The Blockchain Redundant Data Deletion Model Based On The Ring Signature

Weiyi Dai

Southwest Minzu University, Sichuan, 610000, China

Keywords: Blockchain; Ring Signature; Work Efficiency

Abstract: In order to solve the problem of work efficiency and possible crashes caused by excessive storage of useless data in the blockchain distributed system, the elliptic curve algorithm for identity signature in the blockchain is improved, and the signature algorithm is used The generated public key is used as the verification identity key for the deletion operation of each signature block in the blockchain. When the data loses its value, this part of the data in the blockchain is precisely deleted by the signature block, so that the blockchain is not These redundant data will cause various failures due to reduced work efficiency.

1. Introduction

Blockchain technology is the earliest technology used by Bitcoin. The earliest prototype was derived from an article entitled "Bitcoin: A Peer-to-Peer Electronic Cash System" published by Satoshi Nakamoto in 2008. It contains a variety of complex technologies such as distributed ledgers, cryptography, smart contracts and consensus algorithms, and is suitable for many fields. In recent years, people have begun to apply blockchain to the fields of finance, education, logistics, and medical care. However, the waste of resources and low processing efficiency caused by the characteristics of the blockchain system also restrict the development of the blockchain.

In the blockchain, a variety of signature mechanisms are used to improve its performance. Compared with traditional anonymous signature mechanisms such as group signatures and ring signatures, the attribute signature strategy is also a good choice and method.

In 2008, Maji [1] and others proposed the concept of attribute signature and the corresponding security model. Then in 2014 Okamoto et al. [2] proposed a threshold structure scheme based on attribute signature. In 2014, Tang et al. [3] used multi-linear mapping to construct a scheme based on attribute signature with access structure as circuit.

In terms of traceability and revocability, Escala et al. [4] proposed a revocable attribute-based signature scheme in 2011. In 2015, Wei et al. [5] proposed a revocable attribute-based signature scheme using the threshold structure. In 2016, Wei et al. [6] proposed a revocable and traceable attribute signature scheme at the same time.

In 2017, Sun et al. [7] proposed the removal of outsourcing and decentralized multi-authority attribute-based signatures. Compared with the past, it achieves a stronger attribute privacy and prevents collusion. In 2018, Ren et al. [8] proposed a verifiable attribute-based signature scheme through outsourcing. In 2019, Datta et al. [9] studied attribute-based signatures under the arithmetic model and proposed a scheme where the access structure is an unbounded arithmetic branch program.

In the distributed system of the blockchain, an important factor leading to the high failure rate and low operating efficiency of the blockchain is that the CPU processing capacity of a single system in the distributed system of the blockchain is poor, and the storage capacity is not comparable. Centralized system, in order to solve the problem of insufficient CPU processing capacity and insufficient data storage capacity in the blockchain, this paper proposes an attribute signature algorithm deletion model based on the elliptic curve signature algorithm that can delete the blockchain data signature algorithm.

2. Concepts

2.1 Blockchain

Blockchain is a distributed shared ledger. It abandons the traditional centralized thinking and no longer needs servers and databases in the traditional sense. It makes the cost of the blockchain more low-cost, more efficient, and stronger against attacks. The blockchain uses cryptography as the basis for security protection to ensure that the data in the blockchain cannot be tampered with. The chain storage structure in the blockchain enables the data in the blockchain to be stored and verified. Through the consensus mechanism in the blockchain, data consistency is ensured.

2.2 The Ring signature

The ring signature algorithm was first proposed by Rivest [10] and others. As a group signature scheme, the ring signature algorithm uses an asymmetric encryption mode to generate the corresponding public key and private key, the private key is encrypted, the public key and the encrypted ciphertext Send to the recipient.

The scheme model designed in this paper improves the algorithm based on the elliptic curve of the ring signature algorithm. Under the premise of ensuring the absolute security of the signer's information, it accurately deletes the worthless data signed by multiple users. Deleting redundant data can ensure the operating speed of the blockchain and reduce the failure rate of nodes in a distributed system.

3. Data deletion module based on ring signature

3.1Elliptic curve signature algorithm process

The security of the ECC elliptic curve signature scheme is based on the difficulty of solving the discrete logarithm. In practical applications, the signature process of the ECC signature scheme can be described as the following processes:

User-to-message M **To sign, the steps are as follows:**

① User chooses a random number S As a private key, make $S \in [1, N-1]$

② Calculation $G = S \cdot Q$ among them Q Is the base point of the elliptic curve, G Is the private key S The corresponding public key;

③Calculate signature information M Hash value, $e = H(M)$

④ $s = (e \cdot r)^{-1} \cdot (S + d) \bmod n$ among n To select the degree of the elliptic curve d Is a random number;

⑤Among them (r, s) is true M Signature;

Other users receive message signature (r, s) Later, it will need to be signed and verified. To verify the signature, there will be the following steps:

① Calculation $e = H(M)$

②Calculation $w = (e \cdot r) \cdot s \bmod n = (S + d) \bmod n$

③ Calculation $w \cdot Q - G = (SQ + dQ) - dQ = (x_1, y_1)$ among them (x_1, y_1) Is a point on the ellipse;

④ Calculation $v = x_1 \bmod n$

If $v = r$ Prove that the signature is correct, otherwise discard it.

Based on this, this article improves the ECC signature algorithm to achieve the purpose of this article.

3.2 Improved on the ring signature elliptic curve algorithm

Among the many asymmetric encryption algorithms that can be used as ring signature algorithms, this article chooses to use the ECC elliptic curve encryption scheme, and the signing user will randomly choose his own private key S Calculate the public key corresponding to the private key $G = S \cdot Q$ Q It is a base point of the elliptic curve, when users use the ECC algorithm to generate their own public and private keys. After the transaction is initiated, a collective public key set can be generated with all users of the transaction $F = \{G_1, G_2, G_3, ..., G_n\}$ Private key $P = \{S_1, S_2, S_3, ..., S_n\}$ set After all users sign the transaction, in order to ensure the privacy of the user's own information, the entire transaction process can be considered as a ring, and the entire signature becomes a ring signature.

When users sign, use their own public key G Plaintext message m Encryption operation, at this time the private key of the user signature call S The improved **algorithm steps are as follows:**

①Set user signature private key S The time attribute of each signature is t_n, The signature attribute of the user's public key is k The number of transactions is constant m;

②The time attribute private key after signing is $C = S \cdot k$ $k = m \cdot t$;

③The corresponding attribute public key after the private key signature is $Z = t \cdot G$;

④After signing, the public key signature of all signing users is Z_n, After signing, this part of the user's public key is stored in the signing order to form a signature public key set F;

⑤After signing the public key, all the public key sets of the public key are $Z_n = \{t_1 \cdot G_1, t_2 \cdot G_2, t_3 \cdot G_3, ..., t_n \cdot G_n\}$ The private key saved in the user at this time is $Cn = \{m_1 \cdot t_1 \cdot S_1, m_2 \cdot t_2 \cdot S_2, m_3 \cdot t_3 \cdot S_3, ..., m_n \cdot t_n \cdot S_n\}$

⑥ For n The ring signature formed by members is Ts; $Ts = \{M, Z_1, Z_2, Z_3, ..., Z_n\}$

After the signature is completed, when the data reaches the preservation time limit, reaches the preservation purpose, or loses the preservation value, this part of the data can be deleted in the distributed storage of the blockchain.

3.3 Verify the signature process

When the stored data reaches the set delete operation trigger condition, the order data will be based on the public key set signed in the order F The public key in is returned to each signing user. At this time, the signing user will confirm the identity with the returned public key. Z_n Return to the user, at this time the user calls out his private key C_n The steps of the authentication process are as follows:

① $Z = t \cdot G$, Calculate the attribute public key;

② $k' = m \cdot t$ Calculate and public key attributes k Attribute value stored with the private key m and t;

③ $C = S \cdot k'$ Verify the attribute private key;

④ k and k' Is it consistent;

Due to time t Is a known attribute and can be combined with the public key set Z_n Announce the same and use it as a data time node. During the verification process, if $k = k'$ It proves that the identity in the signature is correct, if $k \neq k'$ The identity verification is incorrect.

When the identity verification is passed, all users can choose to vote to decide whether to delete data. Sign order $Ts = \{M, Z_1, Z_2, Z_3, ..., Z_n\}$ in order to delete.

4. Security Analysis

This section analyzes the security, concealment and unforgeability of the data deletion model of the improved ring signature algorithm.

4.1 Improve the security analysis of ring signatures

The ring signature algorithm used in this article is computationally difficult $G = S \cdot Q$ It is a pair of discrete logarithms on the elliptic curve, which is very difficult in calculation, so the security of the private key can be fully guaranteed.

In the improved algorithm, add a constant that is only saved by the user n and k The calculation difficulty is consistent with that of the original algorithm, which also ensures that the improved algorithm will not be forged.

In addition, suppose there is an attacker impersonating a user in the blockchain to sign, and let the attacker be a member of the ring or an attacker who controls the operation of a member of the ring ID_i Then when the attacker performed the attack, the signature was forged $Ts' = \{M, Z_1, Z_2, Z_3, ..., Z_n\}$ The signature is correct, and the data can also be confirmed and processed normally, but when the deletion operation is performed, the signing public key of the order is returned to the signing user, the signing user will first verify $k = k'$ or $k \neq k'$ Because the attacker does not know that the order is the result of the user's signature after how many transactions, and this time Ts' Signing users have no timeline t is recorded. Therefore, it is not possible to impersonate a user to perform signature operations.

4.2 Unforgeability analysis

After signing the user received the returned public key is Z It will perform self-signature verification to check whether it is the user's own signature. At this time, if an attacker impersonates the user to generate a fake user's public key G With a private key of S' Sign the fake user. Timeline generated at this time t With fake public key attributes k' All attackers ID_i Attributes.

After the fake signature is performed at this time, the signature $Ts' = \{M, Z_1, Z_2, Z_3, ..., Z_n\}$

The signature operation is completed, but the timeline of the user signing in the node t It is an attribute known to all signing users, and the verification formula is:

① $G = S' \cdot Q'$,At this time the forger knows the public key, S' and Q' Randomly set a value for the counterfeiter;

② $Z_i' = t_i' \cdot G_i'$ The attribute public key of the forger can be calculated;

③ $k' = t \cdot m'$ The forger can only know the signing time and the number of signatures m' Is also forged, so the attribute value k' It is also forged by a forger;

④ The forger's signature is: $Ts' = \{M, Z_1, Z_2, Z_3, ..., Z_n\}$

⑤ However, the signature process of the real user is: obtain the public key G $G = S \cdot Q$

⑥ The attribute public key is: $Z = t \cdot \{G_1, G_2, G_3, ..., G_n\}$

⑦ $k = m \cdot t$ Attribute value k;

⑧ The real signature is: $Ts = \{M, Z_1, Z_2, Z_3, ..., Z_n\}$

⑨The public key set is returned in the verification signature F the key to signing Ts And creating signatures Ts' the Comparison, and value attribute k and k' is the comparison, at this time you get $Ts \neq Ts'$ $k \neq k'$

The above equation can verify the forgery of the attacker's signature in the signature and cannot replace the original real user to sign, because the attacker uses all public keys known to the user in

the signature G ,But can't know the public key attribute k And detailed transaction records of real users m .

4.3 Forged block control attacks

Suppose there are some fake blocks x ,the total nodes is N The number ratio is x/N If the probability of normal nodes transmitting logistics data is $(N-x)/N$ The probability of the fake node transmitting the logistics information data is x/N .

Therefore:

$(N-x)/(x/N)>1$

$(x/N)/(N-x)<1$ From the perspective of the quantitative relationship between normal blocks and counterfeit blocks, it satisfies the Poisson distribution law. Therefore, we can draw a correlation equation to set the probability of a successful counterfeit block attack for P

$$P=\lim_{\lambda\to\infty}\sum_{\alpha\le k\le\beta}\frac{\lambda^{k}e^{-\lambda}}{k!}\cdot(\ (N-x)\ /N)^{x}$$

α and β Is the interval of the number of nodes, x Is the number of forged blocks. From this formula, it can be concluded that when the number of forged blocks increases, the total number of blocks increases, and the overall probability of success P Into a downward trend. Therefore, the relationship between the anti-attack ability of the ring signature algorithm in the blockchain and the number of forged attack blocks is shown in Figure 1:

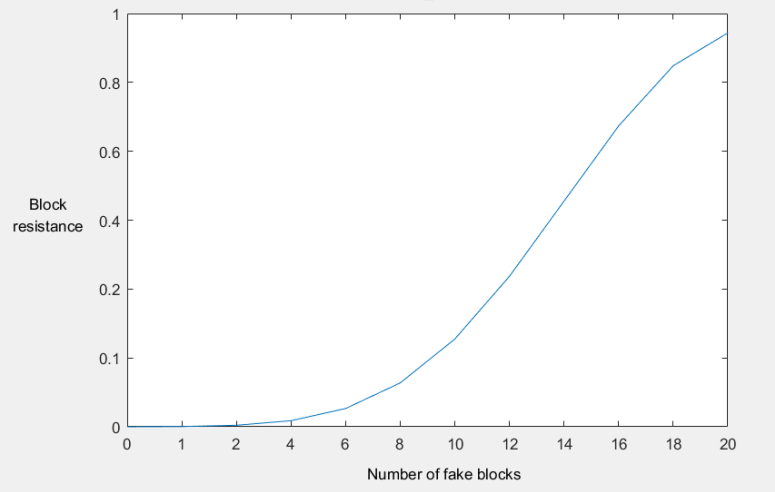

Figure 1. Anti-counterfeit block attack test

It can be concluded that the greater the number of forged blocks, the stronger the ability of the ring signature algorithm to resist attacks on forged blocks.

Conclusion

This paper proposes a data deletion model based on the improved ECC elliptic curve ring signature algorithm to solve the slow running speed and downtime caused by the insufficient storage capacity of the blockchain. The improved ring signature algorithm enables users to ensure their own security in the process of signing, ensuring that user information is invisible, and can resist forged user attacks, forged block attacks, and brute force attacks. Greatly strengthen the safety of users. This article proposes a good solution to the problem that the distributed system of the blockchain runs slowly and the failure rate is too high.

References

[1] Maji H,Prabhakaran M,Rosulek M.Attribute-based signatures: achieving attribute-privacy and collusion-resistance [EB/OL].(2008) [2019-08-13].https://eprint.iacr.org/2008/328.pdf.

[2] Okamoto T, Takashima K. Efficient attribute-based signatures for non-monotone predicates in the standard model[J]. IEEE Trans on Cloud Computing, 2014, 2(4):409-421.

[3] Tang Fei,Li Hongda,Liang Bei.Attribute-based signatures for circuits from multilinear maps [C]//InformationSecurity. Cham: Springer-Verlag, 2014:54-71.

[4] Escala A,Herranz J,Morillo P,et al. Revocable attribute-based signatures with adaptive security in the standard model [C]// Progress in Cryptology-Africacrypt 2011. Berlin: Springer-Verlag, 2011: 224-241.

[5] Wei Jianghong, Huang Xinyi,Hu Xuexian,et al.Revocable threshold attribute-based signature against signing key exposure [C]// Information Security Practice and Experience. Cham: Springer-Verlag, 2015:316-330.

[6] Wei Jianghong,Huang Xinyi,Liu Wenfen,et al. Practical attribute-based signature: traceability and revocability[J].The Computer Journal, 2016, 59(11):1714-1734.

[7] Sun Jiameng, Qin Jing,Ma Jixin.Securely outsourcing decentralized multi-authority attribute based signature [C]// Cyberspace Safety and Security. Cham: Springer-Verlag, 2017: 86-102.

[8] Ren Yanli, Jiang Tiejin. Verifiable outsourced attribute-based signature scheme[J].Multimedia Tools and Application, 2018, 77(14): 18105-18115.

[9] Datta P,Okamoto T,Takashima K.Efficient attribute-based signatures for unbounded arithmetic branching programs [C]// Public-Key Cryptography-PKC 2019. Cham: Springer-Verlag, 2019: 127-158.

[10] Ronald L.Rivest, Adi Shamir, and Leonard M.Adleman.A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM vlo.21, no.2,pp.120-126, 1978.2.