Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 7125472, 13 pages
https://doi.org/10.1155/2022/7125472

Research Article

RBSmix: A Regulatable Privacy-Preserving Method for Cryptocurrency

Rongyu Xiao,[1] **Guozi Sun**,[1,2] **Jiale Yang**,[1] **Yao Wang**,[1] **and Puhe Hao**[1]

[1] *School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China*
[2] *Key Laboratory of Urban Land Resources Monitoring and Simulation, MNR, Shenzhen 518000, China*

Correspondence should be addressed to Guozi Sun; sun@njupt.edu.cn

Received 14 January 2022; Accepted 3 May 2022; Published 8 June 2022

Academic Editor: Jinguang Han

Public chains represented by Bitcoin and Ethereum do not require users to use their real names, and transaction data are open to the whole network. Analysed based on this, researchers have achieved the deanonymization of blockchain transactions to a certain extent. Based on the existing blockchain transaction privacy protection scheme, the true link relationship between the transaction sender and receiver is hidden, which brings difficulties to regulation. In this paper, we propose a cryptocurrency mixing service RBSmix, which allows users to reestablish their financial privacy in Bitcoin and related cryptocurrencies. RBSmix, through blind signature to prevent attackers from linking input and output addresses, by the threshold secret sharing algorithm, encryption technology, and a regulation team, combined with the idea of voting, tracks the source of funds for illegal addresses. Experiments show that the scheme scales to large numbers of users and can provide users with better privacy protection.

1. Introduction

Satoshi Nakamoto published the Bitcoin white paper in 2008 [1] and launched the operation of the Bitcoin mainnet in 2009, ushering in a new era of cryptocurrency. Since then, more cryptocurrencies have appeared. The use of Bitcoin does not require personal information, and its anonymity is favoured by more and more people.

However, Bitcoin is not a completely anonymous system. Conti et al. [2] conducted a systematic survey covering Bitcoin's security and privacy and pointed out that the distributed nature of Bitcoin has problems with users' privacy and anonymity requirements. Attackers can obtain some valuable information by analysing transaction records. Reid and Harrigan [3] proposed the concepts of transaction graph and user graph by analysing the transaction characteristics of Bitcoin. Based on their work, researchers proposed some heuristic cluster analysis methods [4–6] to find different accounts of a user. Once a transaction is real named, the user identity information in the relevant transaction will face the risk of disclosure. The research work [7] analysed the possible risks of directly mapping Bitcoin addresses to IP addresses.

Therefore, there is an urgent need to provide users with better anonymous services. Mixing service creates a random mapping between input and output addresses by mixing funds of different users, thereby achieving complete anonymity and enhancing privacy. Bonneau et al. [8] proposed Mixcoin, a scheme based on confused nodes. Mixcoin used multiple nodes to provide mixing services, but if a node divulges privacy, the privacy of the whole protocol will also be destroyed. Liu et al. [9] proposed a scheme based on ring signature, which puts multiple users in the same transaction, and each output address corresponds to the same amount of currency, so that each user is in an anonymous set of fixed size to protect the privacy of user transaction data. However, the size of anonymous collection is limited, and the degree of anonymous protection obtained by users is not high. Ziegeldorf et al. [10] proposed Coinparty, which is based on decryption hybrid network and threshold signature scheme.

It simulates a trusted third party through secure multiparty computing [11] to realize secure and anonymous Bitcoin mixing. Combined the advantages of centralized and decentralized hybrid services in a single system, compared with the previous work, the anonymity has been greatly improved. However, these mixing services only design anonymous protection mechanism and no regulation mechanism, so that mixing services are often used for illegal activities, such as black-market trading and money laundering. On September 26, 2020, KuCoin issued an official announcement [12] that the platform was attacked by hackers. Information from the blockchain analysis company Elliptic showed that the hackers who stole from KuCoin used different mixing services to launder money. Unregulated mix technologies may cause harm to the society, and it is difficult for law enforcement agencies to trace down and punish it, so that many countries in the world are cautious about cryptocurrencies. In 2018, the U.S. Securities and Exchange Commission (SEC) issued the "Statement on Digital Asset Securities Issuance and Trading" [13], confirming that digital assets belong to the category of securities and must be included in the national regulatory system. Russia, Vietnam, etc. strictly restrict the circulation of cryptocurrencies. Therefore, it is of great significance to design a mixing scheme with both privacy protection and regulation functions.

Aiming at the problems existing in the existing schemes, this paper focuses on solving the problem of unregulated mixing server. This paper proposes a new protocol RBSmix (Regulatory, Blind, Shamir) with both privacy protection and regulation functions. Our contributions are summarized as follows:

(1) RBSmix designed a regulation team to solve the problem of unregulated mixing services. If more than half of the regulation members think it is illegal, they can link the address to its input address through calculation to trace the source of funds at the address

(2) RBSmix will encrypt and divide the transaction data and submit it to multiple institutions for storage. The data leakage of a few institutions will not lead to the destruction of users' transaction privacy and reduce the risk of data leakage

(3) RBSmix divides the user's request for mixing service into sending currency and withdrawing currency, and the two transactions of different users are interspersed. With the increase of the number of users requesting services, the anonymous set size of each user will also increase, realizing better anonymous protection services

The rest of this paper is organized as follows. We introduce some research work on protecting the privacy of blockchain transactions in Section 2. The technology related to this paper are presented in Section 3. The protocol and system design of RBSmix is laid out in Section 4. We provide a comprehensive analysis, evaluation, and discussion of correctness, performance, and security in Section 5. Section 6 concludes this paper.

2. Related Work

To protect the privacy of blockchain transactions and hide both parties and transaction amount, researchers have proposed many schemes.

Valenta and Rowan [14] improved the Mixcoin and proposed the Blindcoin, which protects users' privacy through a blind signature algorithm and a public log. Mix servers cannot obtain the real link relationship between the input and output addresses. However, due to the lack of regulatory mechanism, there is a risk of capital theft in both schemes. Bao et al. [15] proposed Lockmix based on Mixcoin and Blindcoin. The original scheme is further optimized through blind signature and multisignature, which can not only prevent the mix server from obtaining the real link relationship between the input and output addresses but also prevent the mix server from illegally stealing user funds.

Zerocoin [16] is a new type of side chain, which is an encrypted extension of Bitcoin. It uses zero-knowledge proof technology to convert users' Bitcoins into zero coins on the Bitcoin side chain to achieve stronger anonymity. Zerocoin once proposed a soft fork, but it was rejected by Bitcoin developers. Later, Sasson et al. [17] improved Zerocoin and proposed the Zerocash scheme; noninteractive zero-knowledge proofs are used to achieve stronger anonymity.

Coinjoin proposed by Maxwell [18] allows mixing service transactions without the intervention of a third party. In the Coinjoin transaction, multiple users take the same amount of Bitcoin as input to construct the transaction and check whether their address is written into the transaction. Only after obtaining the signatures of all users and merging, the transaction is considered legal and received by the network. However, Coinjoin also has some defects, such as being unable to resist DoS attacks, and users cannot deny that they have participated in mixing service. Aiming at the defects of Coinjoin mechanism, Ruffing et al. [19] proposed Coinshuffle, added the mechanism of shuffling the output addresses on the basis of Coinjoin, and realized the internal unlinkability, but it was vulnerable to DoS attack and cross attack [20]. Barber et al. [21] proposed fair exchange protocol, a bilateral Bitcoin exchange protocol, both parties use Bitcoin scripts, and three types of Bitcoin transactions (guarantee transaction, refund transaction, and claim transaction) realize Bitcoin exchange without mutual trust. Bissias et al. [22] proposed a method of anonymously finding hybrid nodes based on blockchain advertising. With the increase of the number of users, the cost of attack will increase, which can effectively avoid denial of service attack.

Sun et al. [23] proposed an MBDC model suitable for the central bank to regulate digital currency. The central bank can avoid the double flower problem and protect users' privacy by separating users' identity and transaction information. The establishment of DC (data center) and layers of supervision realized strong regulation on the model. Xue et al. [24] proposed a blockchain transaction model with both privacy and regulation functions. Probabilistic encryption is used to hide the true identity of blockchain transactions; commitment scheme and zero-knowledge proof technology are used to protect privacy. Through encryption technology, regulators can store user information without storage regulating blockchain transactions without interest. Tu and Meredith [25] have studied the regulation of virtual currency and proposed to develop a comprehensive, cohesive, and appropriate scale virtual currency regulation model in combination with existing laws.

3. Preliminaries

This section will introduce blockchain transaction, blind signature, threshold secret sharing, Tor, etc., because they are related to the scheme in this paper.

3.1. Blockchain Transactions. Blockchain is a decentralized distributed ledger that records all transaction data, including transaction hash value, time, input and output address, and amount. The input address of each transaction is the output address of the previous transaction, and all funds can be traced back to the source. All transaction data in the blockchain are open to the whole network, and anyone can obtain complete transaction records. Through analysis, attackers may associate an anonymous address with a specific user, destroying user privacy. This is also the problem to be solved in this paper.

3.2. Blind Signature. Blind signature [26] is a special digital signature, which is a bilateral agreement. In blind signature, the signer does not know the specific content of the signed message, and the message owner can get the signer's digital signature of the original message. When the signature is made public, the signer cannot know when it was signed. An ideal blind signature protocol has the characteristics of unforgeability, nonrepudiation, unknown, and untraceable. Blind signature can achieve the purpose of protecting data privacy.

3.3. Threshold Secret Sharing. The concept of secret sharing was first independently proposed by famous cryptologists Shamir [27] and Blakley [28] in 1979. (k, n) threshold secret sharing means that the secret s is decomposed into n subkeys and distributed to n holders, in which no less than k secrets can recover the ciphertext, and no information of the ciphertext can be obtained if less than k secrets. Threshold secret sharing can distribute power to multiple independent users without relying on single point of management.

3.4. Tor Network. Tor [29, 30], known as onion routing anonymous proxy network, is a typical anonymous communication system. It is mainly used for privacy protection in IP layer to prevent attackers from attacking users' traffic and ensure online anonymity of users. Rerouting mechanism plays the role of confusing the actors of network behaviour, making it possible for all nodes in Tor network to participate in network behaviour. Hierarchical encryption erases the relationship between messages received and sent by nodes, that is, all nodes seem to be doing the same network behaviour. The combination of the two realizes the anonymity of network behaviour.

4. RBSmix Protocol

Based on blind signature algorithm, threshold secret sharing algorithm, and encryption technology, we propose a regulatable mixing service protocol RBSmix, which not only provides users with transaction privacy protection services but also realizes the regulation of illegal transactions. Next, we will introduce in detail.

4.1. System Model. The RBSmix model is shown in Figure 1, which mainly includes a central agency, a regulation team, mix servers, and users.

4.1.1. Central Agency. With certification and regulation functions, mix servers or users need to register with the central agency and take the lead in completing regulatory tasks when necessary.

4.1.2. Regulation Team. Assist the central agency to complete the regulation function, and prevent the central agency and mix servers from negotiating privately and undermining user privacy. Regulation members can also be used as ordinary mix server to provide users with mixing services. Team members are selected based on indicators such as the number of users of the mix server service and the amount of funds. If the number of members is too small, the degree of authority will be lower. Too many, it is difficult to guarantee the quality of members. It needs to be set according to the actual situation. This paper is for experimental testing only, and six members are tentatively scheduled.

4.1.3. Mix Servers. The number is variable, providing users with mixing services. It is required to register with the central agency and pay a certain deposit to ensure that it will not illegally violate the provisions of the protocol.

4.1.4. Users. Mainly divided into two categories: the first category is to use fiat currency to purchase cryptocurrency [31], and hope that anyone, including mix servers, cannot associate the receiving address with their own identity. The second category is to transfer cryptocurrency from an address (which may have a certain connection with his identity) to a new address with better anonymity.

As shown in Figure 2, usually, the mix server receives the user's funds, mixes them, and then, sends the funds to the address specified by the user. In the early days, the centralized mix server could know the correspondence between the input and output address. Users cannot judge whether the server will leak or sell their private information. To solve this problem, researchers later proposed some solutions based on blind signatures and ring signatures. Users have got better privacy protection, but they also bring difficulties to regulation.

RBSmix is based on a centralized server that uses a blind signature algorithm to cut the link between the input and output addresses. Adopt threshold secret sharing algorithm and encryption technology to realize the regulation of transactions. Tor protects user privacy at the IP layer.

The protocol is mainly divided into the following steps:

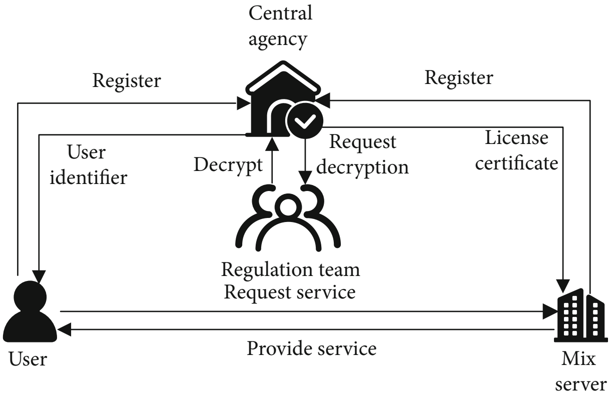

Figure 1: System model.

(1) User requests the central agency to sign his identity information

(2) User requests the mix server to sign the address and identification information through the signature of the central agency

(3) User relies on the signature of the mix server to request the withdrawal service from the mix server through the Tor anonymous network

(4) When necessary, the central agency requests transaction information from the mix server and submits it to the regulation team for voting to realize the regulation function

4.2. Protocol Goals. As a mixing service, we propose the following goals for RBSmix:

(1) *Anonymity Protection Service*. Users can transfer funds to addresses with better privacy in an unlinkable way through RBSmix

(2) *Better Anonymity*. The size of the anonymity set implemented by most of the current mixing services is limited. We hope to provide users with better privacy protection, so it is required that the anonymity set provided by RBSmix for users can become larger as the number of users increases

(3) *Antitheft*. RBSmix is implemented based on a centralized mix server, and we need to avoid mix server from stealing user funds

(4) *Defend against Malicious User Attacks*. If a malicious user attacks RBSmix, will he affect other users requesting the service, and whether the attacker can carry out a DDoS attack. This is the problem we need to solve

(5) *Deniability*. It is required that no one except the mix server can judge which transactions are mixed transactions from the transaction form. Because if the transaction form of the mixed transaction is significantly different from the normal transaction, even if the specific address correspondence is not known, the scope of the user anonymity set can be narrowed, and the risk of user privacy leakage can be increased

(6) *Monitorability*. Design a regulatory mechanism to avoid being used by illegal elements for illegal activities such as money laundering

The scheme in this paper is based on elliptic curve encryption algorithm, a blind signature algorithm based on elliptic curve [32] and Shamir secret sharing algorithm [27]. Therefore, the security of RBSmix is based on the security of these three algorithms. However, the RBSmix model may still face some other security threats. For this, we propose the following security goals:

(1) In RBSmix, the regulation function is realized through the signature information of the user identifier. We need to ensure that even if the attacker steals the signature information of the legitimate user, he cannot use the information to request the mixing service to evade regulation

(2) In RBSmix, the user needs to transfer money to the address specified by the mix service. We need to ensure that the attacker cannot tamper with the address to his own address during the communication process to deceive the user; the mix service also cannot deny that the address is its own after receiving the user's transfer

(3) In RBSmix, users need to use their own identifier-related information to request mixing service. We need to ensure that attackers cannot use this information for cluster analysis to destroy user privacy

4.3. Protocol Process. The specific process of the RBSmix protocol is shown in Figure 3. The parameter table is shown in Table 1. Next, each step will be described in detail.

(1) User **A** wants to request mixing service. First, find the cryptocurrency that meets his requirements and the mix server **M** that provides the service from the public data provided by the central agency. Then, **A** and **M** negotiate the amount v and service fee vp and confirm the number of blocks required for the transaction ω

(2) After the negotiation is completed, **M** sends a consent reply to **A**

(3) **A** receives the message from **M** and performs the following operations:

(i) **A** uses a blind signature algorithm [32] based on elliptic curve to generate a blind factor r_1, which is used to blind the information later

(ii) **A** chooses 5 of the 6 regulation team members as the regulation team members for this service. If the mix server of **A** requesting service is one of the 6 team members, he can only choose the remaining 5 as members of this

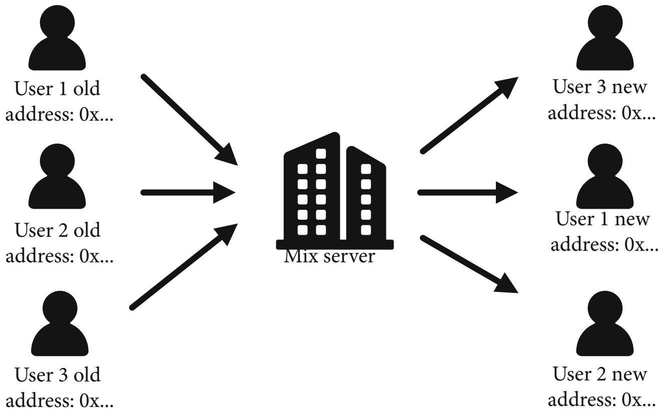
User 1 old address: 0x...
User 2 old address: 0x...
User 3 old address: 0x...
Mix server
User 3 new address: 0x...
User 1 new address: 0x...
User 2 new address: 0x...

Figure 2: Centralized mix server model.

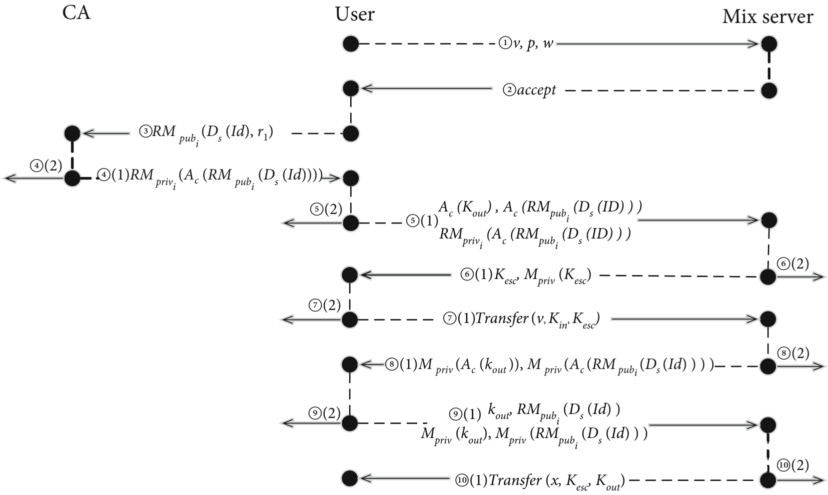
CA
User
Mix server
①v, p, w
②$accept$
③$RM_{pub_i}(D_s(Id), r_1)$
④(2)
④(1)$RM_{priv_i}(A_c(RM_{pub_i}(D_s(Id))))$
⑤(2)
⑤(1) $A_c(K_{out})$, $A_c(RM_{pub_i}(D_s(ID)))$ $RM_{priv_i}(A_c(RM_{pub_i}(D_s(ID))))$
⑥(1)K_{esc}, $M_{priv}(K_{esc})$
⑥(2)
⑦(2)
⑦(1)$Transfer(v, K_{in}, K_{esc})$
⑧(1)$M_{priv}(A_c(k_{out}))$, $M_{priv}(A_c(RM_{pub_i}(D_s(Id))))$
⑧(2)
⑨(2)
⑨(1) k_{out}, $RM_{pub_i}(D_s(Id))$ $M_{priv}(k_{out})$, $M_{priv}(RM_{pub_i}(D_s(Id)))$
⑩(1)$Transfer(x, K_{esc}, K_{out})$
⑩(2)

Figure 3: Protocol diagram.

service. The reasons will be explained in Section 4.3

(iii) **A** uses a threshold secret sharing algorithm to divide its identifier into 5 parts. Add KG_M, t_1 , t_2 after each part, then the information is encrypted with the public keys of 5 team members and send them to the central agency

(4) The central agency receives the message from **A**, decrypts it, and then, sends the corresponding fragment information to the corresponding regulation member. The regulation member receives the message, decrypts it, and sends the obtained identifier information to the central agency. The central agency chooses 3 of the 5 fragments to verify whether the identifier is legal. All combinations need to be verified for a total of 10 rounds

(i) If all are successful, inform 5 regulation members that the verification is successful. After receiving the successful message, regulation members encrypt the identifier fragment with their own public keys and then blind the message with r_1. Then, sign the information with his own private key and send it to the central agency. After receiving it, the central agency will uniformly send it to user **A**

(ii) If there is a failure, inform the regulation member that there is an error and the protocol stops. Then, send a verification failure reply to **A**

(5) User **A** receives the message and verifies the signature. For the five parts of the identifier division in step 3 of process 3, the corresponding regulation member public key is used for encryption, and then, the same blind factor r_1 is used to blind the message. Five signatures are verified by using the public keys of five regulation members

(i) After verification, **A** sends a mixing service request to the mix server. First, generate the address k_{out} which **A** wants to receive cryptocurrency, and generate a new blind factor r_2 to blind the address. Finally, send the blinded address, blinded information containing the identifier generated in step 3 of process 3, the

Table 1: Parameter table.

Parameters	Description
$\boldsymbol{p}$	The mixing fee rate that **A** will pay
$\boldsymbol{v}$	Amount of **A** need to be mixed
$\boldsymbol{x}$	Coin value withdrawal allowed by **M**
$\boldsymbol{\omega}$	The number of blocks which is required to confirm payment
$\boldsymbol{Id}$	Identifier of **A**
$\boldsymbol{r_i}$	Blinding factor (the general name of the factors used in blind processing)
$\boldsymbol{k}_{\text{in}}$	The input address of **A**
$\boldsymbol{k}_{\text{out}}$	The output address of **A**
$\boldsymbol{k}_{\textbf{esc}}$	The escrow address of **M**
$\boldsymbol{k}'_{\textbf{esc}}$	Another escrow address of **M**
$\boldsymbol{CA}_{\textbf{pub}}$	The public key of CA
$\boldsymbol{CA}_{\textbf{priv}}$	The private key of CA
$\boldsymbol{RM}_{\textbf{pub}_i}$	The public key of RM_i
$\boldsymbol{RM}_{\textbf{priv}_i}$	The private key of RM_i
$\boldsymbol{M}_{\textbf{pub}}$	The public key of **M**
$\boldsymbol{M}_{\textbf{priv}}$	The private key of **M**
$\boldsymbol{A_c}$	Blinding function
$\boldsymbol{A'_c}$	The inverse of A_c
$\boldsymbol{D_s}$	Secret distribution
$\boldsymbol{M_s}$	Secret reconstruction

signature information of the five regulation members received from the central agency, and which five members are chosen to the mix server

(ii) Verification failed: check whether there are any errors in your operation and restart process 3

(6) The mix server receives the request sent by **A** and verifies the signature. Get the blinded information containing the identifier and the signature information containing the identifier, and verify the signature by using the public key of five regulation members

(i) If the verification is successful, send the address k_{esc} that is going to receive **A**'s cryptocurrency and the signature $RM_{\text{priv}_i}(k_{\text{esc}})$ of the address to **A**

(ii) Failed to verify, reply to user **A** failed

(7) **A** receives the message from the mix server

(i) If successful, **A** needs to transfer the cryptocurrency amount v negotiated in the process 1 to the address k_{esc} designated by **M**. And send the transaction information to **M**

(ii) If it fails, **A** checks whether there is an error in his previous operation and reexecutes process 3 or process 5

(8) After receiving the reply from **A**, **M** checks whether it has received the negotiated amount of encrypted currency at the address specified by itself (for the second type of users, the mix server also needs to determine whether the received signature about the address is the signature of the central agency on the address sent by the user this time)

(i) Confirm receipt, wait for ω block confirmation, and sign the received blind address $A_c(k_{\text{out}})$ and $A_c(RM_{\text{pub}_i}(D_s(Id)))$ containing identifier. Send them to **A**

(ii) If it is not received or the amount is incorrect, reply with an error message

(9) **A** receives the information replied by **M**, verifies the signature, and withdraws the coin

(i) Reply as a signed message, and the signature is valid. Save the signature. **A** can anonymously send the original address k_{out}, $D_s(Id)$ containing the identifier generated in step 3 of process 3, and the received signature of the mix server to **M** through the Tor network at any time to initiate a withdrawal request

(ii) If the signature verification fails or an error message reply is received, check the reason. If it is **M**'s problem, you can appeal to the central agency by virtue of k_{esc} and $M_{\text{priv}}(k_{\text{esc}})$ received in process 6 and the transfer record to the address

(a) The central agency receives the appeal information and checks the correctness of the information

(b) If the information is correct, draw the transaction amount from the deposit paid by the mix server and transfer it to user **A**. At the same time, a part is taken as the punishment for the mix server's violation of the agreement

(c) If there is an error in the information, inform **A** that there is a problem with the appeal, and recheck the information

(10) The mix server receives an anonymous withdrawal request and verifies the validity of the signature

(i) Valid, agree to the request, and transfer coins to this address. At the same time, the request information $k_{\text{out}}, RM_{\text{pub}_i}(D_s(Id))$ is stored locally

(ii) Invalid, discard the request

(11) After a while, **A** checks whether the specified receiving addresses receives the specified number of currencies

  (i) If a specified amount of currency is received, the entire mixing service is completed

  (ii) Otherwise, **A** reinitiates the withdrawal request. If **A** still cannot receive the currency after multiple requests, he can appeal to the central agency with the signature information received in process 9. Same as step 2 of process 9

4.4. Regulation Process. In the future, if someone proposes that an address served by the mix server is involved in illegal and criminal activities, the central agency needs to organize regulation team to vote to decide whether to undermine the privacy of the address and trace the address of the source of funds. The regulation model of RBSmix is shown in Figure 4; the specific process is as follows:

(1) User **B** believes that an address K_{out} is involved in illegal activities and puts forward his views to the central agency

(2) The central agency accepts the request and requests the secret information containing the identifier corresponding to the address from the mix server who has served the address

(3) The mix server finds the corresponding information $k_{\text{out}}, RM_{\text{pub}_i}(D_s(Id))$ and sends it to the central agency

(4) The central agency distributes the relevant secret fragment information to the corresponding regulation members and organizes the regulation team to discuss whether the address behaviour is indeed illegal

(5) After receiving the information, the regulation members first judge whether the address is indeed involved in illegal and criminal activities, and if so, decrypt it to obtain $D_s(Id)$. The message is then sent to the central agency

If **A** chooses one of the six regulation members as the mix server and also chooses it as the regulation member to save one of the five subkeys that can decrypt the identifier information, the regulation member finds that one of the five signatures is his signature when serving the user and verifying the five signatures, and can directly pair and store the fragment information with the user locally. Then, the mix server can find the input-output link relationship of the service address alone. Therefore, in step 3 of process 3, users must choose mix servers and regulation members according to regulations.

(6) The central agency receives the reply from the regulation member

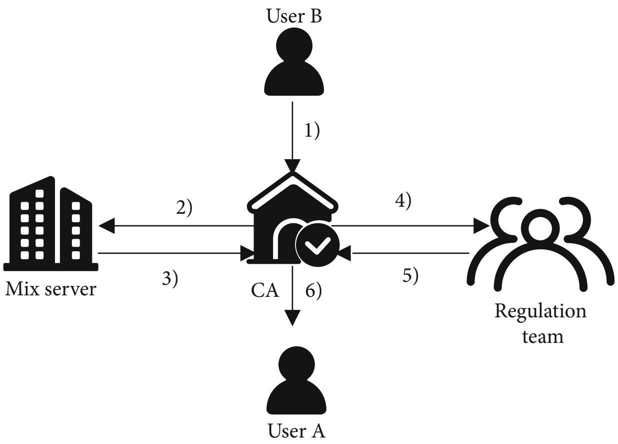

Figure 4: Regulation model.

  (i) If three or more regulation members believe that the address is indeed illegal and agree to decrypt it, the central agency can use the information to calculate user identifier and find the source address of the address funds

  (ii) If less than 3 regulation members believe that the address is illegal and do not agree to the decryption, the central agency will not be able to decrypt the user identifier information

5. Experiment and Analysis

In this section, the effectiveness of the scheme will be verified through experiments, and then, the various attributes of RBSmix will be discussed through comparison with other schemes. Finally, the scheme will be analyzed and the possible security threats will be discussed.

5.1. Experiment. The main purpose of our experiment was to measure the efficacy of RBSmix. The experimental environment is a virtual machine with 4-core 4G and running 64-bit Ubuntu 18 (the physical machine with an Intel Core i7-8750H CPU at 2.20 GHz 2021 GHz with 16 G of RAM, and running 64-bit Windows 10). The method proposed in this paper adopts Python 3 7.6 language design and implementation: the program designs a central agency and six mix servers. The mix servers act as members of the regulation team at the same time, and different institutions use different ports of the virtual machine for simulation implementation. Experiments were conducted on the Ethereum test chain Ropsten and the local Bitcoin test chain built using the open-source project bitcoin-testnet-box [33].

We have conducted many experiments. To make the experimental results easier to observe, we show from the perspective of a mix server the situation of mixing services for 6 users on the Bitcoin test chain built locally, involving a total of 13 transactions, as shown in Table 2.

People other than users and mix server cannot know who sent each transaction, let alone determine the relationship between the user's input addresses and the receiving

Table 2: Transaction records.

Transaction	Inputs	Outputs	Value [BTC]
Transaction 1	User 1	bcrt1qcmsjawreuk80as8g2fl7yaqs7kfrpm3dqyf8tf	1
Transaction 2	User 2	bcrt1qurndyuql97thg0ycfz8g9ecy29htktg2upzh7r	1
Transaction 3	Mix server	bcrt1q4yypg9amgzd2uzrr055em5frhwwj9j3pceyd7t	1
Transaction 4	Mix server	bcrt1q9jw04nx7gryrjhyud693zkkygyzp2t4ysv2chl	1
Transaction 5	User 3	bcrt1qpamtz0kpcdyza40pufjrkl0u2dn8dx45qv7w9p	1
Transaction 6	Mix server	bcrt1q7rls7z6kx5x98j2s0hjjk0j6r2skwpy64myxtm	1
Transaction 7	User 4	bcrt1qurndyuql97thg0ycfz8g9ecy29htktg2upzh7r	1
Transaction 8	User 5	bcrt1qpamtz0kpcdyza40pufjrkl0u2dn8dx45qv7w9p	2
Transaction 9	User 6	bcrt1qcmsjawreuk80as8g2fl7yaqs7kfrpm3dqyf8tf	1
Transaction10	Mix server	bcrt1qgam5smv0k2750mczczx4hhhjs0j23rpvrmj4hw	1
Transaction 11	Mix server	bcrt1qy2jdydcx565aekrd7n3m79fzpvw3zd7yrgwdc6	1
Transaction 12	Mix server	bcrt1q8weae9fsvsgepgaaakqcrtrt9qgexulu4x9std	1
Transaction 13	Mix server	bcrt1qv4gzdx25crdwerztqyjussjh608z2yusdtzmh4	1

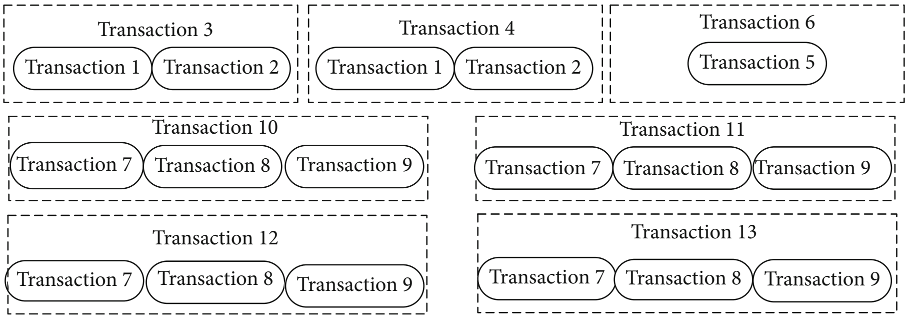

Figure 5: Anonymous set corresponding to each withdrawal transaction.

addresses, or even whether these transactions are mixed transactions. In this case, users can even deny that they have participated in a mixed transaction.

The mix server knows which are the addresses in its address pool and which are user's addresses, but cannot associate user's receiving addresses with the input addresses. As shown in the third transaction in Table 2, the mix server can determine that the address bcrt1q4yypg9amgzd2uzrr055em5frhwwj9j3pceyd7t is the receiving address of one of user 1 and user 2, but cannot determine which one it is. Because in its view, all withdrawal transactions are the same.

The size of the anonymity set of each withdrawal exchange in Table 2 is shown in Figure 5. It can be seen that the size of the anonymous set of the sixth transaction (belonging to the withdrawal transaction) is one. This is because the user who initiated the mixing service request has already withdrawn the coin. For the address bcrt1q7rls7z6kx5x98j2s0hjjk0j6r2skwpy64myxtm, the coin only may come from user 3. In this case, the user did not obtain the expected anonymity. But for other transactions, the anonymity set is greater than 1, for example, the 10th transaction, the coin of the address bcrt1qgam5smv0k2750mczczx4hhhjs0j23rpvrmj4hw may come from 3 addresses, and the anonymity set size is 3, achieving the purpose of mixing service.

The size of the anonymity set at the withdrawal exchange is the number of users who have not requested the withdrawal service before the withdrawal request is initiated. In the operation of the protocol, as the number of users requesting services gradually increases, the number of users that may correspond to each withdrawal exchange also increases, and the better the anonymity obtained. Therefore, when a user initiates a withdrawal request, he can pay attention to the number of users requesting mixing service, so as to put himself in a larger anonymous concentration and obtain better privacy protection.

Then, we used a parallel strategy to simulate multiple users' requests for mixing services to verify the effectiveness of the scheme. Test the time required for RBSmix to serve different numbers of users without considering transaction confirmation. Firstly, the time required for different number of mix servers to serve a large number of users is tested. As shown in Figure 6, it can be seen that it takes about 14 s for a mix server to serve 10 users, 144 s for 100 users, and 1470 s for 1000 users. There is a linear relationship between the number of users and the running time as a whole. When the number of mix servers increases, the service time decreases. The time required for two mix servers to serve users is about half that of one mix server, but when the number of mix servers becomes three, the time reduction is not obvious, because the service performance of the central agency has not been improved accordingly. Then, the program of the central agency is changed to dual-thread parallel processing, the number of mix servers is set to 4, and the experiment is carried out again. The experimental results

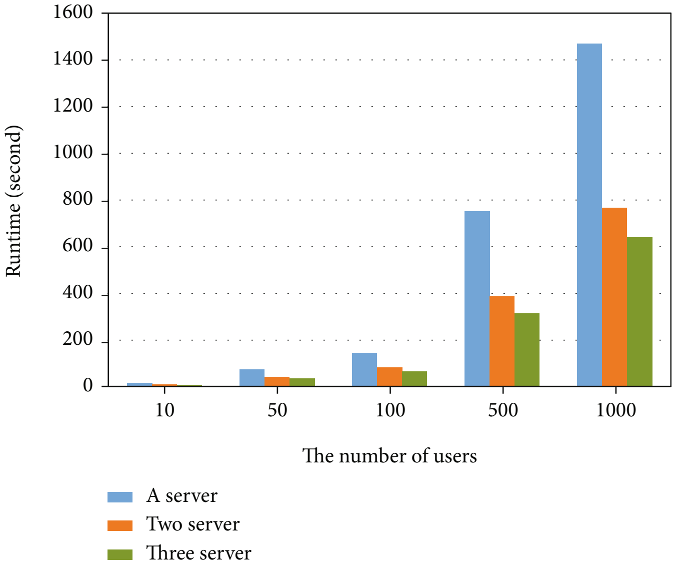

Figure 6: Running time in different numbers of users.

are shown in Figure 7. For the same number of users, compared with single thread processing, the performance of the central agency with dual thread parallel processing has been greatly improved.

Generally speaking, the running time of RBSmix increases with the increase of the number of users and decreases with the improvement of the number of mix servers and the service capacity of the central agency. Compared with the transaction confirmation time in the running process, the protocol process takes up very little time.

Then, we verified the regulation function. To realize the regulatory function in the protocol, the members of the regulation team need to vote. To verify the effectiveness of the regulatory function in the experiment, we assume that each time the central institution organizes a vote, most members will vote in favour, so that, each time, it can decrypt and complete the tracing of the source addresses of the addresses. Figure 8 shows the time required to complete different times of regulatory experiments. It can be seen that the running time of the program is very short after completing traceability of the source of address funds. In the actual operation of the agreement, most of the time required for regulation is the time when the central agency requests data from the mix server and the time for the members of the regulation team to vote. Code running time is very small.

It can be seen from the experimental results that compared with the transaction confirmation time, the time to complete encryption, decryption, signature, and verification is very short. In addition, multiple mix servers can serve a large number of users at the same time, and the scalability of the scheme is also relatively good.

5.2. Protocol Analysis. This section analyses the properties of the RBSmix protocol. The specific analysis is as follows:

5.2.1. Anonymity. Using the blind signature algorithm, the mix server cannot correspond to the user and the user's receiving address, but only knows which addresses it has served. In order to resist the damage to the privacy of transactions caused by the amount-based disambiguation method [34], the withdrawal amount of services provided by the same mix server to users must be the same. As shown in the experiment in Figure 5, each user is mapped to a different number of receiving addresses. Users can control the size of their anonymous set by adjusting the withdrawal time, because users who have requested services from the mix server before the withdrawal request is initiated may initiate the withdrawal request; the anonymous assembly gradually becomes larger with the increase of users. Ideally, the anonymous set can be as large as the total number of users.

5.2.2. Antitheft and Accountability. RBSmix requires mix servers to register with the central agency and pay a certain deposit. If the user requests the withdrawal service, the mix server refuses to transfer money in violation of the protocol and steals the user's funds; user can appeal to the central agency by the transfer records and the mix server's signature on the address; once it is determined that the appeal is successful, the central agency will send part of the mix server's deposit to the user to make up for the loss of the user and draw part as the punishment of the mix server. During the operation of the RBSmix, violations of the protocol may occur at every step. After the negotiation is completed, the service provider may refuse the service, affecting the user's service experience, and the user may refuse to request the service, resulting in the waste of service resources of the mix server. In these cases, they can appeal to the central agency. After the appeal is successful, part of the deposit will be deducted from the mix service's illegal agreement. Users who violate the protocol will not be able to request mixing services for a certain period. The loss of violating the protocol is far greater than the benefits obtained. In theory, neither side will do so.

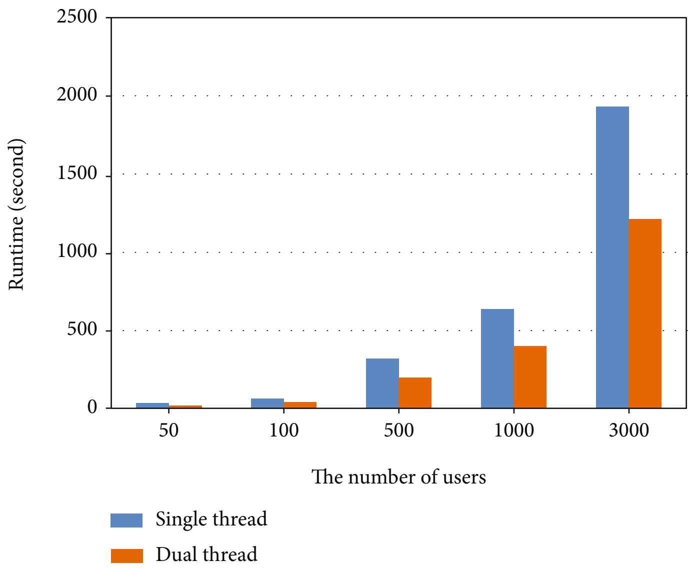

FIGURE 7: Running time in different CA.

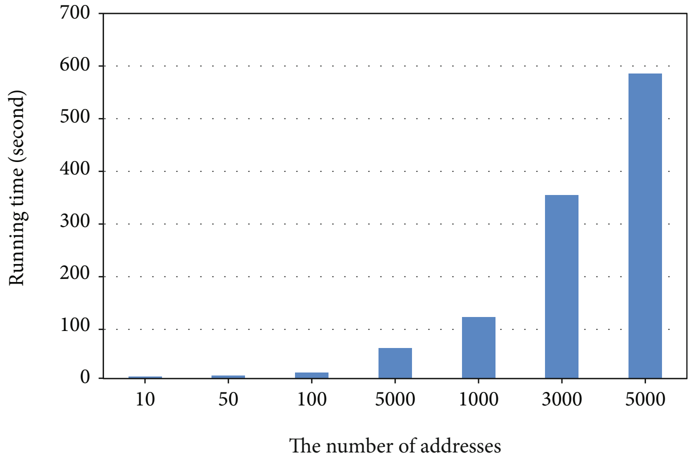

FIGURE 8: Running time of regulation function.

5.2.3. Scalability. According to the experimental results in Section 5.1, RBSmix can serve a large number of users at the same time, and with the increase of the number of users, the anonymity of users is better.

5.2.4. Costs. During the operation of RBSmix, a total of two transactions are required. Therefore, the cost is mixing service fee and the cost of two transactions.

5.2.5. Compatibility. The whole protocol runs independently of the cryptocurrency system and does not need to change the existing system. The transaction part of the scheme can be completed by automatic script or user manually. If an automated script is used, you need to add a call script related to the wallet in the scheme. To test the performance of RBSmix, in the experimental part of the local Bitcoin test chain, all transactions are completed through scripts. In the Ropsten experiment part of Ethereum test chain, users manually confirm the transaction. We recommend manual trading because it is more secure.

5.2.6. Resilience to DoS Attack. Attackers can carry out two kinds of attacks, malicious termination of the protocol or DoS attack. The mix server provides services for each user separately, and users do not affect each other. Even if the attacker maliciously terminates the agreement, it will not have any impact on other users. RBSmix is different from Coinjoin. Users who request mixing services need to pay corresponding service fees. If an attacker implements a DoS attack, it requires a great economic cost. Therefore, rational attackers would not use this attack method.

5.2.7. Deniability. The existing partial coin mixing schemes are to put the input and output addresses of multiple users in the same transaction; to resist the amount-based unmixing method, the output amount will generally be the same. This transaction form can be easily identified as mixed transaction. For example, Meiklejohn and Orlandi proposed an imprecise method [35] to identify Coinjoin [18] transactions, believing that transactions with more than 5 inputs

Table 3: Comparison of the properties with other schemes.

Approach	Accountability	Scalability	Costs	Compatibility	Resistant to DoS attacks	Deniability	Monitorability
RBSmix	√	√	$vp + 2tx$	√	√	√	√
Mixcoin [8]	√	√	$vp + 2tx$	√	√	√	×
Blindcoin [14]	√	√	$vp + 2tx$	√	√	√	×
Coinjoin [18]	×	√	tx	√	×	×	×
Coinswap [36]	×	×	$2tx$	√	√	×	×
Zerocoin [16]	×	√	$2tx$	×	√	√	×
Zerocash [17]	×	√	$2tx$	×	√	√	×

and more than outputs are mixed transactions. In this scheme, withdrawal transactions are transferred from one address (the address of the mix server) to one address (the receiving address specified by the user), which is no different from the normal transaction form. Therefore, it is impossible to judge whether the transaction is a mixed transaction from the transaction form alone.

5.2.8. Monitorability. The threshold secret sharing algorithm and the regulation team are used to regulate the transaction. Once someone proposes that an address is involved in illegal activities, the source of funds of the address can be found through the mix server, the central agency, and most regulation members. A voting idea is adopted here. When there is a problem, only the central agency or mix server cannot complete the regulation function alone. The central agency needs to send the secret fragments related to the address to the corresponding regulation members. The members first make their own judgment on the address and then decide whether to decrypt the information. Only when most regulation members agree to decrypt, the central agency can calculate the original secret information and complete the regulation function. This avoids the malicious destruction of user privacy to a certain extent.

There can be multiple mix servers in RBSmix, which can provide different services to meet users' different needs for cryptocurrency types, amount, etc. Compared with those of other mainstream schemes, this scheme has the basic characteristics of mixing service and realizes the regulation function, as shown in Table 3.

However, compared with the existing schemes, the scheme proposed in this paper has some limitations. The scheme needs an authoritative organization to cooperate with multiple institutions for implementation, so that the implementation cost is higher than the existing schemes (some existing schemes only need one mix server. Some solutions do not even need a mix server, and only need to negotiate between users to achieve the purpose of currency mixing). The premise for a user to reestablish financial privacy is that the user's request for services intersects with that of other users; otherwise, the user cannot reestablish privacy.

Chiu et al. [37] design a scheme that uses smart contract and blockchain to provide a secure data sharing and access environment. Smart contract can better control data, protect user data privacy, better ensure the legal operation of the protocol, and avoid many problems. For example, the user's behavior is controlled through the smart contract, and the request for withdrawal can be initiated only when the user's request intersects with that of other users, which can ensure that users can rebuild their financial privacy through this scheme. In the future, we will try to use smart contract for design and implementation to further improve our scheme.

5.3. Security Analysis. In Section 4.2, we propose the security threats that RBSmix may face, which we will analyse in this section.

Signature theft attack: if the attacker intercepts the signature $RM_{\text{priv}_i}(A_c(RM_{\text{pub}_i}(D_s(Id))))$ sent by mix server **M** to **A**, can the signature be used to request mixing service? First, RBSmix requires the communication process to use the other party's public key for encryption when sending information. When receiving the information, decrypt it with **A**'s private key. As long as **A** ensures the security of his private key, the communication information will not be stolen when the encryption algorithm is secure. If the attacker illegally and successfully obtains the decrypted signature in some way, but because he does not know the blind factor and all identifier fragment information, he cannot successfully construct the blind information $A_c(RM_{\text{pub}_i}(D_s(Id)))$ and still cannot legally initiate the request. If the attacker successfully obtains the signature $RM_{\text{priv}_i}(A_c(RM_{\text{pub}_i}(D_s(Id))))$ and blind information $A_c(RM_{\text{pub}_i}(D_s(Id)))$ after **A** initiates a complete mixing service request, in this case, the attacker can legally initiate the mixing service request and successfully obtain the signature of the mix server. However, because he does not know the blind factor, he cannot unblind the signature and cannot legally initiate the withdrawal request. Still unable to attack successfully. Therefore, as long as user guarantees the security of the private key and blind factor, on the premise of the security of the encryption algorithm, the attacker cannot steal the signature of other users to request mixing service.

Address tampering attack and address denial attack: in protocol process 6, the mix server sends an address k_{esc} to user and asks user to transfer the funds to the address. Consider two attack methods: (1) after intercepting the information, the attacker tampers the address into his address, making user transfer the funds to his own address to realize the attack; (2) after receiving the transfer, the mix server does not recognize that the address is its own address and falsely claims that the address has been tampered with in the process of communication. These two attacks cannot be solved only by using encrypted communication. This scheme requires the mix server to add the mix server's signature $M_{\text{priv}}(k_{\text{esc}})$ to the address when sending this part of the information. After receiving the information and verifying the signature, user transfers the funds to the address. In this way, the mix server cannot deny its signature, and the attacker cannot forge the mix server's signature to ensure the security of user transfers.

User identifier information clustering attack: when users request mixing services from mix servers, they need to segment their personal identifiers to obtain $D_s(Id)$ and then request the signature $A_c(RM_{\text{pub}_i}(D_s(Id)))$ of the regulation member from the central agency. When withdrawing, they need to carry $RM_{\text{pub}_i}(D_s(Id))$. If user requests a signature from the central agency, and then frequently uses the signature to request mixing services, the signature information can be regarded as an account, and all mixed addresses related to the "account" can be found by clustering method. Once one of the addresses is real named, all mixed addresses related to it will face the risk of privacy disclosure. If user uses threshold secret sharing to divide the information and requests a signature from the central agency before requesting mixing service each time, it can ensure that the signature information used each time is different. For mix server, even if a user continuously requests mixing services, the personal information and address information used each time are different. Mix server can only regard them as different users to achieve stronger anonymity protection.

In summary, RBSmix can resist these potential attacks and provide users with safe and reliable mixing service.

6. Conclusion

This paper analyses the privacy issues of cryptocurrency transactions and proposes a regulatable mix server scheme. This scheme has the basic ideal properties of mixing service, realizes the accountability of the agreement when necessary, and provides a new solution to the conflict between the anonymity and regulation of cryptocurrency. In addition, the solution does not depend on a specific consensus mechanism and can be used as an independent module. Finally, experiments verify that multiple mix servers in the protocol can efficiently serve a large number of users at the same time, then several attack methods are proposed, and the security of this scheme is proved, and users can obtain better privacy protection through this scheme.

This paper also discusses some limitations of RBSmix and possible improvements, such as design and implementation through smart contract. In the future, we will continue to try to improve RBSmix to achieve better results.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (no. 61906099), the Open Fund of Key Laboratory of Urban Land Resources Monitoring and Simulation, Ministry of Natural Resources (no. KF-2019-04-065).

References

[1] S. Nakamoto and A. Bitcoin, "A peer-to-peer electronic cash system," 2008, https://bitcoin.org/bitcoin.pdf.

[2] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Communication Surveys and Tutorials*, vol. 20, no. 4, pp. 3416–3452, 2018.

[3] F. Reid and M. Harrigan, "An analysis of anonymity in the bitcoin system," in *Security and Privacy in Social Networks*, pp. 197–223, Springer, New York, NY, 2013.

[4] S. Meiklejohn, M. Pomarole, G. Jordan et al., "A fistful of bitcoins: characterizing payments among men with no names," in *Proceedings of the 2013 conference on Internet measurement conference*, pp. 127–140, Barcelona, Spain, 2013.

[5] K. Liao, Z. Zhao, A. Doupé, and G. J. Ahn, "Behind closed doors: measurement and analysis of CryptoLocker ransoms in Bitcoin," in *2016 APWG symposium on electronic crime research (eCrime)*, pp. 1–13, Toronto, ON, Canada, 2016.

[6] B. Zheng, L. Zhu, M. Shen, X. Du, and M. Guizani, "Identifying the vulnerabilities of bitcoin anonymous mechanism based on address clustering," *Science China Information Sciences*, vol. 63, no. 3, pp. 1–15, 2020.

[7] P. Koshy, D. Koshy, and P. McDaniel, "An analysis of anonymity in bitcoin using p2p network traffic," in *International conference on financial cryptography and data security*, pp. 469–485, Springer, Berlin, Heidelberg, 2014.

[8] 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, Springer, Berlin, Heidelberg, 2014.

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

[10] J. H. Ziegeldorf, F. Grossmann, M. Henze, N. Inden, and K. Wehrle, "Coinparty: secure multi-party mixing of bitcoins," in *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*, pp. 75–86, San Antonio, Texas, USA, 2015.

[11] I. Damgård, M. Geisler, M. Krøigaard, and J. B. Nielsen, "Asynchronous multiparty computation: theory and implementation," in *International Workshop on Public Key Cryptography*, pp. 160–179, Springer, Berlin, Heidelberg, 2009.

[12] "Official announcement," http://Kucoin.comhttps://www.kucoin.com/news/kucoin-security-incident-update.

[13] US Securities And Exchange Commission, "Statement on digital asset securities issuance and trading," https://www.sec.gov/

news/public-statement/digital-asset-securites-issuuance-and-trading.

[14] L. Valenta and B. Rowan, “Blindcoin: blinded, accountable mixes for bitcoin,” in *International Conference on Financial Cryptography and Data Security*, pp. 112–126, Springer, Berlin, Heidelberg, 2015.

[15] Z. Bao, W. Shi, S. Kumari, Z. Y. Kong, and C. M. Chen, “Lockmix: a secure and privacy-preserving mix service for Bitcoin anonymity,” *International Journal of Information Security*, vol. 19, no. 3, pp. 311–321, 2020.

[16] 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, Berkeley, CA, USA, 2013.

[17] E. B. Sasson, A. Chiesa, C. Garman et al., “Zerocash: decentralized anonymous payments from bitcoin,” in *2014 IEEE Symposium on Security and Privacy*, pp. 459–474, Berkeley, CA, USA, 2014.

[18] G. Maxwell, “CoinJoin: bitcoin privacy for the real world,” 2013, https://bitcointalk.org/index.php?topic=279249.0.

[19] 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, Springer, Cham, 2014.

[20] G. Danezis and A. Serjantov, “Statistical disclosure or intersection attacks on anonymity systems,” in *International Workshop on Information Hiding*, pp. 293–308, Springer, Berlin, Heidelberg, 2004.

[21] S. Barber, X. Boyen, E. Shi, and E. Uzun, “Bitter to better—how to make bitcoin a better currency,” in *International Conference on Financial Cryptography and Data Security*, pp. 399–414, Springer, Berlin, Heidelberg, 2012.

[22] G. 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, Scottsdale, Arizona, USA, 2014.

[23] H. Sun, H. Mao, X. Bai, Z. Chen, K. Hu, and W. Yu, “Multi-blockchain model for central bank digital currency,” in *2017 18th International conference on parallel and distributed computing, applications and technologies (PDCAT)*, pp. 360–367, Taipei, Taiwan, 2017.

[24] Z. Xue, M. Wang, Q. Zhang, Y. Zhang, and P. Liu, “A regulatable blockchain transaction model with privacy protection,” *International Journal of Computational Intelligence Systems*, vol. 14, no. 1, p. 1642, 2021.

[25] K. V. Tu and M. W. Meredith, “Rethinking virtual currency regulation in the Bitcoin age,” *Washington Law Review*, vol. 90, pp. 271–347, 2015.

[26] D. Chaum, “Blind signatures for untraceable payments,” in *Advances in Cryptology*, pp. 199–203, Springer, Boston, MA, 1983.

[27] A. Shamir, “How to share a secret,” *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.

[28] G. R. Blakley, “Safeguarding cryptographic keys,” in *1979 International Workshop on Managing Requirements Knowledge (MARK)*, pp. 313–313, New York, NY, USA, 1979.

[29] R. Dingledine, N. Mathewson, and P. Syverson, *Tor: The Second-Generation Onion Router*, Naval Research Lab, Washington DC, 2004.

[30] A. Chaabane, P. Manils, and M. A. Kaafar, “Digging into anonymous traffic: A deep analysis of the tor anonymizing network,” in *2010 fourth international conference on network and system security*, pp. 167–174, Melbourne, VIC, Australia, 2010.

[31] X. Yi and K. Y. Lam, “A new blind ECDSA scheme for bitcoin transaction anonymity,” in *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, pp. 613–620, Auckland, New Zealand, 2019.

[32] F. G. Zhang, C. J. Wang, and Y. M. Wang, “Digital signature and blind signature based on elliptic curve,” *Journal-China Institute of Communications*, vol. 22, no. 8, pp. 22–28, 2001.

[33] Freewill, “bitcoin-testnet-box,” https://github.com/freewil/bitcoin-testnet-box.

[34] Y. Hong, H. Kwon, J. Lee, and J. Hur, “A practical de-mixing algorithm for bitcoin mixing services,” in *Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts - BCC '18*, pp. 15–20, Incheon, Republic of Korea, 2018.

[35] S. Meiklejohn and C. Orlandi, “Privacy-enhancing overlays in bitcoin,” in *International Conference on Financial Cryptography and Data Security*, pp. 127–141, Springer, Berlin, Heidelberg, 2015.

[36] G. Maxwell, “CoinSwap: transaction graph disjoint trustless trading,” 2013, https://bitcointalk.org/index.php?topic=321228.0.

[37] W. Y. Chiu, W. Meng, and C. D. Jensen, “My data, my control: a secure data sharing and access scheme over blockchain,” *Journal of Information Security and Applications*, vol. 63, article 103020, 2021.