Anonymous Transaction of Digital Currency Based on Blockchain

Yang Liu, Mingxing He, and Fangyuan Pu
(Corresponding author: Mingxing He)

School of Computer and Software Engineering, Xihua University
999 Jin Zhou Road, Jin Niu District, Chengdu, 610039, China
(Email: he_mingxing64@aliyun.com)

(Received Aug. 3, 2018; Revised and Accepted Jan. 24, 2019; First Online Oct. 14, 2019)

Abstract

Blockchain can be seen as a shared database, and keep all data public and traceable. Everyone is accessible to the data recorded on the blockchain, which brings the risk of privacy leakage. When digital currency transactions are performed on the blockchain, users may not want to reveal their real identities. Therefore, it is particularly important to preserve the identity privacy of users. To solve the problem, we present an anonymous transaction scheme of digital currency to ensure the anonymity of the sender and receiver. we design a linkable ring signature algorithm based on elliptic curve cryptography (ECC) to conceal the real identity of sender and check double-spending. It is intermediate address that is used for concealing the real identity of receiver. Furthermore, we utilize a agency to reduce computational burden for receiver. Throughout the transaction process, the real identities of two sides are not disclosed to others, ensuring anonymous transaction.

Keywords: Anonymous Transaction; Blockchain; Digital Currency; Linkable Ring Signature

1 Introduction

The essence of blockchain is a huge distributed database without unified manager. The data is stored in blocks, and all blocks are linked in the form of chain structure. All records on the blockchain are public and traceable. Users can believe in records on the blockchain, and not have to trust the third parties such as banks or governments. Blockchain is mostly used for storing transactions information to keep traceable and avoid central domination. It has wide application prospect in various fields, especially digital currency.

Bitcoin [16] is regarded as the first digital currency based on blockchain, and also the most typical and successful application of blockchain technology. Bitcoin transactions are verified by all nodes on the blockchain and can never be falsified. All digital currencies based on blockchain that appear after Bitcoin are derived from Bitcoin. Therefore, our scheme can also be regarded as being based on Bitcoin.

To verify transactions without relying on the third parties, blockchain must build consensus among distributed nodes [8]. Therefore, all records on the blockchain must be public and can be viewed by any node, which leads to plenty of private information being exposed [10].

In response to the demand for privacy-preserving, there are some schemes have been proposed. Most schemes utilize mixing coins, being divided into centralized and decentralized. The idea of mixing coins originates from the paper published by Chaum [3]. It is used to achieve anonymous communication between the two sides through the intermediary transferring information, so that the attacker is unable to accurately determine whether the two sides communicate. The mixing coins in the transaction of digital currency draws on this idea, and confuses the transaction contents without changing the transaction results, hiding the relationship between input and output.

Some centralized mixing coins are operated by the third parties. Many companies offer mixing coins service to make money, such as Bitcoin Fog and Bitlaunder. Users can enjoy the mixing coins service after paying the service fee, but this approach carries the risk of funds being stolen by the third parties. There are some centralized mixing cions algorithms by utilizing a central node to execute. Mixcoin [2] adds an accountability mechanism to expose theft. Blindcoin [24] is optimizing of Mixcoin, and use blind signature to hide the relationship between input and output. Then, ShenTu *et al.* [22] propose a mixing coins scheme based on blind signature and it increases computational efficiency on the basis of ensuring anonymity. Recently, Liu *et al.* [13] propose a mixing coins scheme based on ring signature with centralized mixing server. However, centralized mixing coins has a distinct shortcoming and the central node may leak the information about mixing coins.

The decentralized mixing coins has been first proposed by Gregory in CoinJoin [14]. It combines multiple transactions into one transaction to provide anonymity for users, which requires users to execute mixing coins autonomously. CoinShuffle [18] designs a shuffle protocol to improve CoinJoin, and requires participants to be online at the same time. Thus, it has low efficiency and is vulnerable to Dos attack. Subsequently, Xim [1] utilizes announcements on the blockchain for aggregating users who want to take part in mixing coins, and is able to resist Dos attack, but it only supports two-party mixing coins and has low efficiency. SecureCoin [7] improves security and efficiency over the CoinShuffle. Coinparty [27] makes use of secure multi-party computation to ensure the availability of mixing coins when there are malicious processing. In short, mixing coins need numerous users to participate and cooperate with each other, so there is still a risk of information leakage.

Many anonymous digital currencies also provide a new way for privacy-preserving. We take Zerocash and Monero as example in the following. Zerocash [20] inherits the thought of Zerocoin [15] scheme, forming the best anonymous digital currency. It converts the user's coins into equivalent commitment. When users want to spend the funds, they utilize zero-knowledge proofs to prove that the funds belong to themselves and have not been spent. It ensures unlinkability of transactions, but has a bottleneck in efficiency. The core of Monero is CryptoNote [19] protocol. It ensures anonymity of transaction by ring signature based on non-interactive zero-knowledge proofs, so it is quite complicated in calculation.

Recently, some new privacy-preserving schemes are proposed about blockchain. Heilman *et al.* [5] present the micropayment channel networks and combine blind signature with smart contract, to achieve the anonymity for Bitcoin transactions. Kosba *et al.* [9] present Hawk scheme, and it combines zero-knowledge proofs with secure multiparty computation to achieve privacy-preserving about smart contract on the blockchain. Yuan *et al.* [26] propose a new ring signature scheme for the transactions on blockchain based on aggregate signature and ECC. When the transaction contains multiple inputs and outputs, it can achieve both hiding the amount of the transactions and constant-size signature, but it is only aimed at privacy-preserving of the transactions, without regarding to double-spending. There are also encryption schemes about identity, such as Liu *et al.* [12] propose an anonymous identity-based encryption scheme, and it improves the SKOS scheme [21] and proves its security under l-computational Diffie-Hellman assumption.

Based on blockchain, we propose a anonymous transaction scheme about digital currency without the third parties. There are two crucial technologies, that is, linkable ring signature and intermediate address. We design a new linkable ring signature algorithm based on ECC and make use of the advantages of ECC, that is, high security and fast processing. Linkable ring signature is used for concealing the real identity of sender to ensure anonymous payment, and also used for checking double-spending. Namely, double-spending means that someone spends the same money twice, and it especially occurs in the transactions of digital currency. Intermediate address can be regarded as a virtual address, which is generated by sender. Intermediate address is used for concealing the real identity of receiver to ensure anonymous receiving. Nobody has the ability to judge who the intermediate address belongs to, except the sender and receiver. Our scheme is able to preserve simultaneously the identity privacy of two sides and achieve anonymous transaction.

The content of this paper is organized as follows: Section 1 introduces briefly some background knowledge and major components about this paper. Section 2 introduces the preliminaries. Section 3 proposes a linkable ring signature algorithm based on ECC. Section 4 introduces details of our anonymous transaction scheme. we present analysis about our proposed scheme in Section 5. The last section concludes this paper.

2 Preliminaries

2.1 Ring Signature

In 2001, ring signature was first proposed by Rivest, Shamir and Tauman [17]. The signer aggregates an arbitrary set of users (their public keys) with his own private key to form a ring structure in a certain rule. Ring signature provides an anonymous way to sign message without revealing any identity information. The verifiers can be convinced that the signature comes from this group. However, nobody has the ability to identify who is the real signer unless the real signer exposes himself.

In some cases, While ensuring anonymity, we also need to know whether two signatures are signed by the same signer. To solve this problem, Liu *et al.* [11] first propose the concept of linkable ring signature. It has the characteristic of linkability compared to ordinary ring signatures. It can prove whether two signatures are signed by the same signer by means of adding an linkable tag to the signature. If two signatures have the same linkable tag, it means that they are signed by a signer for the same message, so they are linked. Base on this notion, Gu *et al.* [4] present a fully traceable certificateless ring signature scheme. However, it is not enough efficient in judging linkability of signatures.

In this paper, we design a new linkable ring signature algorithm, and utilize the linkability to check double-spending in the transactions of digital currency. To ensure the uniqueness of every linkable tag, we add the private key of signer and the signature of previous transaction to generate the linkable tag.

2.2 Elliptic Curve Cryptography

The elliptic curve cryptography (ECC) is an important branch of the public key cryptosystem (PKC), and its security is based on the difficulty of elliptic curve discrete logarithm problem [23,25]. Compared with the RSA public key cryptosystem, ECC has less computation, faster processing, and less storage space and transmission bandwidth [6]. The Bitcoin also selects ECC as the encryption algorithm. Our scheme is based on ECC and completely compatible with Bitcoin.

We briefly introduce the principle of ECC as following. Consider $A = aP$, where A, P are the points on the elliptic curve E, q is the order of P, and a is an integer less than q. According to the addition rule on the elliptic curve, given a and P, it is easy to compute A, but conversely, given A and P, it is very difficult to find a. Therefore, we usually take a as private key, A as public key.

3 Linkable Ring Signature Based on ECC

Let E represent an elliptic curve defined on a finite field $GF(p)$. Let G be a group with generator P on elliptic curve E. Let q represent the order of P, where q is a large prime number. $L = \{K_1,K_2,\cdots,K_n\}$ represents the list of n public keys. For $i = 1,2,\cdots,n$, each user i has a distinct public key K_i and private key k_i such that $K_i = k_iG$, where $k_i \in [1, q-1]$. It is worth noting that μ represents the signature of previous transaction in our anonymous transaction scheme, that is to say, it stands for the source of the funds in the current transaction, so it is public and unique on the blockchain. We define two cryptographic hash functions :

$$H_1 : \mathbb{Z}_q \to G \text{ and } H_2 : \{0,1\}^* \to \{0,1\}^d.$$

3.1 Signature Generation

Given message $m \in \{0,1\}^*$, list of public keys $L = \{K_1,K_2,\cdots,K_n\}$. Let j stand for the real signer, and the public key K_j corresponding to private key k_j, where $1 \leq j \leq n$. User j generates a linkable ring signature $\sigma(m)$ as following steps:

1) Compute $h = H_1(\mu)$, $W = \mu h$, and $U = \mu G = (x, y)$.

2) Compute $\tilde{h} = xk_jh$, and $(\tilde{h}, U)$ is regarded as linkable tag.

3) Pick $t \in_R [1, q-1]$, and compute $T = tG$, $T' = th$, and $c_{j+1} = H_2(m,\ T,\ T')$.

4) For $i = j$+1, $\cdots$, n, 1, $\cdots$, j-1, pick $s_i \in_R [1, q-1]$, and compute $c_{i+1} = H_2(m,\ s_iG + xc_iK_i + c_iU,\ s_ih + c_i\tilde{h} + c_iW)$, and take $c_1 = c_{n+1}$.

5) Compute $s_j = t - xc_jk_j - c_j\ \mu \pmod q$.

6) Finally, construct the signature

$$\sigma(m) = \{L,\ c_1,\ s_1,\ \cdots,\ s_n,\ h,\ \tilde{h},\ U\}.$$

3.2 Signature Verification

The verifier verifies the validity of the signature $\sigma(m)$ as follows:

1) Extract μ from blockchain, and compute $W = \mu h$.

2) Extract x from U, for $i = 1,2,\cdots,n$, compute $T_i = s_iG + xc_iK_i + c_iU$, $T_i' = s_ih + c_i\tilde{h} + c_iW$, and then $c_{i+1} = H_2(m,\ T_i,\ T_i')$ if $i \neq n$.

3) Check whether $c_1 \overset{?}{=} H_2(m,\ T_n,\ T_n')$. If yes, accept. Otherwise, reject.

3.3 Linkability

Given two signatures,

$$\sigma'(m') = \{L',c_1',s_1',\cdots,s_n',h',\tilde{h}',U'\},$$
$$\sigma''(m'') = \{L'',c_1'',s_1'',\cdots,s_n'',h'',\tilde{h}'',U''\},$$

the verifier checks if $\tilde{h}' \overset{?}{=} \tilde{h}''$ and $U' \overset{?}{=} U''$. If two equations both hold, it means that the linkable tag of two signatures are the same. The verifier can conclude that $\sigma'(m')$ and $\sigma''(m'')$ are linked, namely, they are generated when a user signs two transactions m' and m'' that include the same money. Otherwise, the verifier concludes that two signatures are not linked. Therefore, two signatures are linked if and only if their linkable tags are the same.

In our anonymous transaction scheme, the linkable tag is generated by utilizing the private key k_j of signer and the signature μ of previous transaction. Because k_j is unique for the signer, and μ is also unique for the funds in the current transaction, the linkable tag is certainly unique. Therefore, two linkable tags must be the same when a user signs two transactions that include the same money, and it indicates that the user spends the same money twice, that is to say, double-spending. Consequently, we check double-spending in our scheme by utilizing the linkability of linkable ring signature.

3.4 Properties of the Signature

This linkable ring signature algorithm based on ECC inherits the characteristics of both ECC and linkable ring signature, like high security, anonymity, linkability, and unforgeability.

1) anonymity. User signs the transaction by utilizing the linkable ring signature. The verifier can be convinced that the signature comes from the group. Since every member of the group has equal position, anyone of the group may generate the signature $\sigma(m)$. Therefore, nobody has the ability to identify who is the real signer unless the real signer exposes himself.

2) linkability. Both the private key k_j of signer and the signature μ of previous transaction are unique, so the linkable tag $(\tilde{h},\ U)$ is certainly unique. If two

signatures have the same linkable tags, and it means that two signatures are linked. If two signatures are linked, they have the same linkable tags. Therefore, two signatures are linked if and only if their linkable tags are the same. When a user signs two transactions that include the same money, two signatures are linked and have the same linkable tags. It indicate that the user spends the same money twice, that is to say, double-spending.

3) unforgeability. Firstly, this linkable ring signature algorithm is based on ECC, and its security is based on the difficulty of elliptic curve discrete logarithm problem. Secondly, the signer generates a valid linkable ring signature $\sigma(m)$ and must use his own private key. If the attacker wants to forge the signature $\sigma(m)$, he must solve the elliptic curve discrete logarithm problem and also hold the real signer's private key. It is difficult to solve the elliptic curve discrete logarithm problem, and he is also unable to obtain the real signer's private key. Therefore, nobody can forge the signature $\sigma(m)$.

4 Transaction Scheme

4.1 Scheme Overview

We present the details of our anonymous transaction scheme in this section. This scheme has a virtual intermediate address and three participants, that is, sender Alice, receiver Bob and agency Carlo. The overview of our anonymous transaction scheme is shown in Figure 1. The symbols used in our scheme are listed in Table 1.

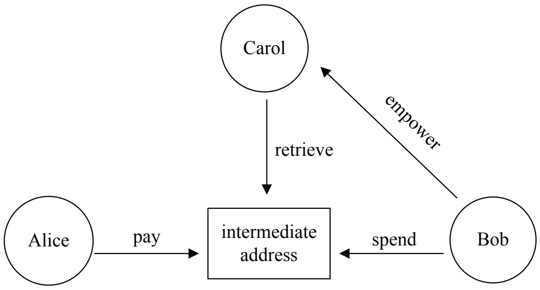

Figure 1: Overview of the scheme

In order to ensure anonymous simultaneously of sender Alice and receiver Bob, they have three public and private key pairs in our scheme as shown in Table 2, that is, a main public and private key pair and two standby public and private key pairs. The main public and private key pair is used for generating linkable ring signature $\sigma(m)$. Two standby public and private key pairs are used for generating the intermediate address and empowering the agency Carlo to retrieve transactions. The intermediate address of our scheme is slightly similar to the stealth address of CryptoNote [19]. However, the difference is that our scheme uses three public and private key pairs and adds an agency Carlo to help receiver Bob retrieve transactions.

It is worth noting that agency Carlo can only be regarded as an assistant to receiver Bob for retrieving transactions. Since it has heavy computational burden to retrieve transactions on the blockchain, our scheme adds an agency Carlo to help receiver Bob retrieve transactions. When Bob empowers Carlo to retrieve transactions on the blockchain, Bob sends anonymously a part of keys to Carlo with a sum of agency fee. Carlo retrieves transactions belonging to Bob on the blockchain. Certainly, Bob can also retrieve it by himself if he has plenty of computing resources. Emphatically, we add the agency in our scheme only when Bob has limited computing resources. The agency is based on reputation for the purpose of making money in our scheme. If the agency has fraudulent behavior, his reputation will be damaged leading to poor business.

Table 1: Symbol and description

Symbol	Description
p	Order of the generator P
H	Hash function
R	Payment evidence
L	The list of public keys
Y	Intermediate address
Y^*	The address computed by agency
K^*	Sum of the Bob's standby public keys
$\sigma(m)$	Linkable ring signature for message m
$(\tilde{h}, U)$	Linkable tag

Table 2: Key and description

Key	Description
$K_{a1} = k_{a1}G$	K_{a1} is the main public key of Alice. k_{a1} is the main private key of Alice.
$K_{a2} = k_{a2}G$ $K_{a3} = k_{a3}G$	K_{a2} and K_{a3} are the standby public keys of Alice. k_{a2} and k_{a3} are the standby private keys of Alice.
$K_{b1} = k_{b1}G$	K_{b1} is the main public key of Bob. k_{b1} is the main private key of Bob.
$K_{b2} = k_{b2}G$ $K_{b3} = k_{b3}G$	K_{b2} and K_{b3} are the standby public keys of Bob. k_{b2} and k_{b3} are the standby private keys of Bob.

4.2 Payment Protocol

Alice intends to initiate a payment of digital currency to Bob, and generates a transaction including receiver's address, payment amount, payment evidence, time-stamp, sender's signature. Let m represent the transaction information. In fact, Alice pays a sum of money to intermediate address instead of the real address of Bob.

Alice generates a transaction as following steps:

1) Obtain the main public key K_{b1} and two standby public keys K_{b2} and K_{b3} of Bob from blockchain.

2) Pick $r \in_R [1, q-1]$, and compute $R = rG$, and compute intermediate address $Y = H(rK_{b1})G + K_{b2} + K_{b3}$. Y is specified as receiver's address. R is specified as payment evidence, which is used for resisting to denial of receiver.

3) Send R to Bob.

4) Use the main public key K_{a1} and main private key k_{a1} to construct the linkable ring signature $\sigma(m)$ by the signature generation algorithm of Section 3.1. $\sigma(m)$ is specified as sender's signature, and it includes linkable tag $(\tilde{h}, U)$.

5) The time-stamp is generated automatically by blockchain to record current time.

6) Finally, broadcast the transaction anonymously to blockchain.

4.3 Verification Protocol

Our transaction scheme is based on blockchain, and it is based on Bitcoin for the process of verifying transaction. Therefore, we omit the details about verifying Bitcoin transaction, and only describe the part of our design.

When the verifier receives the transaction, he firstly checks double-spending then verifies signature $\sigma(m)$. Our scheme requires that all nodes on the blockchain store a spent-list including the linkable tag of every transaction to check double-spending. Every node verifies the transaction as following steps:

1) Extract linkable tag $(\tilde{h}, U)$ from signature $\sigma(m)$.

2) Check $(\tilde{h}, U)$ whether exist in the spent-list. If yes, indicate double-spending and reject this transaction. Otherwise, go on verifying $\sigma(m)$ according to the signature verification algorithm of Section 3.2.

3) If $\sigma(m)$ is verified being valid, this transaction is also valid and can be recorded in blocks, then is added to the blockchain. Otherwise, reject this transaction.

4.4 Retrieval Protocol

Bob empowers Carlo to retrieve transactions on the blockchain When his computing resources are limited. Bob sends anonymously a part of keys to Carlo and does not reveal his own identity. The steps of retrieving transactions are as following:

1) Bob computes $R^* = k_{b1}R$ and $K^* = K_{b2} + K_{b3}$, and sends the set (R^*, K^*) anonymously to Carlo with a sum of agency fee.

2) Carlo computes $Y^* = H(R^*)G + K^*$, and retrieve whether there is a transaction on the blockchain that satisfies $Y^* = Y$. If yes, it stands for this transaction belonging to Bob, and Carlo issues an announcement about this transaction.

3) Once Bob observes this announcement, he looks for this transaction on the blockchain.

4) Bob computes again $H(k_{b1}R)G + K_{b2} + K_{b3}$ to ensure this transaction belong to him.

4.5 Spend Protocol

Bob takes advantage of his own three private keys for computing $x = H(k_{b1}R\ ) + k_{b2} + k_{b3}$, and x is exactly the private key of the intermediate address. When Bob wants to spend the funds, he uses x for signing it. Because only Bob has the private key corresponding to the intermediate address, he can spend the funds instead of others.

5 Analysis

5.1 Anonymity

There are three participants as Alice, Bob and Carlo in our scheme. Carlo is only an agency, who has no knowledge about the relationship between Alice and Bob. Alice as sender signs the transaction by utilizing the linkable ring signature algorithm based on ECC. The verifier can confirm that the signature is generated by someone included in the group. The real identity of signer is absolutely anonymous for any verifier. Therefore, the linkable ring signature ensures the anonymity of the sender.

The intermediate address is used for concealing the real identity of receiver. Alice uses a part of Bob's public keys, and generates the intermediate address. Alice pays the funds to the intermediate address instead of the real address of Bob. No one has the ability to judge who the intermediate address belongs to, except Alice and Bob. Therefore, the intermediate address ensures the anonymity of the receiver. Although we utilize the agency Carlo to help receiver Bob retrieve transactions when he has finite computing resources, Carlo has no knowledge about the real identity of Bob. Bob sends a message anonymously to Carlo, and Carlo replies with an announcement. The receiver Bob is still anonymous for agency Carlo.

5.2 Resistant to Double-spending

Our scheme not only achieves completely anonymous transaction, but also can resist double-spending. When users spend a sum of money, he must sign it by utilizing linkable ring signature in our scheme. Due to the linkability of linkable ring signature, nobody can spend the same money twice. We make use of the linkable tag to realize the linkability and resist double-spending.

Especially, the linkable tag is generated by utilizing the private key k_j of signer and the signature μ of previous transaction on the blockchain. With emphasis, μ stands for the source of the funds in the current transaction and it is public and unique. In addition, every user has unique private key. Therefore, if the malicious user attempts to spend the same money twice, he must sign it twice and result in generating two signatures with the same linkable tags. When there are the same linkable tags, the verifier can conclude that the user spends the same money twice, that is to say, double-spending. Once the verifier finds double-spending, he can reject directly the transaction. Therefore, the malicious user can certainly fail to double-spending.

5.3 Resistant to Denial of Receiver

Since the intermediate address conceals the real identity of the receiver, the receiver can deny that he receives the payment from sender. To solve this problem, the payment evidence R plays a important role in our scheme. R is recorded in the transaction and public to all nodes on the blockchain, but only the sender knows r. When the receiver deny that he receives the payment from sender, the sender can disclose r and prove that he pays indeed a sum of money to the intermediate address and it belongs to the receiver. Once the sender discloses r, all nodes on the blockchain can verify the correctness of $R = rG$. Therefore, all nodes on the blockchain can prove the innocence of sender and expose the denial behavior of receiver.

6 Conclusions

It is transaction information that are public on the blockchain leading to leakage about privacy information. Our scheme aims to ensure anonymous transaction and preserve the identity privacy of two sides in the transaction. We make use of the linkable ring signature to conceal the real identity of sender, and the intermediate address to conceal the real identity of receiver. The funds are deposited in the intermediate address, and only the receiver can spend it, so users do not have to worry about the funds being stolen. Nobody has ability to know the relation of sender and receiver. There is a agency, but he has no knowledge of two sides in the transaction. Furthermore, we add a agency in our scheme only when the receiver has limited computing resources. Certainly, the receiver can also retrieve transactions by himself if he has plenty of computing resources. In short, our scheme achieves completely anonymous. All algorithms used in our scheme are based on ECC having high security, and fully compatible with Bitcoin. It is worth noting that users have three public and private key pairs in our scheme, resulting in a large amount of computation. However, It is significant for us to ensure completely anonymous transactions at the expense of a large amount of computation.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (No. U143310218), by the Chunhui Project of Education Ministry of China (No. Z2014045), by the Science and Technology Bureau Project of Chengdu Municipality (No. 2016-XT00-00015-GX).

References

[1] G. D. Bissias, A. P. Ozisik, B. N. Levine, and M. Liberatore, "Sybil-resistant mixing for bitcoin," in *Proceedings of the 13th Workshop on Privacy in the Electronic Society*, pp. 149–158, 2014.

[2] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, "Mixcoin: anonymity for bitcoin with accountable mixes," in *International Conference on Financial Cryptography and Data Security*, pp. 486–504, 2014.

[3] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–90, 1981.

[4] K. Gu, L. Y. Wang, N. Wu, and N. D. Liao, "Traceable certificateless ring signature scheme for no full anonymous applications," *International Journal of Network Security*, vol. 20, no. 4, pp. 762–773, 2018.

[5] E. Heilman, F. Baldimtsi, and S. Goldberg, "Blindly signed contracts: anonymous on-blockchain and off-blockchain bitcoin transactions," in *International Conference on Financial Cryptography and Data Security*, pp. 43–60, 2016.

[6] M. S. Hwang, S. F. Tzeng, and C. S. Tsai, "Generalization of proxy signature based on elliptic curves," *Computer Standards and Interfaces*, vol. 26, no. 2, pp. 73–84, 2004.

[7] M. H. Ibrahim, "Securecoin: a robust secure and efficient protocol for anonymous bitcoin ecosystem," *International Journal of Network Security*, vol. 19, no. 2, pp. 295–312, 2017.

[8] A. Judmayer, N. Stifter, K. Krombholz, and E. Weippl, "Blocks and chains: introduction to bitcoin, cryptocurrencies, and their consensus mechanisms," *Synthesis Lectures on Information Security Privacy and trust*, vol. 9, no. 1, pp. 1–123, 2017.

[9] A. Kosba, A.Miller, E. Shi, Z. K. Wen, and C. Papamanthou, "Hawk: the blockchain model of cryptography and privacy-preserving smart contracts," in *2016 IEEE symposium on security and privacy*, pp. 839–858, 2016.

[10] I. C. Lin and T. C. Liao, "A survey of blockchain security issues and challenges," *International Journal of Network Security*, vol. 19, no. 5, pp. 653–659, 2017.

[11] J. K. Liu, V. K. Wei, and D. S. Wong, "Linkable spontaneous anonymous group signature for ad hoc groups," in *Australasian Conference on Information Security and Privacy*, pp. 325–335, 2004.

[12] L. H. Liu, Z. Z. Guo, Z. J. cao, and Z. Chen, "An improvement of one anonymous identity-based encryption scheme," *International Journal of Electronics and Information Engineering*, vol. 9, no. 1, pp. 11–21, 2018.

[13] Y. Liu, X. T. Liu, C. J. Tang, J. Wang, and L. Zhang, "Unlinkable coin mixing scheme for transaction privacy enhancement of bitcoin," *IEEE Access*, vol. 6, pp. 23261–23270, 2018.

[14] G. Maxwell, "Coinjoin: bitcoin privacy for the real world," in *Post on Bitcoin forum*, 2013.

[15] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: anonymous distributed e-cash from bitcoin," in *2013 IEEE Symposium on Security and Privacy*, pp. 397–411, 2013.

[16] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," *Consulted*, 2008.

[17] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 552–565, 2001.

[18] T. Ruffing, P. Moreno-Sanchez, and A. Kate, "Coinshuffle: practical decentralized coin mixing for bitcoin," in *European Symposium on Research in Computer Security*, pp. 345–364, 2014.

[19] N. V. Saberhagen. "Cryptonote v 2.0,", 2013.

[20] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: decentralized anonymous payments from bitcoin," in *2014 IEEE Symposium on Security and Privacy*, pp. 459–474, 2014.

[21] J. H. Seo, T. Kobayashi, M. Ohkubo, and K. Suzuki, "Anonymous hierarchical identity-based encryption with constant size ciphertexts," in *Proceedings of public key cryptography (PKC' 09)*, pp. 215–234, Irvine, CA, USA, March 2009.

[22] Q. C. ShenTu and J. P. Yu, "A blind-mixing scheme for bitcoin based on an elliptic curve cryptography blind digital signature algorithm," *Computer Science*, 2015.

[23] S. F. Tzeng, M. S. Hwang, "Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem", *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 61–71, Mar. 2004.

[24] L. Valenta and B. Rowan, "Blindcoin: blinded, accountable mixes for bitcoin," in *International Conference on Financial Cryptography and Data Security*, pp. 112–126, 2015.

[25] C. C. Yang, T. Y. Chang, and M. S. Hwang, "A new anonymous conference key distribution system based on the elliptic curve discrete logarithm problem," *Computer Standards and Interfaces*, vol. 25, no. 2, pp. 141–145, 2003.

[26] C. Yuan, M. X. Xu, and X. M. Si, "Research on a new signature scheme on blockchain," *Security and Communication Networks*, vol. 2017, no. 2, pp. 1–10, 2017.

[27] J. H. Ziegeldorf, R. Matzutt, M. Henze, F. Grossmann, and K Wehrle, "Secure and anonymous decentralized bitcoin mixing," *Future Generation Computer Systems*, vol. 80, pp. 448–466, 2018.

Biography

Yang Liu is a Master Candidate at the School of Computer and Software Engineering, Xihua University. Her research interests include Cryptography and blockchain technology.

Mingxing He is a Professor at the School of Computer and Software Engineering, Xihua University. He is the member of the International Association for Cryptologic Research, and is also the member of the CCF and ACM. His research interests include Cryptography and Network Security.

Fangyuan Pu is a Master Candidate at the School of Computer and Software Engineering, Xihua University. Her research interests include Network Security and Security Multi-Party Computation.