2021 IEEE International Conference on Consumer Electronics and Computer Engineering (ICCECE 2021)

2021 IEEE International Conference on Consumer Electronics and Computer Engineering (ICCECE) | 978-1-7281-8319-0/20/$31.00 ©2021 IEEE | DOI: 10.1109/ICCECE51280.2021.9342568

A Distributed Authentication Scheme Based on Zero-knowledge Proof

Lang Qin
Department of Electronic and Information Engineering
Shenzhen University
Shenzhen, China
1910433069@email.szu.edu.cn

Feng Ma
Department of Electronic and Information Engineering
Shenzhen University
Shenzhen, China
Mafeng0909@163.com

Hao Geng Xie
Department of Electronic and Information Engineering
Shenzhen University
Shenzhen, China
1611163329@qq.com

Sheng Li Zhang
Department of Electronic and Information Engineering
Shenzhen University
Shenzhen, China
zsl@szu.edu.cn

Abstract— As an underlying technology and infrastructure, blockchain creates great value when combining with other emerging information technologies, such as Artificial Intelligence, Big Data Analysis, Cryptography Technology. Although the blockchain system has been contunuously upgraded in recent years, current blockchain still has its deficiency in terms of node control and privacy protection. First of all, the high existence rate of malicious nodes in the chain made it difficult to well purify the network environment, meanwhile the malicious nodes cannot be easily dealt with. Secondly, the correlation between nodes can still be discovered through analysis. As a result, the privacy of users' information cannot be well protected. This paper proposes a distributed identity authentication scheme based on Zero-knowledge proof, which uses face recognition technology to ensure the uniqueness and legitimacy of identity and control the generating of malicious nodes; Zero-knowledge proof algorithm is used to encrypt and support face data to prevent user identity information from being disclosed. At the same time, the linkable ring signature algorithm is adopted to confuse the correspondence between nodes and private information to further protect users' privacy information.

Keywords- Blockchain; Smart contract; Zero-knowledge Proof; Linkable ring signature

I. Introduction

In the information and data age**,** the user's personal information becomes more and more valueable consequently the losses caused by data leakage continuously escalates. It also brings issues on bad social impact and even national security threats. According to incomplete statistics**,** in 2019 alone**,** there were 43 breaches of user data released through public channels**,** involving 16 countries and 11 industries worldwide. It can be seen that the traditional means of identity information authentication-the way of completing the authentication of the user's personal information and storing it in the backend of the server has been difficult to protect the user's personal identity information and privacy. For the blockchain domain with de-centralization as the core feature, how to achieve identity information authentication without disclosing users' identity information through technical means becomes particularly important.

Since the release of the Satoshi Nakamoto white paper[1] in 2008, in the past ten years of technology and application evolution, the blockchain is a peer-to-peer payment protocol described in the Satoshi Nakamoto white paper, which natively supports payment and weakening on the basis of a third party, combined with more technology and application requirements, it has gradually developed into a "world computer". However, blockchain still has problems such as insufficient control ability and imperfect confidentiality, that is, the existence rate of malicious nodes in the chain is very high, and malicious nodes will not be dealt with accordingly. The connection between nodes can be mined, and the privacy of user information cannot be well guaranteed.

More and more scholars are trying to solve these problems. In literature[2], a distributed network user authentication mechanism using key distribution was proposed, but the scheme cannot resist the attacks caused by disguised attacks and identity leakage. Literature[3][4] proposed a password-based anonymous identity authentication key exchange protocol, but this scheme uses a password table on the server side, which requires a large number of exponential calculations and is not efficient.Monero[5] combines three mechanisms of stealth address, ring signature[6] and ring confidential transaction (ringCT)[7] to realize transaction anonymity. However, the use of ringCT will lead to a huge transaction scale, and it is now considering replacing the original ring confidential implementation with a Zero-knowledge proof algorithm.In 2013, Zerocoin[8], a decentralized anonymous payment scheme based on the Bitcoin model was proposed. It adopted the Zero-knowledge proof NIZK scheme[9] to enhance the anonymity of Bitcoin payments by hiding the address of the issuer. In 2014, the Zerocoin team proposed the idea of Zerocash[10]. Zerocash divides the wallet address into a hidden address and a transparent address. The transaction information of the transparent address is publicly visible, while the address of the

978-1-7281-8319-0/21/$31.00 ©2021 IEEE

hidden address transaction, the amount of funds and the remark field are encrypted. Then it verifies the transaction under the network consensus rule by Zero-knowledge proof. However, this method still cannot solve the problem of the high rate of malicious nodes in the blockchain. The Hyperledger Indy[11] project is a virtual mirror of the real world, which aims to migrate the management mechanism of the real world to the virtual world.It is proposed by the Sovrin Foundation with the standards and verification methods for all authentication materials. Nodes that need to be authenticated can be authenticated on the Indy chain. However, it cannot solve the problem of the high rate of malicious nodes in the blockchain, and it cannot effectively protect the relationship between nodes and private information. It only provides a function that can be used for identity verification.

To solve the above-mentioned problems, this paper proposes a distributed identity authentication scheme based on Zero-knowledge proof.

(1) According to the characteristics of identity authentication, this paper uses face recognition technology to ensure the uniqueness and legitimacy of the identity, and control the generation of malicious nodes.

(2) In order to ensure the privacy of user identity, Zero-knowledge proof theory is introduced, which can make the system believe the uniqueness and legitimacy of user identity without disclosing users' identity information.

(3) The link ring signature algorithm[12] is used to confuse the correspondence between nodes and private information to further protect users' privacy.

The paper is organized as follows：Section II describes the relevant knowledge of the technology used in this paper. Section III explains the overall framework and implementation process of the scheme in detail.In section IV**,** the project summary and future work are discussed in conclusion.

II. Related Knowledge

A. *Zero-knowledge Proof Algorithm*

Zero-knowledge proof means that the prover can convince a verifier that a statement is true without revealing anything else. The prover convince the verifier that he knows or possesses a certain message, but through the certification process, no information about the certified message will be disclosed to the verifier. It has been proved that Zero-knowledge proof is very useful in cryptography. It has three core properties[13]:

Completeness: Given a statement and a witness, the prover can convince the verififier.

Soundness: A malicious prover cannot convince the verififier of a false statement.

Zero-knowledge: The proof does not reveal anything but the truth of the statement, in particular it does not reveal the prover's witness.

B. *Linkable Ring Signature Algorithm*

Ring signatures allow a member of the ring to sign on behalf of all ring members without revealing their identity, thereby providing the anonymity of the signer. The disadvantage of ring signatures is that no one can determine whether the issuers of two ring signatures are the same person, which leads to many limitations in the actual application of ring signatures.

In 2004, Liu et al. proposed the idea of adding the definition of linkability to ring signatures. In this concept, the identity of the actual signer is still anonymous in the ring, but if the two ring signatures are issued by the same person, then these two ring signatures can be linked.

C. *Related address introduction*

- One-time address:The one-time address refers to the intermediate address generated by the user registering for the on-chain account for the first time. Each user can generate only one one-time address. A one-time address can only initiate a one-time address verification transaction, no other transactions can be made, and no virtual currency can be received.
- Primary address:The primary address is the user's account address on the chain, which can be regarded as a child address with a one-time parent address. Each primary address is associated with a legal one-time address through a linkable ring signature, and the dependency relationship is not visible, which means that each user can only have one primary address. The primary address can be used to participate in all on-chain activities such as mining and community voting.
- Privacy address:The privacy address has the same function as the primary address, which can be regarded as the child address generated by the primary address or other private address as the parent address. The generation of a private address is determined based on the user's transaction volume. Users who exceed a certain transaction volume can generate a private address.

III. Proposed Method

In this section we explain our proposed distributed identity authentication scheme based on Zero-knowledge proof. First the architecture and concept of the scheme is discussed, and then the concrete flow of the scheme implementation is given.

A. *Solution Architecture*

Figure 1 shows the overall architecture of the scheme, which includes ethereum public chain, face recognition module, Zero-knowledge proof module, address generating module, linkable ring signature module and front-end interface.

Among them, the Ethereum public chain serves as the underlying operating environment of the entire system; the face recognition module is mainly used to extract the face information in the photo of the person holding the ID card and verify whether it is the same person. Only when the verification is passed can the registration continue; The Zero-knowledge proof module is mainly used to generate and verify the proof of the face data comparison process; Address generating module is mainly used to generate one-time addresses, primary addresses and private addresses; The linkable ring signature module is mainly used for one-to-one association of various addresses, but the dependencies are not visible; The front-end interface is mainly to provide a visual operation platform, allowing users to use it more conveniently.

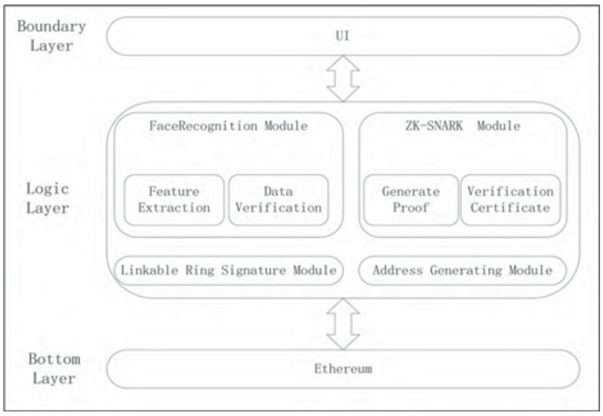

Figure 1: The overall structure of the proposed scheme

B. Solution implementation process

The specific process of this program is shown in Figure 2.

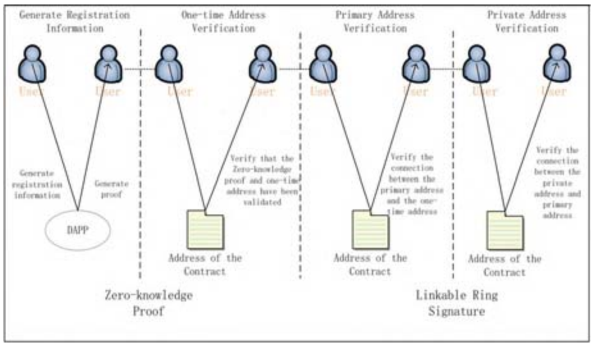
Generate Registration Information
One-time Address Verification
Primary Address Verification
Private Address Verification
User
User
User
User
User
User
User
User
Generate registration information
Generate proof
DAPP
Verify that the Zero-knowledge proof and one-time address have been validated
Address of the Contract
Verify the connection between the primary address and the one-time address
Address of the Contract
Verify the connection between the private address and primary address
Address of the Contract
Zero-knowledge Proof
Linkable Ring Signature

Figure 2: Distributed authentication process based on zero-knowledge proof

a) Generate registration certification

First, the user logs in via the front interface and then registers the account address on the chain.During registration, a picture of a person holding an ID card should be taken in real time and uploaded. Two faces should be found in the photo through the face recognition module, and then corresponding facial feature data should be extracted respectively to determine whether the two person are the same one. When the error value is within the set range, the person would be recognized as the same one and the identity verification would be passed.

After the authentication is passed, the Zero-knowledge proof module is used to convert the face data comparison process into a Zero-knowledge proof. This process is divided into Zero-knowledge proof setup process, proof process and verification process.

The setting process refers to generating a certification key and a verification key, and generating a constraint relationship according to the face data comparison process and converting it into a QAP description, generating $u_i(x), v_i(x), w_i(x)$ and $t(x)$; The proof process is divided into two steps, generating linear relationship and generating proof $\pi = \prod \sigma$; The verification process refers to verification based on the constraint relationship and the proof process data. The implementation process of this program is as follows:

Z_p^* is defined as a p order finite multiplication cyclic group, G_1 , G_2 and G_T are three finite groups, and the corresponding generators are $g, h, e(g,h)$ respectively. The calculation of a finite group of G_1 is represented by $[y]_1 = g^y$, and the calculation of the finite group of G_2 is represented by $[y]_2 = h^y$. G_1 and G_2 to G_T are a bilinear mapping.

(1)Setting process: Randomly select $\alpha, \beta, \gamma, \delta, \chi \leftarrow Z_\pi^*$ to generate $\sigma \in F^m, \tau \in F^n$.

$$\tau = (\alpha, \beta, \gamma, \delta, x), \sigma = ([\sigma_1]_1, [\sigma_2]_2) \tag{1}$$

$$\sigma_1 = (\alpha, \beta, \delta, \{x^i\}_{i=0}^{n-1}, \left\{\frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\gamma}\right\}_{i=0}^{l}, \left\{\frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\delta}\right\}_{i=l+1}^{m}, \left\{\frac{x^i t(x)}{\delta}\right\}_{i=0}^{n-2}) \tag{2}$$

$$\sigma_2 = (\beta, \gamma, \delta, \{x^i\}_{i=0}^{n-1}) \tag{3}$$

(2)Proof process: Two parameters r and s are randomly selected to calculate $\pi = \prod \sigma = ([A]_1, [C]_1, [B]_2)$.

$$A = \alpha + \sum_{i=0}^{m} a_i u_i(x) + r\delta \tag{4}$$

$$B = \beta + \sum_{i=0}^{m} a_i v_i(x) + s\delta \tag{5}$$

$$C = \frac{\sum_{i=l+1}^{m} a_i(\beta u_i(x) + \alpha v_i(x) + w_i(x)) + h(x)t(x)}{\delta} + As + rB - rs\delta \tag{6}$$

(3)Verification process: Verify whether the following equation is true.

$$[A]_1 \cdot [B]_2 = [\alpha]_1 \cdot [\beta]_2 + \sum_{i=0}^{l} a_i \left[\frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\gamma}\right]_1 \cdot [\gamma]_2 + [C]_1 \cdot [\delta]_2 \tag{7}$$

b) One-time address authentication

After the registration authentication certificate is generated, the user can generate the corresponding one-time address based on the ID number in the photo of the person holding the ID card. The generation process is similar to the ordinary address of Ethereum[14]： Based on the elliptic curve encryption standard, a 256-bit string is generated as the private key according to the ID number, and the public key and address are calculated. Here we assume that a one-time account (pk_{temp}, sk_{temp}) is generated, pk_{temp} is the public key, and sk_{temp} is the private key.

Once the one-time address is generated, the transaction can be initiated through the one-time address verification contract. When a one-time address authentication transactio- n enters the transaction pool of a public chain node, the correctness of the transaction will be verified, invalid transactions will be directly discarded, the node will not forward, and these invalid transactions cannot be packaged in the block. When the smart contract is executed, a Zero-knowledge proof is calculated to determine whether the face data comparison process is correct, and to check whether the one-time address has been used. If it has been used, the registration would be refused to continue. Otherwise, the one-time address in the internal space of the contract would be stored. All legal one-time addresses are stored in a separate space, separated from other ordinary addresses.

c) Primary address authentication

After the one-time address authentication is passed, the primary account address can be generated and verified. The user first generates a set of primary account key pairs (pk_{main}, sk_{main}), pk_{main} is the public key, and sk_{main} is the private key; Then the user generates a linkable ring signature pk_{main} for the public key σ of the master account; Finally, a transaction is initiated to the primary address contract to verify the linkable ring signature, which in turn proves that the primary account address is associated with the one-time address.

The specific implementation process of this program is as follows:

(1)GEN:The signer selects the private key $x \in [1, l-1]$ to generate a characteristic label g_0 (the label generated by each user is unique and verifiable). At the same time, a one-time public key is randomly selected on the blockchain to form a set $S = \{p_i | = 1,2,...,n\}$, where $p_s = pk_{temp}$. $H_p(p_i)$ is a point on the elliptic curve, $g_0 = p_s H_p(S)$.

(2)SIG: The signer chooses a random number:

$$\{q_i | i = 0,1,...,n, q_i \in [1,l]\} \tag{8}$$

$$\{w_i | i = 0,1,...,n, i \neq s, w_i \in [1,l]\} \tag{9}$$

Perform the following transformation:

$$L_i = \begin{cases} q_i G, & i = s \\ q_i G + w_i p_i, i \neq s \end{cases} \tag{10}$$

$$R_i = \begin{cases} q_i H_p(p_i), & i = s \\ q_i H_p(p_i) + w_i g_0, i \neq s \end{cases} \tag{11}$$

Conduct the next step calculation:

$$c = H_p(m, L_1, ..., L_n, R_1, ..., R_n) \tag{12}$$

Conduct the signer calculation:

$$c_i = \begin{cases} w_i, & l = s \\ c - \sum_{k=0}^{n} c_i \bmod l, l \neq s \end{cases} \tag{13}$$

$$\sum_{k=0}^{n} c_i = H_p(m, L'_1, ..., L'_n, R'_1, ..., R'_n) \tag{14}$$

The final signature is:

$$\sigma = (g_0, c_1, ..., c_n, r_1, ..., r_n) \tag{15}$$

(3) VER: When the verifier verifies the signature, it is calculated based on the message m, the sum of public parameters, and the signature:

$$\begin{cases} L'_i = q_i G + c_i P_i \\ R'_i = r_1 H_p(P_i) + c_i g_0 \end{cases} \tag{16}$$

Verifier calculation:

$$\sum_{k=0}^{n} c_i = H_p(m, L'_1, ..., L'_n, R'_1, ..., R'_n) \tag{17}$$

If they are equal, the signature is proved legal. We can determine whether a person performs multiple registration signatures by verifying the feature tag. If he does so, the verifier would reject the registration operation. After the primary address authentication transaction is generated, it will be broadcast to all blockchain nodes. After receiving the authentication transaction, the node will verify whether the format of the main address verification transaction is correct. Based on message $M(pk_{main})$, public key set S and signature σ, verify whether the chainable ring signature is valid and whether the chainable ring signature public key set is a legal one-time address public key. Invalid primary address verification transactions will be discarded directly.

After the address contract receives the primary address verification request, if the primary address is already in use, it rejects the primary address verification request. Otherwise, store the main address transaction verification information in the storage space of the contract. Since the label generated by an address is unique, a one-time account can generate only one valid primary address.

d) Private address authentication

The generation of a private address is determined based on the user's transaction volume. Users who exceed a certain transaction volume can generate a private address. After the transaction volume of the private address reaches a certain amount, the corresponding private address can be continuously generated. Each private address is associated with the primary address or other private addresses through a linkable ring signature.

The authentication process of the private address is similar to that of the primary address. The difference is that the parent address of the private address can be the primary address or the private address.

IV. CONCLUSION

This paper proposes a distributed identity authentication scheme based on Zero-knowledge proof, which uses face recognition, Zero-knowledge proof algorithm and linkable ring signature technology. On the issue of user identity authentication, Zero-knowledge proof can protect the privacy of user information and ensure the correctness of the authentication result while completing the interaction in identity authentication. Face recognition technology ensures the uniqueness and legitimacy of the user's identity, and the linkable ring signature technology confuses the correspondence between nodes and private information, thus effectively protecting user's privacy. The scheme eliminates the security loophole well and has good anonymity and authentication.

In the next step, we will further improve the program by combinating with cryptography technology to reduce the complexity of the algorithm while ensuring user information privacy and improving the management and control capabilities of blockchain nodes.

ACKNOWLEDGMENT

This paper is partially supported by Shenzhen Base Research Fundation projects with no. JCYJ20170412104656685，JCYJ20170302142312688.

REFERENCES

[1] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system [Online], available: https://bitcoin.org /bitcoin.pdf, 2009

[2] W.B. Lee, C.C. ChangUser identification and key distribution maintaining anonymity for distributed computer network Comput. Syst. Sci., 15 (4) (2000), pp. 211-214

[3] Viet D.Q., Yamamura A., Tanaka H. (2005) Anonymous Password-Based Authenticated Key Exchange. In: Maitra S., Veni Madhavan C.E., Venkatesan R. (eds) Progress in Cryptology - INDOCRYPT 2005. INDOCRYPT 2005. Lecture Notes in Computer Science, vol 3797. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11596219_20

[4] Yang J., Zhang Z. (2008) A New Anonymous Password-Based Authenticated Key Exchange Protocol. In: Chowdhury D.R., Rijmen V., Das A. (eds) Progress in Cryptology - INDOCRYPT 2008. INDOCRYPT 2008. Lecture Notes in Computer Science, vol 5365. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978- 3-540-89754-5_16

[5] Monero project. https://getmonero.org/.

[6] Zhang F., Kim K. (2002) ID-Based Blind Signature and Ring Signature from Pairings. In: Zheng Y. (eds) Advances in Cryptology — ASIACRYPT 2002. ASIACRYPT 2002. Lecture Notes in Computer Science, vol 2501. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-36178-2_33

[7] Noether, S., Mackenzie, A., & Research Lab, the M. (2016). Ring Confidential Transactions. Ledger, 1, 1-18. https://doi.org/10.5195/ledger.2016.34

[8] Miers, C. Garman, M. Green and A. D. Rubin, "Zerocoin: Anonymous Distributed E-Cash from Bitcoin," 2013 IEEE Symposium on Security and Privacy, Berkeley, CA, 2013, pp. 397-411, doi: 10.1109/SP.2013.34.

[9] Groth J. (2006) Simulation-Sound NIZK Proofs for a Practical Language and Constant Size Group Signatures. In: Lai X., Chen K. (eds) Advances in Cryptology – ASIACRYPT 2006. ASIACRYPT 2006. Lecture Notes in Computer Science, vol 4284. Springer, Berlin, Heidelberg. https://doi.org/ 10.1007/11935230_29

[10] E.B. Sasson et al., "Zerocash: Decentralized Anonymous Payments from Bitcoin," 2014 IEEE Symposium on Security and Privacy, San Jose, CA, 2014, pp. 459-474, doi: 10.1109/SP.2014.36.

[11] Dhillon V., Metcalf D., Hooper M. (2017) The Hyperledger Project. In: Blockchain Enabled Applications. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-3081-7_10

[12] Liu J.K., Wei V.K., Wong D.S. (2004) Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups. In: Wang H., Pieprzyk J., Varadharajan V. (eds) Information Security and Privacy. ACISP 2004. Lecture Notes in Computer Science, vol 3108. Springer, Berlin, Heidelberg. https://doi.org/ 10.1007/978-3-540-27800-9_28

[13] Goldreich, O., Oren, Y. Definitions and properties of zero-knowledge proof systems. J. Cryptology 7, 1–32 (1994). https://doi.org/10.1007/BF00195207

[14] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger", Ethereum Project Yellow Paper, 2014