A traceable ring signature algorithm based on blockchain

Jingyuan Li[1,*]

[1]Shaanxi Normal University, Xi'an 710119, China
[*]Corresponding Author

Abstract: *The application of ring signature in blockchain can protect personal privacy anonymously, but the bad behavior records of malicious users cannot be tracked in practical use. In order to solve the problem of dishonest real signers, this paper modifies the ring signature algorithm, ensures the decentralized distributed application of the ring signature algorithm by adding some relevant information and key generation mechanism, and cooperatively tracks the identity of dishonest signers through polling and interaction with ring members at critical times, The generation and verification of algorithm signature are automatically completed by the blockchain smart contract code to realize the security characteristics of the system, such as transparency, anonymity, unforgeability and traceability. Through security analysis, the scheme is feasible and more efficient.*

Keywords: *Blockchain, Ring signature, Privacy protection, Smart contract*

1. Introduction

Blockchain is a decentralized distributed ledger system, which completes the technical scheme of data calculation, processing, storage and verification through distributed nodes in different geographical locations. Each transaction record will be stored in one of the chain blocks in the form of blocks. The hash value of each block is generated according to the hash value of the previous block, which is tamperable [1,2,3]. The data stored in the blockchain is open to all users, and the privacy and security issues related to transaction information records and other data are worth considering. Ring signature algorithm the signature implies a parameter and forms a ring according to certain rules. The signature generated by it has the characteristics of spontaneity, anonymity and group. It can realize the unconditional anonymity of the signer. The signer can specify his own anonymity range to form a beautiful ring logic architecture, It can complete the main functions of group signature, but does not need a trusted third-party organization or group administrator [4,5]. Applying the ring signature algorithm to the blockchain can realize the privacy protection needs of both sides of information interaction. The receiver cannot and needs to know who sent the information. It only needs to confirm that the information has not been tampered according to the signature, which plays a positive role in fully protecting the personal identity of members in the blockchain.

Some scholars have been studying the signature algorithm. For example, document [5] proposed a certificateless ring signature method, which can reduce the security risk of centralized certificate management. Document [6] studied the ring signature algorithm of verifiable agent. All of these have a trusted third-party organization to generate the key PKG (private key generator), This is inconsistent with the decentralized distributed architecture of the blockchain. The third-party key generation institutions have the risk of security trust, and their research can not achieve the identity verification of traceable signature senders. In case of disputes between bad users in the signature system, they need to be located and tracked. In this paper, a traceable ring signature algorithm based on blockchain is proposed to solve the above two problems. The smart contract of blockchain is used to manage PKG to generate signatures, which fully protects the privacy and confidentiality of users. At the same time, the identity of message sender can be tracked and verified after polling with members in the ring.

The main contributions of this paper are as follows:

(1) The decentralized data storage is realized based on the blockchain technology. There is no third-party key management organization to generate the key. The nodes on the blockchain randomly form group members to generate and maintain the key. The security of the system is improved.

(2) The algorithm based on ring signature ensures the personal privacy protection of the signer in

data transmission, and prevents the signer's relevant information from being cracked after being eavesdropped during data transmission.

(3) The ring signature method supporting traceable verification can track and verify in the process of normal users' malicious operations, and find users to verify.

2. Preparatory knowledge

2.1 Bilinear mapping

Bilinear groups can be described by quintuples(p, G_1, G_2, G_T, e). In a quintuple, p is a given security constant λ The related large prime numbers, G_1, G_2 and G_T, are multiplicative cyclic groups of order p, and e is a bilinear mapping $e{:}G_1\times G_2\rightarrow G_T$, which meets the following three conditions:

Bilinear: for any $g\in G_1, h\in G_2,\ a, b\in \mathbf{Z_p}, e(ga, hb)=e(g, h)^{ab}$;

Non degeneracy: there are at least elements $g_1\in G_1, g_2\in G_2,$ satisfying $e(g_1, g_2)\neq 1$;

Computability: for any $u\in G_1, v\in G_2,$ there is a safety constant corresponding to the given value λ The related polynomial time algorithm can efficiently calculate $e(u, v)$.

2.2 Diffie Hellman problem

Diffie Hellman problem is divided into two problems: computational problem and deterministic problem. It is very difficult to calculate discrete logarithm problem on finite field. Let G be a cyclic addition group with order q, then the two problems are as follows:

Problem 1 (CDHP problem) calculates abR for R, aR, bR, any $a, b\in Z_q$ in group G.

Problem 2 (ddhp problem) judge whether $c=ab \bmod q$ is true for R, aR, bR, cR, any $a, b, c\ \in Z_q$ in group G.

On the basis of bilinear mapping and Diffie Hellman problem, there is a difficult assumption problem to find the inverse. For $e = e\ (g, H)$, if $g\in G_1$ is known, it is difficult to find $Q\in G1$ [7].

2.3 Blockchain Technology

Blockchain originated from bitcoin. On November 1, 2008, a person calling himself Satoshi Nakamoto published bitcoin: a point-to-point e-cash system, which described the architecture concept of e-cash system based on P2P network technology, encryption technology, timestamp technology and blockchain technology, which marked the birth of bitcoin. Two months later, the theory came into practice, and the first creation block with serial number 0 was born on January 3, 2009. A few days later, on January 9, 2009, the block with serial number 1 appeared and connected with the creation block with serial number 0 to form a chain, marking the birth of the blockchain [8]. Blockchain technology is the core technology adopted by bitcoin and Ethereum platforms. The technologies related to blockchain include smart contract, digital currency, consensus mechanism algorithm, etc. among them, there are more relevant knowledge of applied cryptography, and a distributed decentralized ledger maintained by multiple parties.

Smart contract is a piece of code deployed in the blockchain node. After meeting the input conditions, it triggers the automatic verification and execution of the code without manual operation intervention, realizes the non repudiation and decentralization of transactions such as digital currency, and reduces the transaction cost of users.

2.4 Ring signature algorithm

Ring signature is a kind of signature technology. Frankly speaking, there is usually a group of public keys, and the signer knows the private key corresponding to a public key in a group of public keys (just know one). In this way, he can use this set of public keys and the corresponding private key to generate a ring signature. The verifier can verify that the ring signature is indeed generated by the owner of a private key in this group of public keys, but he does not know which public key corresponds to the private key.

The ring signature name hides the real signature identity in the ring, which can realize the digital currency protocol of the blockchain and protect the identity privacy of users. The ring signature generates a common PK_i and SK_i for each user according to the probability polynomial algorithm. Assuming that the ring member public key $L=\{PK_1, PK_2, \cdots, PK_n\}$ and a member private key SK_i generate a signature R for message m, then R should have the following security requirements:

1) Unconditional anonymity. Even if the attacker illegally obtains all the private keys, the probability that he can determine the real signer is no more than $1/n$, and n is the number of ring members.

2) Unforgeability. The attacker does not know any member's private key. Even if the signature R is obtained from the random oracle, the probability of the attacker forging a legal signature is negligible.

3) Ring signature has good characteristics. Unconditional anonymity of signers can be realized; The signer can freely specify his own anonymous range to form a beautiful ring logical structure; The main functions of group signature can be realized, but there is no need for a trusted third party or group administrator.

3. Ring signature model in blockchain

The blockchain based ring signature model includes three roles: signing user, group member set and selected ring signing member. They are all composed of nodes in the blockchain, in which the group member set ring signature members do not cross, and each node cannot play two or more roles at the same time. The respective division of labor of the three roles is as follows:

(1) Signing user: the signing user is the initiator, mainly completing the tasks related to signing the transmission message. It can obtain the list of selected PKG group members and ring signing members from the blockchain system, and sign the message content according to the key generated by PKG initialization.

(2) Group member set: the PKG group member set is a list of randomly selected members on the blockchain. Its main task is to distribute keys to ring signing members or signing users. The group member set does not know who the generated keys are to be given or what the specific purpose is. It is only responsible for key distribution and parameter initialization. Finally, the signature result is verified and calculated. If the signature fails, an error message is returned. If the signature verification is successful, the data and signature are packaged to generate a new block. According to the blockchain smart contract algorithm, the new block is added to the blockchain, and the signature user verification result is returned.

(3) Ring signature member: the ring signature member is also a list randomly selected by the blockchain system. It cannot duplicate the PKG group member list. It is mainly responsible for the ring signature task. It also does not know the message content to be signed, and is only used to assist the signing user to complete the final signature work.

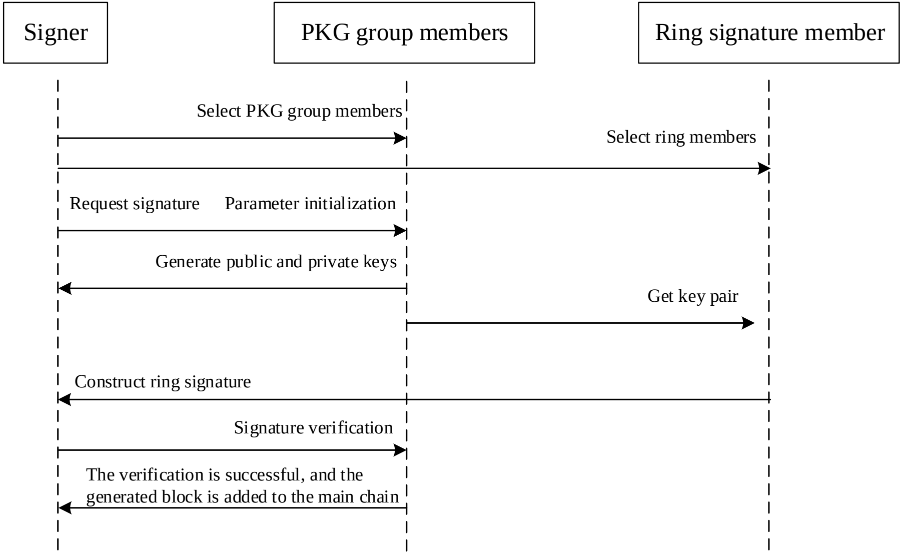

Figure. 1 work flow chart of ring signature in blockchain

As shown in Figure 1, the flow chart of each role signing in the ring can be seen that they cooperate with each other to complete the final ring signature, trigger the execution of smart contract code, and add the generated new blocks to the blockchain system.

4. Algorithm of traceable ring signature

The final ring signature algorithm is mainly divided into five parts: initialization, member selection, key generation, signature generation and signature verification, which are introduced below:

Algorithm 1. Initialize the system parameter $P \leftarrow Init(ID_i, PKG_i)$.

Input: bilinear mapping $e{:}G_1 \times G_1 \rightarrow G_2$, hash functions H_1 and H_2, ID_i, random number $S_i \in \mathbf{Z_q}$;

Output: system parameter P;

① Calculate the public key $P_i=S_i{*}E$ of each node ID_i, where S_i is the private key and E is the G_1 generator;

② Set PKG group members as $PKG=\{PKG_i\}(i=1, 2, ... , n)$, and set ID_i and PKG_i to correspond one by one;

③ Each node i has a key pair $PKG_i=\{P_i, S_i\}$, and publishes system parameters $P=\{G_1, G_2, H_1, H_2, PKG\}$;

Algorithm 2. Select member $(L,C) \leftarrow Setup(ID_j)$.

Input: ID_j of the actual signer;

Output: ring signature L, participating in signature PKG group set C;

① The signer randomly selects the signature ring $L=\{ID_i\}(i=1, 2, ... , n)$, and $ID_j \in L$;

② m members are randomly selected from PKG to form C participating in the signature, which is not duplicate with the signature ring L;

Algorithm 3. Generate key $(Q_i, D_{ui}) \leftarrow Setup(L,C, ID_j)$.

Input: ring signature L, set C, signer ID_j;

Output: Q_i, D_{ui};

① Calculate the public key $Q_i = H_1(ID_i)$ of each member in the ring signature L;

② Calculate $D_{ji} = S_i{*}Q_j$ corresponding to signer ID_j;

③ Sending Q_i and D_{ji} to ID_i and ID_j through encrypted channel;

Algorithm 4. Signature generation $Sig \leftarrow Setup(m, ID_j)$.

Input: Signature content m, ID_j;

Output: sig;

① Select $n\text{-}1$ random numbers $\chi_i \in \mathbf{Z_q}$ is used as the key and Ui is calculated $\chi_i{*}E$, of which species Ui has not been used;

② Calculate $Y_i=H_2(m, L, U_i)$, where $i \in (i=1, 2, ... , n)$, $i \neq j$;

③ Signer selects random number $\chi_j \in \mathbf{Z_q}$ as the key, U_j and Y_j are calculated as follows:

$$U_j = x_j * E - \sum_{i=1, i\neq j}^{n} (U_i + Y_i * Q_i)$$

calculate $Y_j=H_2(m, L, U_j)$, $i \in (i=1, 2, ... , n), i \neq j$.

④ The signer randomly selects $r \in \{0, 1\}^*$, and calculates

$P_j = \sum_{k=1}^{n} P_k$, $V = (x_j + Y_j) * \sum_{k=1}^{n} D_k$

⑤ Calculation $T = (x_j + Y_j) * Q_j$, $t=H_1(V, T, \chi_i, P_j, r)$;

⑥ Calculate the final signature $Sig=(m, U_1, U_2, ... ,U_n, V, t, C)$;

Algorithm 5. Signature verification $result \leftarrow verify(Sig, m)$.

Input: Signature Sig and signature content m;

Output: if $result$ is $true$, the signature is valid; otherwise, the signature is invalid;

① *if*$(e(E,V) == e(P_j, \sum_{i=1}^{n}(U_i + Y_i * Q_i)))$ *then*

② *return True*

③ *else*

④ *return False*

Algorithm 6. Track the signer $result1 \leftarrow Trace(Sig, m,T, P_i, r)$.

Input: Signature Sig, signature content m, T, P_j, r;

Output: $result1$ is $true$, which is the real signer;

① In order to trace the real signer identity from the ring signature L member, it is necessary to traverse and query each information T_i, P_i, χ_i and r values, and then calculate as follows;

② Calculate $t=H_1(V,T, \chi_i, P_i, r)$;

③ Calculate $e(P_i, T)=e(E, V)$;

④ If both ① and ② are satisfied, it can be determined that ID_i is the signer.

Algorithm is run under the system framework of chain blocks, execute code deployed in intelligent contract part of the chain block, and stored in blocks are frozen in the chain, each node ACTS as a link in a chain block signature member or PKG group members different roles, such not only can protect the privacy of signer's identity and in need of find true the identity of the signer can track, Improve the stability and reliability provided.

5. Safety analysis

The security of the algorithm is mainly based on the ring signature technology, which has unforgeability, unconditional anonymity and authentication. The following three aspects are analyzed.

(1) Unforgeability: the Challenger may randomly select $U=\{U_i\}(i=1, 2, \ldots ,n)$ and the ring signature is known to be *Sig*, so it is necessary to obtain V from $e(E,V) == e\left(P_j, \sum_{i=1}^{n}(U_i + Y_i * Q_i)\right)$. According to the difficult problems in Chapter 2.2, it is not feasible, so the ring signature *Sig* is unforgeable.

(2) Unconditional anonymity: according to algorithm 4, both U and V are calculated and the selected random number is calculated χ_j correlation, the final ring signature result is generated after hash calculation, and the members in the ring signature L are evenly distributed on the group. So if the Challenger wants to guess the real signer, the probability is *1/n*.

(3) Traceable authentication: in order to verify the signature identity, the signer can provide his own relevant information to prove that he is a real signer. The signer identity can be verified through the verification formula of algorithm 5 and algorithm 6, with traceable and verifiable functions.

6. Performance analysis

We analyze the efficiency and performance of this scheme from the calculation cost. We use i5 CPU, 8g memory and Linux operating system, download and install PBC library and GMP library to call logarithmic function and exponential operation. Based on the bilinear function construction and operation analysis of elliptic curve, assuming that there are 100 nodes in the blockchain, P and m are used to represent the overhead time of logarithmic function and scalar multiplication respectively. The simulation operation is carried out according to the algorithm in Chapter 4, and the measured results are shown in Table 1.

Table 1 Computing overhead of ring signature based on blockchain

Task	Theory cost	Experimentalcost (ms)
Signature	*(3n+2)*m*	1208
Verify	*2p+n*m*	434.8

7. Conclusion

The application of ring signature in blockchain can improve the privacy and confidentiality of the system. Through the identity of anonymous information sender and decentralized distributed key generation group members, the message content can be transmitted more reliably and stably. There is no centralized third-party organization to distribute management keys, reducing the risk of data disclosure. At the same time, for dishonest signers, the platform has a traceable verification method to identify malicious users and enhance the authority and transparency of the system.

References

[1] L.Xiaoqi, J.Peng, C.Ting. A survey on the security of blockchain systems.Future Generation Computer Systems, 2020. 107841~853.

[2] Sirer Emin Gun,Eyal Ittay.Majority Is Not Enough: Bitcoin Mining Is Vulnerable.Communications of the ACM,2018,61(7).95~102.

[3] L Chao, H Debiao, H Xinyi,et al.BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0.Journal of network and computer

applications,2018,116(Aug.).42~52.

[4] J.LV, X.Wang. Verifiable Ring Signature [c]//Proceedings of 2003 9th International Conference on Distributed Multimedia System. New York: ACM, 2003: 32-44.

[5] L.Dawen, H.Mingxing, L.Xiao. Certificateless Verifiable Ring Signature Scheme [J].Computer Engineering, 2009, 35(15): 135-137.

[6] V.DHIVYA, H.ANANDAKUMAR, M.SIVAKUMAR. An Effective Group Formation in the Cloud Based on Ring Signature[C]//Proceedings of the 2015 IEEE 9th International Conference on Intelligent Systems and Contr01. Piscataway: IEEE, 2015: 7282366.

[7] Y.YACOBI. A Note on the Bilinear Diffie-Hellman Assumption. IACR Cryptology ePrint Archive, 2002: 113-119.

[8] S.NAKAMOTO. Bitcoin: A Peer-to-Peer Electronic Cash System [EB/OL]. [2021-10-31]. https://bitcoin.org/bitcoin.pdf.