{i\neq s}\sigma_iY_i)$;

3. Calculating $\sigma_s=h-\sum_{i\neq s}\sigma_i$;

4. Calculating $z=t-\sigma_sx_s$;

5. Output $\sigma=(\sigma_1,\sigma_2,...,\sigma_n,m,z)$;

Ring signature verification RingV. Given the public key $\{Y_1,Y_2,...,Y_n\}$ of n users and a ring signature σ , a verifier V can use the following equation to verify the validity of the ring signature σ .

$$\sum_{i=1}^{n}\sigma_i=H(m,zP+\sum_{i=1}^{n}\sigma_iY_i)$$

If the equation is true, the verifier accepts the ring signature, otherwise it rejects.

In the following, based on the ring signature, combined with the aggregate signature technology, an improved signature scheme is given. Under this signature scheme, the number of ring signatures remains the same as the number of ring signature participants increases.

4.2. Aggregate and Ring Signature Scheme

The ring signature scheme protects the address information of the sender of the transaction, but when a transaction contains multiple input addresses, multiple signature messages are generated. In the blockchain, this can seriously affect the performance of the system. In order to reduce the signature space of the transaction, this paper combines the aggregate signature and the ring signature to obtain an aggregate ring signature scheme. Similarly, the aggregation ring signature scheme also includes three algorithms: aggregation key generation AGen, aggregation ring signature ARingS, and aggregation ring signature verification ARingV. Similarly, the definition F_1 is a large prime q -order

cyclic addition group. Define P as the generator of F_1. The definition $H:\{0,1\}^*\times\mathrm{F}_1\to\mathbf{Z}_q^*$ is a secure password hash function.

Aggregate key generation AGen. For a particular user $A_j(j=1,2,...,m)$, randomly select $x_j\xleftarrow{R}\mathbf{Z}_p$ and calculate $v_j\leftarrow x_jP$. The user's public key is defined as $v_j\in\mathrm{F}_1$ and the private key is $x_j\in\mathbf{Z}_p$.

Aggregate ring signature ARingS. Given the public key $v_1^1,v_1^2,...,v_1^n,...,v_m^1,v_m^2,...,v_m^n\in\mathrm{F}_2$, m transaction messages $T_{x_1},T_{x_2},...,T_{x_m}=\{0,1\}^*$, and the private key $\{x_1,x_2,...,x_m\}$ corresponding to m public keys $\{v_1,v_2,...,v_m\}$, $t_j\xleftarrow{R}\mathbf{Z}_p$, $\sigma_j^i\in\mathbf{Z}_q^*$, $j=1,2,...,m$, $i=1,2,...,n$ is chosen randomly for all $i\neq s$. Calculate $tx_i=H(T_{x_i})\in\mathrm{F}_1$ and set

1. Calculating $h_j=H(tx_j^i,t_jP+\sum_{i\neq s_j}\sigma_j^iv_j^i)$;
2. Calculating $\sigma_{s_j}=h_j-\sum_{i\neq s_j}\sigma_j^i$;
3. Calculating $z_j=t_j-\sigma_{s_j}x_{s_j}$;
4. Setting $\sigma_j=\left(\sigma_1,\sigma_2,...,\sigma_n,tx_j^i,z_j\right)$;
5. For all $i\neq s_j$, output aggregate signature $\sigma_{aggre}=\left(\prod_{j=1}^m\sigma_j,...,\prod_{j=1}^m\sigma_j\right)$.

Aggregate ring signature verification ARingV. Give $v_1^1,v_1^2,...,v_1^n,...,v_m^1,v_m^2,...,v_m^n\in\mathrm{F}_1$ the public key $T_{x_1},T_{x_2},...,T_{x_m}=\{0,1\}^*$, m transaction messages, and the signature σ_{aggre}, calculate $tx_j=H(T_{x_j})\in\mathrm{F}_1$, and verify

$$\sum_{i=1}^n\sigma_{aggre_i}=H(tx,zP+\sum_{i=1}^n\sigma_{aggre_i}v_i)$$

The aggregation signature scheme presented in this paper can solve the privacy protection and performance problems of blockchain to some extent. However, in the application of cryptocurrency, linkable ring signature is necessary, so the combination of aggregate signature and linkable ring signature will be an important research direction next.

5. Conclusion

This paper presents a signature scheme combining ring signature and aggregate signature, which solves the privacy protection and performance of cryptocurrency to some extent. Under this signature scheme, compared with the traditional ring signature scheme, when a transaction contains *n* input addresses and *m* output addresses, the number of signatures can be reduced from *n* to 1, greatly improving the blockchain system performance. At the same time, this signature scheme can effectively protect the address information of the sender of the transaction. The method presented in this paper only solves these two problems by using cryptography. Most of the previous solutions use structural improvements to solve these problems. It is easy to introduce new problems while solving these two problems. At the same time, the signature scheme given in this paper can protect the address information of both parties at the same time, and the length of the generated signature message remains unchanged as the number of users participating in the signature increases and the number of input addresses and output addresses included in the transaction increases.

References

[1] Nakamoto S. Bitcoin: A peer - to - peer electronic cash system[J]. Consulted, 2008.
[2] Reid F, Harrigan M. An Analysis of Anonymity in the Bitcoin System[C]// IEEE Third International Conference on IEEE Third International Conference on Privacy, Security. 2012.
[3] Liao K , Zhao Z , Doupe A , et al. Behind closed doors: measurement and analysis of CryptoLocker ransoms in Bitcoin[C]// Electronic Crime Research. IEEE, 2016.
[4] Ron D , Shamir A . Quantitative Analysis of the Full Bitcoin Transaction Graph[C]// International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2013.
[5] Meiklejohn S , Pomarole M , Jordan G , et al. A fistful of bitcoins: characterizing payments among men with no names[C]// Proceedings of the 2013 conference on Internet measurement conference. ACM, 2013.
[6] Zhao C , Guan Y . A GRAPH-BASED INVESTIGATION OF BITCOIN TRANSACTIONS[M]// Advances in Digital Forensics XI. Springer International Publishing, 2015.
[7] Zhang Guoyin, Wang Lingling, Ma Chunguang. Research on ring signature research [J]. Journal of Communications, 2007, 28(5): 109-117.
[8] Van Saberhagen N. Cryptonote v2.0[J]. 2013: 1-13.
[9] Yang Tao, Kong Lingbo, Hu Jianbin, et al. Review of Polymeric Signatures and Their Applications[J]. Journal of Computer Research and Development, 2012(s2):192-199.
[10] Chaum D , Eugène van Heyst. Group Signatures[J]. 1991.
[11] Rivest R L , Shamir A , Tauman Y . How to Leak a Secret[C]// International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2001.
[12] Zhang F , Kim K . ID-Based Blind Signature and Ring Signature from Pairings[C]// International Conference on the Theory & Application of Cryptology & Information Security: Advances in Cryptology. Springer-Verlag, 2002.
[13] Chen Y, Susilo W , Mu Y . Identity-based anonymous designated ring signatures[C]// International Conference on Wireless Communications & Mobile Computing. ACM, 2006.