International Journal of Computational Intelligence Systems
Vol. **14(1)**, 2021, *pp.* 1642–1652
DOI: https://doi.org/10.2991/ijcis.d.210528.001; ISSN: 1875-6891; eISSN: 1875-6883
https://www.atlantis-press.com/journals/ijcis/

Research Article

A Regulatable Blockchain Transaction Model with Privacy Protection

Zhiyuan Xue[1], Miao Wang[2], Qiuyue Zhang[3], Yunfeng Zhang[2,4], Peide Liu[3,*]

[1]*School of Software, Shandong University, Jinan, 250101, China*
[2]*School of Computer Science and Technology, Shandong University of Finance and Economics, Jinan, 250014, China*
[3]*School of Management Science and Engineering, Shandong University of Finance and Economics, Jinan, 250014, China*
[4]*Shandong Key Laboratory of Blockchain Finance, Shandong University of Finance and Economics, Jinan, 250014, China*

ARTICLE INFO

Article History
Received 04 Mar 2021
Accepted 25 May 2021

Keywords
Blockchain
Privacy protection
Supervision
Encryption

ABSTRACT

Blockchain is a decentralized distributed ledger technology. The public chain represented by Bitcoin and Ethereum only realizes the limited anonymity of user identity, and the transaction amount is open to the whole network, resulting in user privacy leakage. Based on the existing anonymous technology, the concealment of the sender, receiver, amount of the transaction, and does not disclose any information, which makes the supervision difficult. Therefore, the design of blockchain scheme with privacy protection and supervision functions is of great significance. In this paper, a blockchain transaction model with both privacy and supervision function is proposed. It uses probability encryption to realize the hiding of the true identity of the blockchain transaction, and uses the commitment scheme and zero-knowledge proof technology to realize the privacy protection and guarantee legitimacy verification of the transaction. With the use of encryption technology, the regulators can supervise blockchain transactions without storing the users' information, which greatly reduces the pressure on storage, computing and key management. In addition, it does not rely on specific consensus mechanism and can be used as an independent module. The security performance analysis shows that the proposed scheme has great practicability and has potential application in many fields.

1. INTRODUCTION

Blockchain technology first emerged as a tool to manage cryptocurrency in 2008 when Nakamoto introduced "Bitcoin" as first P2P digital cash system using blockchain [1]. It is a new application model for various computer technologies, such as data storage, peer-to-peer transmission, consensus mechanism, encryption algorithm, etc. The blockchain also known as distributed ledger technology, which leads a new round of technological and industrial changes around the world, playing an important role in improving corporate productivity, reducing corporate costs, increasing customer satisfaction and expanding new markets. Some researchers are integrating blockchain technology into some areas of daily life. For example, the application of blockchain has extended from the financial to the physical field, including electronic information storage, copyright management and trading, product traceability, digital asset trading, Internet of Things, intelligent manufacturing, supply chain management and other fields [2]. All these applications show that blockchain will take over some major areas of daily life in the future. Moreover, the blockchain can bring people into a fair, safe and transparent environment. Obviously, as a trust system construction technology, blockchain has great potential and is expected to become the cornerstone of the new era of digital economy. Now, blockchain has begun to be used in various industries such as energy, finance, e-commerce, e-government and medical care. Especially in the field of privacy protection, a large number of experts and scholars have been attracted to achieve better results. With the further development and wide application of blockchain, it also faces more and more technical challenges, especially in privacy protection and supervision.

Blockchain works in the use of shared distributed ledger distribution system, which is basically a data structure that contains transaction lists in an orderly form. However, these decentralized transactions have produced certain privacy risks and attacks in daily life, which need to be solved before blockchain integration [3]. First of all, Conti *et al.* [4] gave one of the groundbreaking research articles on bitcoin security and privacy, which highlighted all the basic technologies of bitcoin and its feasibility and robustness analysis. Up to now, some research has been devoted to the study of Bitcoin, and a lot of results have been achieved. Later, with the development of blockchain technology, Ethereum began to appear, intended for the next generation of cryptocurrency and decentralized application platform. Ethereum is the representative of Blockchain 2.0, which uses smart contracts to solve the problem of decentralized application in the monetary field [5,6].

*Corresponding author. Email: peide.liu@gmail.com

Neither Bitcoin nor Ethereum can guarantee the privacy of the transaction [7]. For a transaction on the blockchain, the sender, receiver and transaction amount are mainly involved. The identities of the sender and receiver are realized by the user's public-key address with a certain degree of anonymity, but some related information of the transaction subject can mine through data analysis or machine learning methods, and then combine some background knowledge to obtain the identity information of trader [8]. Hence, the transaction amount is completely exposed on the public chain, anyone can query and access it through the entire node of the blockchain. Attackers can obtain valuable information by analyzing transaction records, such as specific account fund balances, transaction details and specific capital flows, so the privacy of transactions cannot be guaranteed [9].

At the beginning of the design, the blockchain provides a certain degree of security for the designed system through a series of technologies to avoid damage, modification and data leakage due to external malicious attacks. In terms of privacy, the open and transparent nature of the blockchain has caused serious privacy issues such as transaction data and network node addresses. In order to further ensure the protection of user privacy, some related technologies have been applied in this field in recent years. In particular, anonymous digital currencies, such as Monero, Zcash and the newly launched Beam and Grin, etc., using ring signatures, zero-knowledge proofs, password commitments and other technologies to ensure the privacy of transaction senders, receivers and transaction amounts [10–13]. However, the privacy protection strategies are so strong that no one can supervise and control them, and they may be used in some illegal financial transaction activities, which is harmful to the society. Therefore, it is very valuable to find a suitable method that can protect privacy and facilitate supervision at the same time.

Blockchain, as a data structure that stores data in chronological order, can support different consensus mechanisms. The consensus mechanism is an important component of blockchain technology. The goal of the blockchain consensus mechanism is to enable all honest nodes to maintain a consistent view of the blockchain while satisfying consistency and effectiveness [14]. For example, there are plenty of consensus algorithms, such as proof of work (PoW), proof of importance (PoI), practical Byzantine fault tolerance (PBFT), measure of trust (MoT), proof of stake (PoS) and proof of space (PoSpace) [15,16]. In fact, the consensus mechanism is mainly used to eliminate trusted third parties or centralized entities. All nodes of the blockchain follow a specific consensus so that there will be no conflicts in the future, and the essence is to achieve privacy protection. However, the current consensus mechanism still has problems such as waste of computing power and energy, Matthew effect and low security. Therefore, adopting an effective consensus-based blockchain model to better solve the privacy protection is a current challenge.

To solve the above problems, this paper integrates multiple cryptographic technologies and proposes a blockchain transaction model with both privacy and supervision functions. First of all, we make use of the advantages of probabilistic public-key encryption to hide the real identity information of users. Then, with the help of the cryptographic commitment schemes and Zero-Knowledge Proof technology to verify the legality of blockchain transactions. Based on this, the regulators may obtain the real identity information of users through decryption, which fulfills the requirements of transaction privacy protection and the function of supervision. Moreover, regulators do not need to store the real identity and key information of user. Comparative analysis shows that the blockchain transaction model proposed in this paper is feasible and has practical value in various industrial scenarios such as digital currency, finance and energy.

The contributions of this paper are as follows:

- We combine with the cryptographic commitment scheme and Zero-Knowledge Proof to complete the legality verification of privacy transactions for the first time. Therefore, the identity-based encryption system enables regulators to obtain transaction amounts through decryption calculations without storing the key information, which satisfies the requirements of transaction privacy protection and supervision functions.
- Taking advantage of probabilistic public-key encryption to hide the users' real identity information. The same real identity can be encrypted for unlimited times to generate different anonymous identities. Regulators can directly obtain the real information by decrypting the anonymous identity without storing identity information.
- The blockchain transaction model with privacy protection and supervision functions proposed in this paper does not rely on a specific consensus mechanism and can be used as an independent module in the existing blockchain technology.

The remainder of this paper is organized as follows. Section 2 describes recent advances in protecting the privacy of blockchain transactions. Section 3 describes background related to blockchain technology. Section 4 describes the overall methodology. Section 5 presents and discusses the experimental results. Section 6 summarizes and presents conclusions.

2. RELATED WORK

To protect the privacy of blockchain transactions and hide the information of the sender, receiver and transaction amount, many blockchain-based technologies have been proposed.

In 2015, DASH was proposed, the process of mixing coins is carried out by means of main node deposit, which can hide the mapping relationship between input address and output address to achieve the purpose of anonymity [17]. But this is a centralized processing method, so there may be problems such as denial of service attacks and mixed coin users of leaking the mixing process. Maurer *et al.* proposed CoinJoin, which merges multiple transactions into one transaction and hides the correspondence between input and output parties to enhance the privacy protection ability of users, but it also faces the threat of centralized mixing coins [18]. Compared with the mixing coins' scheme, Li *et al.* used a ring signature mechanism to implement privacy protection digital currency, and it no longer needs to interact with other users [10]. Users implement anonymous processing by themselves, which can effectively eliminate the problems faced by the centralized mixed coins scheme. However, due to the use of complex cryptography technology, the speed of system operation and verification process is reduced. Zcash is a new type of digital currency constructed on

the basis of Zerocoin, which uses a cryptographic commitment scheme to encapsulate the sender, receiver and transaction amount of the transaction into parameters, and then uses zkSNARKs Zero-Knowledge Proof to prove the transaction and realize the concealment of the sender, receiver and transaction amount of blockchain transactions, it has the best privacy protection until now [11,19,20]. But the process of its proof is very slow, and there are bottlenecks in efficiency. In 2019, Beam and Grin went online, which used MimbelWimble protocol and aggregated signatures to achieve the purpose of privacy protection of blockchain transactions [12,13,21]. However, both parties of the transaction need to perform an online interaction process, which is not convenient to use in practice. Therefore, we need to develop an effective and practical method to solve the problem of privacy protection.

Due to the strong privacy protection capabilities of anonymous digital currency, it is difficult for financial institutions and state agencies to supervise digital currency participants and transactions between them, making digital currency has gradually become the tool of money laundering, tax evasion and illegal transactions. Sun *et al.* proposed a multi-chain model suitable for central bank-supervised digital currencies, but the communication between chain nodes is more complicated, and the design of super chain makes it lose decentralized characteristics and cannot guarantee the privacy of transactions [22]. Zhang *et al.* proposed a digital currency supervision model with a double-chain structure, anchoring the alliance chain on a public chain [23]. As a consensus participant, the alliance chain guarantees the privacy of transactions through secret sharing, and provides the characteristics of supervision, while ensuring the decentralization and anonymity of digital currencies. Therefore, how to enable blockchain transactions to achieve both privacy capabilities and requirement of regulatory is a hot topic of current research, but the current research results are still very few.

This paper integrates a variety of cryptographic techniques to propose a blockchain transaction model that takes into account privacy protection and supervision functions. Among them, the probabilistic public-key encryption algorithm is used to hide users' real identity information and realize the identity anonymity of user transactions. The cryptographic commitment scheme and Zero-Knowledge Proof are used to realize the privacy protection of the blockchain transaction amount and ensure the legality of transaction verification. In addition, the use of identity-based encryption technology to realize the supervision function of transaction information. Based on the above advantages, the blockchain transaction model proposed in this paper is of great application value while ensuring the privacy of users' transactions, making it easier for regulators to track illegal financial transaction activities.

3. BACKGROUND

In this section, through detailed theoretical analysis, we will reveal the internal process of the blockchain technology, unspent transaction output (UTXO) model and cryptography applied in this paper, which are the basic components of the scheme.

3.1. Blockchain Technology

Blockchain is a decentralized distributed ledger, which can be simply understood as a distributed database that distributed on various nodes around the world, which is connected by blocks in chronological order to form a chain. If the data in any block was changed, it will cause subsequent changes to the blockchain, which makes it immutable [15,24]. Current mainstream blockchain platforms include Bitcoin, Ethereum and Hyperledger Fabric [1,5,25]. From Figure 1, we can see the structure of the blockchain, there are multiple transactions recorded in the block. Whether blockchain is licensed or multi-licensed depends on how individuals verify and send transactions or how entities are authorized to verify and execute transactions (or conduct transactions alone). Blockchain is based on cryptography rather than credit, allowing any two parties to reach an agreement to pay directly without the involvement of a third-party intermediary.

Transactions are written into the blockchain through a consensus mechanism. It is one of the core technologies of the blockchain and determines which node is responsible for accounting, and the accounting method will affect the security and reliability of the whole system. Common consensus mechanisms mainly include PoW, PoS, PBFT, etc. [26–28]. This paper mainly studies the blockchain transaction model and does not rely on specific consensus mechanisms.

3.2. UTXO Model

Blockchain technology is the bottom technology of bitcoin and the core and basic structure of Bitcoin. We define bitcoin transaction as a transfer of BTC ownership from the buyer's purse to the seller's purse in exchange for a product or service. The buyer's BTC wallet assembles a transaction using the buyer's UTXO stored in the blockchain. A BTC amount claimed in advance by a UTXO designated buyer for transactions previously processed. UTXO stands for the unspent transaction output and is the core concept of bitcoin transaction generation and verification. Multiple transactions are recorded on the bitcoin ledger, each of which has several transaction inputs (transferors), which is the source of funds; and several transaction outputs (receivers), which is the destination of funds. Figure 2 is an example of the Bitcoin UXTO model. We can see that the input of transaction 1 is 1 BTC, and the two outputs are 0.4 BTC and 0.5 BTC. The difference of 0.1 BTC between input and output is caused by transaction fee. Transaction 2 is similar to transaction 1, and its output is used as the input of transaction 3, thus forming a chain structure of the transaction.

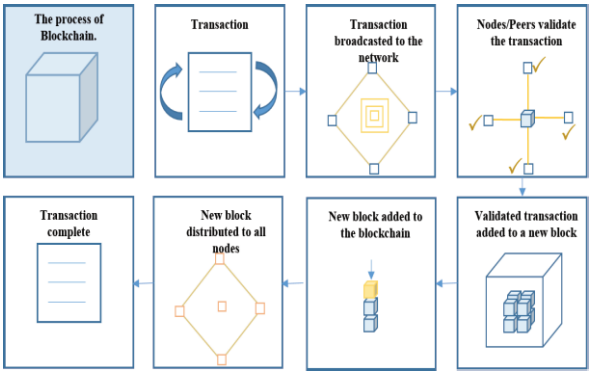

Figure 1 The structure diagram of blockchain.

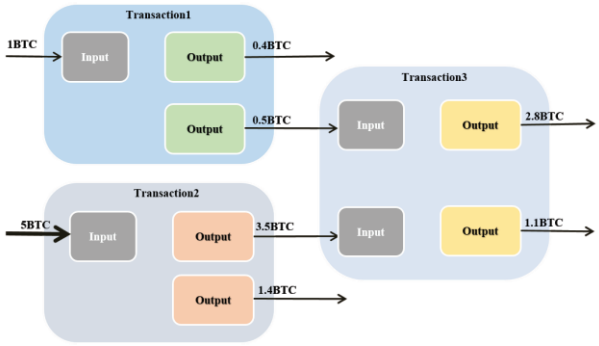

Figure 2 The example of Bitcoin UTXO transaction model.

In this paper, the blockchain transaction form mainly adopts bitcoin's UTXO model, and the transaction consists of sender, receiver and transaction amount. Transaction privacy refers to the protection of the sender's identity, receiver's identity and transaction amount without external disclosure; transaction supervision refers to the ability of regulators to query the information of the transaction sender, receiver and transaction amount by using curtain methods.

3.3. Cryptography

The cryptography is the most important invention and progress of modern cryptography. It is generally understood that cryptography is to protect the confidentiality of information transmission. The verification of the true identity of the sender and receiver of the information, the nonrepudiation of the sent/received information after the fact, and the protection of the integrity of the data are another aspect of modern cryptography. In blockchain transactions, it is necessary to adopt relevant cryptographic techniques to ensure security, we will introduce the probabilistic public-key cryptosystem, identity-based cryptographic algorithms and cryptographic commitment schemes in this subsection. These three technologies belong to classic cryptographic algorithms and play a vital role in ensuring the privacy of the transaction model proposed in this paper.

3.3.1. Probabilistic public-key cryptosystem

Probabilistic public-key encryption is a kind of nondeterministic cryptography. For the ciphertext generated by the same plaintext randomly changes, under the assumption of computational security, it is impossible to obtain any valid information of the plaintext through ciphertext related attacks in polynomial time. Goldwasser *et al.* used the quadratic residue theorem to design a probabilistic public-key cryptographic scheme, but it has high ciphertext scalability [29]. Blum *et al.* gave a more effective probabilistic public-key encryption system, which greatly reduces the expansion of ciphertext data [30]. Therefore, based on the above theoretical analysis, we chose the Blum–Goldwasser (BG) scheme to encrypt the users' identity information, which is more effective and uses the Blum Blum Shub (BBS) generator to improve the randomness of the ciphertext [31]. The idea of BG's probabilistic public-key cryptosystem is as follows: A random seed s_0 uses a BBS generator to generate m pseudo-random bits $z_1, z_2, \ldots z_m$, and then uses z_i as a key stream, i.e., they are XORed with l-length plaintext bits to form a ciphertext. At the same time, the $m+1th$ element $s_{m+1} = (s_0)^{2^{m+1}} \bmod n$ Transmit as part of the ciphertext. When the receiver receives the ciphertext, he can calculate s_{i+1} from s_0; then reconstruct the key stream, and finally XOR the key stream with m ciphertext bits to obtain the plaintext. The detailed algorithm process of BG is as follows:

Parameter setting: Set $n = pq$, where p and q are large prime numbers, $p \equiv q \equiv 3$, then n is public key, and p and q are private keys. Suppose the plaintext space $P = (Z^2)^m$, ciphertext space $C = (Z^2)^m \times Z_n^*$ and keyspace $K = \{(n, p, q)\}$.

Encryption algorithm: For $K = \{(n, p, q)\}$, $x \in (Z_2)^m$, $r \in Z_n^*$, the process of encryption is:

- select the seed s_0 randomly, use the BBS generator to generate m random bits $z_1, z_2, \ldots z_m$ as the keystream;
- calculate $s_{m+1} = (s_0)^{2^{m+1}} \bmod n$;
- calculate $y_i = (x_i + z_i) \bmod 2$, where $1 \le i \le m$;
- ciphertext is $c = E_k(x, r) = (y_1, \ldots, y_m, s_{m+1})$.

Decryption algorithm: To decrypt y, the following steps should be completed:

- calculate $a_1 = ((p+1)/4)^{m+1} \bmod p - 1$;
- calculate $a_2 = ((q+1)/4)^{m+1} \bmod q - 1$;
- calculate $b_1 = s_{m+1}^{a_1} \bmod p$;
- calculate $b_2 = s_{m+1}^{a_2} \bmod q$;
- use Chinese Remainder Theorem calculates r and satisfies the following conditions:
  $r \equiv b_1 \bmod p$ and $r \equiv b_2 \bmod q$;
- use the BBS generator to calculate $z_1, z_2, \ldots z_m$ from the seed $S_0 = r$;
- calculate $x_i = (y_i + z_i) \bmod 2$, where $1 \le i \le m$;
- the decrypted plaintext is $x = x_1, x_2, \ldots, x_m$.

3.3.2. Identity-based cryptography

Identity-based cryptography (IBC) can effectively solve the problem of public key infrastructure (PKI) digital certificate management [32]. The security of cryptographic mechanisms mostly relies on the assumption of certain mathematical problems and achieves a certain security strength under a certain security model. Therefore, we first introduce the relevant theoretical hypothesis.

Definition 1. The problem of Diffie–Hellman (DH) [33]. Given a large prime number q, a large integer generator $g \in Z_q^*$, and $g^a \bmod q$ and $g^b \bmod q$ generated by large random numbers a, b, $g^{ab} \bmod q$ is required to be found.

Definition 2. The problem of computational Diffie–Hellman (CDH) [33]. For randomly given $< P, aP, bp >$, where a, b belongs to the point group Z_q^* with order q, calculate the value of abP.

Definition 3. The problem of computational decision Diffie–Hellman (DDH) [34]. Distinguish the distribution between a given

tuple $<P, aP, bp, abp>$ and $<P, aP, bp, cp>$, i.e., determine whether c is equal to ab mod q, where a, b, c belong to the point group Z with order Z_q^*.

Definition 4. The problem of strong Diffie–Hellman inversion (q-SDH) [35]. Given $q+1$ dimensional tuple $<g, g^x, g^{x_2}, ..., g^{x_p}> \in G$, calculate $g^{1/x} \in G$.

Definition 5. The problem of bilinear Diffie–Hellman (BDH) [36]. Let G_1 and G_2 be two point groups with prime order q, $e: G_1 \times G_1 \rightarrow G_2$ is an acceptable bilinear mapping, P is the generator of G_1, for a given $<P, aP, bP, Cp>$, where $a, b, c \in Z_q^*$, calculate $W = e(P,P)^{abc} \in G_2$.

IBC generates the master public key and master private key by key generation center (KGC), then KGC uses its own key to generate the users' private key according to the identity information ID (such as name, email, ID number, etc.), which is the public key without digital certificate binding. This paper mainly adopts SM9 standard algorithm of China as an example of the IBC cryptosystem. SM9 uses various unique identifiers as public keys for data encryption and identity authentication, which is very suitable for applications such as email protection, secure circulation of official documents, multimedia converged secure communications, identity authentication, secure communications in the Internet of Things, cloud data protection, etc. The SM9 algorithm uses the bilinear pairing on the elliptic curve as the basic mathematical tool, and constructs a security proof based on the relevant calculation complexity assumptions, which greatly improves the protection level of my country's information security. Such a system has a natural password delegation function, which is very suitable for a supervised application environment, and has considerable advantages in the management and control of a large number of interconnected devices. SM9 standard is divided into five parts: general principles, digital signature algorithm, key exchange protocol, key encapsulation mechanism, public-key encryption algorithm and parameter definition. The following mainly introduces SM9 digital signature algorithm.

Let P_1 be the generator of the elliptic curve additive cyclic group G_1, P_2 is the generator of the elliptic curve additive cyclic group $G_1, H(\cdot)$ is the Hash function and $e(\cdot)$ is the bilinear pair. Assuming that A is the signer and B is the verifier, the process of generating the SM9 digital signature is as follows:

Key generation: The random number $Ks \in [1, N-1]$ generated by KGC is used as the master private key of signature, calculate $P_{pub-s} = [ke] P_2$ as the master public key of signature, then the encryption master key pair is (ke, P_{pub-s}). User A's identification is ID_A. To generate user A' s signature private key ds_A, KGC calculates $t_1 = H(ID_A, N) + ks$, $t_2 = ks \cdot t_1^{-1}$ on the finite field F_N, then gets $ds_A = [t_2] P_1$.

Process of signing: Suppose the message to be signed is M, the signature process of user A is as follows:

- calculate $g = e(P_1, P_{pub-s})$;
- choose a random number $r \in [1, N-1]$;
- calculate $w = g^r$, $h = H(M \| w, N)$, $l = (r-h) \bmod N$;
- calculate $S = [l] ds_A$, then the signature of M is (h, S).

Process of verification: In order to verify the signature (h', S') of message M', B performs the following process:

- calculate $g = e(P_1, P_{pub-s})$;
- calculate $t = g^{h'}$, $h_1 = H(ID_A, N)$;
- calculate $P = [h_1] P_2 + P_{pub-s}$, $u = e(S', P)$, $w' = u \cdot t$;
- calculate $h_2 = H_2(M' \| w', N)$, if $h_2 = h'$, then sign verification passes, otherwise it fails.

3.3.3. Cryptographic commitment scheme

In this paper, cryptographic commitment scheme mainly adopts Pedersen commitment and is used in Monero to protect the privacy of transaction finance [10]. Pedersen commitment is a homomorphic commitment protocol that satisfies perfect concealment and computational binding. Its perfect concealment does not depend on any difficult assumptions. The computational binding relies on the discrete logarithm assumption (DLA). And its construction is divided into 3 stages.

- **Setup:** Select the multiplicative group G and generator with the order of large prime q, $G =< g >=< h >$, open tuple (g, h, q);
- **Commitment:** The promise party chooses a random number r as the blind factor, calculates the promise value and then sends commitment to the receiver;
- **Open:** The promiser chooses a random number r as the blind factor, calculates the promise value and then sends commitment to the receiver; open phase open: the promiser sends (v, r) to the receiver, and the receiver verifies whether commitment is equal to $g^v h^r$ mod q, if they are equal, then accept, otherwise refuse to promise.

The complete data formula is expressed as follows:

$$P = xg + rH \tag{1}$$

where g and H are the base points in elliptic curve cryptography (ECC), and r is the blind factor to protect the privacy of the value x. In addition, it is necessary to use Bulletproofs Zero-Knowledge Proof to realize the range proof of the transaction amount in a more efficient way [36]. Bulletproofs is a more space-efficient form of zero-knowledge proofs. Importantly, for our purposes, these proofs also have native support for commit values such as Pedersen commitments and public keys. This allows us to implement functions such as range proofs in a general zero-knowledge framework, instead of implementing complex elliptic curve algorithms in zero-knowledge.

4. REGULATABLE BLOCKCHAIN TRANSACTION PRIVACY PROTECTION MODEL

This paper combines UXTO, BG, IBC, Pedersen commitment and other technologies to propose a regulatable blockchain transaction

privacy protection model, which could be seen in Figure 3. From the Figure, we can describe the complete implementation process as the regulators first realize the identity anonymity of the sender and the receiver, UTXO ensures the security of the amount during the transaction and the miner is used to ensure the legitimacy of the identity of the trader and the transaction amount. Next, we will introduce the design process in detail.

4.1. Transaction Model

The participants of the transaction in this scheme are shown in Figure 4, mainly including (1) sender and receiver of the transaction, hoping to protect their identity anonymity and the privacy of the transaction amount through a secure transaction; (2) blockchain miner, verify the legitimacy of transactions and packing them into blocks and storing them on the blockchain through consensus mechanisms; (3) regulators, track relevant participants in transactions and transaction finance to combat financial illegality criminal activities if necessary; (4) third party, who steals transaction-related information through certain technical means to obtain improper benefits.

The blockchain transaction privacy protection is relative, which mainly prevents the third parties from maliciously collecting user information. However, for regulators, it's necessary to track some illegal transactions to combat illegal and criminal activities. Therefore, it is necessary to ensure that transactions are regulatable. The content of supervision includes the identity of participating traders and the amount of transactions.

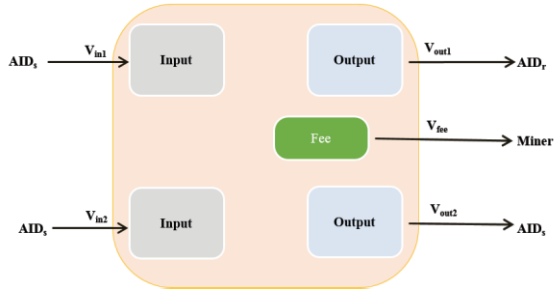

Figure 3 The example of Bitcoin UTXO transaction model.

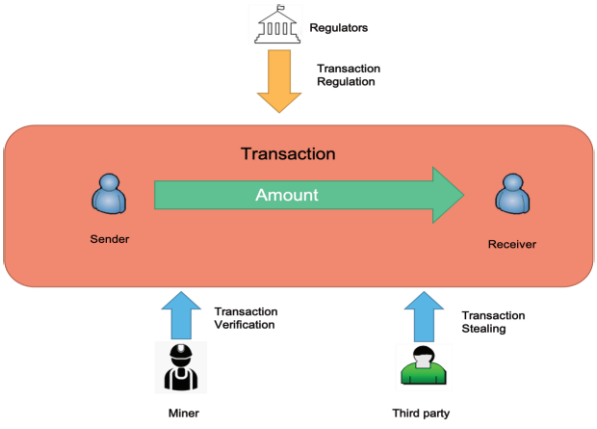

Figure 4 The blockchain transaction entity in the scheme proposed of this paper.

4.2. Realization of Anonymous Identity

In the initial phase of the model, regulators need to generate three pairs of public and private keys: one pair is, regulators use BG to generate the corresponding private key Sk_{BG} and public key Pk_{BG}; another one, regulators act as the KGC in the IBC cryptosystem and generates the master public key MPK and master private key MSK; the other one, regulators define the identity of the IBC as ID_a, and sets ID_a as the public key, based on the IBC algorithm, use MSK to generate the corresponding signature's private key Sk_a.

$$Sk_a = IBC.KeyGen_{MSK}\left(ID_a\right) \tag{2}$$

Then the user in the system applies for key distribution to regulators through the uniquely identifying information ID_u. ID_u needs to be self-certified, which can be the user's email address, ID number and mobile phone number, etc. After authenticating the user's identity information, the regulators use the BG algorithm's public key Pk_{BG} to encrypt the user's identity information ID_u to generate AID_1, as follows:

$$AID_1 = BG.Enc_{Pk_{BG}}\left(ID_u\right) \tag{3}$$

To ensure that the user's ID_u is certified by regulators, need regulators to perform signature verification on AID_1 and generate AID_2,

$$AID_2 = IBC.Sign_{Sk_a}\left(AID_1\right) \tag{4}$$

Define $AID_u = AID_1 \parallel AID_2$, because AID_1 is obtained by using ID_u with BG, with good randomness. AID_2 is AID_1 obtained by IBC signature, so AID_u also has good randomness, which can effectively hide the user's user real identity information ID_u, realize identity anonymity.

Then use AID_u as the public-key identity. Based on the IBC algorithm, regulators use MSK to generate the user's corresponding private key Sk_u, which is

$$Sk_u = IBC.KeyGen_{MSK}\left(AID_u\right) \tag{5}$$

Users' self-certified real identity information is ID_u, the calculated anonymous identity information is AID_u, and the corresponding private key is Sk_u. Due to the BG probabilistic public-key encryption algorithm, the same ID_u can be encrypted to generate different AID_u, ID_u and AID_u have a one-to-many relationship, and theoretically the same ID_u can generate an unlimited number of AID_u, enabling users to continuously update AID_u, thereby achieving good anonymity of users' identity.

In order to facilitate the subsequent description, we define the identities of the sender and receiver of the transaction as ID_s and ID_r respectively. The corresponding anonymous identities are calculated as AID_s and AID_r, the private keys are Sk_s and Sk_r. When the sender conducts a transaction with the receiver, he only needs to use Sk_s to unlock the UTXO input script and use AID_r as the receiver's address to achieve identity anonymity. In order to prevent the sender from sending the transaction to an illegal address

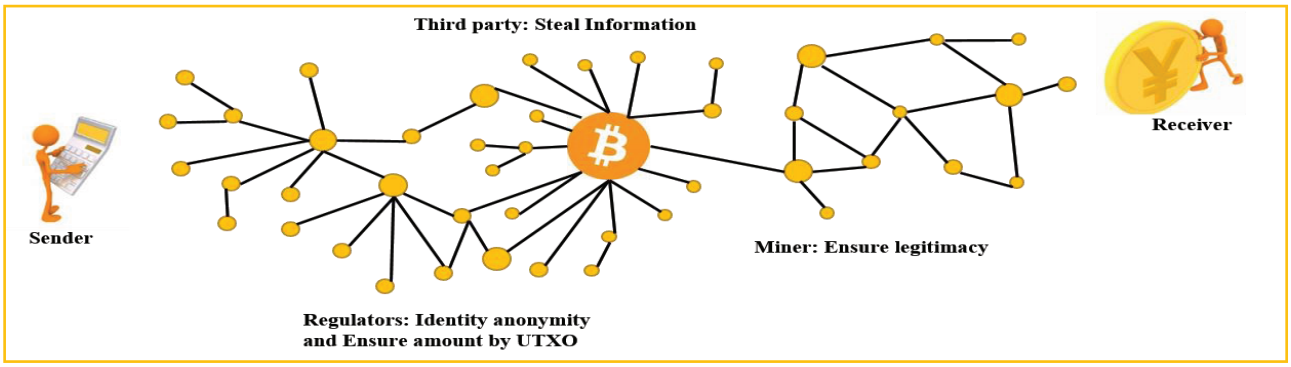

Figure 5 | The complete framework diagram of the scheme.

that does not exist, resulting in asset loss, it is necessary to verify the legitimacy of the receiver's address with the help of miners.

4.3. Privacy Protection of Transaction Amount

When the sender AID_s needs to conduct a transaction with the receiver AID_r, the generality is not lost, as shown in Figure 5:

In the transaction, AID_s has two inputs, the amount is V_{in1} and V_{in2}; there are two outputs, which are the transaction using AID_r, the amount is V_{out1}, and the change fee returned to itself is V_{out1}, and the other part of V_{fee} is the handling fee, i.e., the cost of the miner's package transaction.

The scheme in this paper mainly adopts Pedersen commitment to realize the privacy protection of the transaction amount $\left(V_{in1}, V_{in2}, V_{out1}, V_{out2}\right)$, and the handling fee V_{fee} is publicly disclosed. For transaction's input, the previous output needs to be introduced, then

$$P_{in1} = V_{in1}G + a_1H \tag{6}$$

$$P_{in2} = V_{in2}G + a_2H \tag{7}$$

$\left(V_{in1}, a_1\right)$ and $\left(V_{in2}, a_2\right)$ can be decrypted by AID_s with the private key Sk_s.

For output, the sender AID_s selects two random numbers b_1, b_2 and then calculate

$$P_{out1} = V_{out1}G + b_1H \tag{8}$$

$$P_{out2} = V_{out2}G + b_2H \tag{9}$$

$$P_{fee} = V_{fee}G \tag{10}$$

P_{out1} and P_{out2} are mainly for miners to verify the legality of transactions. In order for the receiver to obtain $\left(V_{out1}, b_1\right)$ and $\left(V_{out2}, b_2\right)$ they need to be encrypted with receiver's public key respectively, then get

$$C_{out1} = IBC.Enc_{AID_R}\left(V_{out1}, b_1\right) \tag{11}$$

$$C_{out2} = IBC.Enc_{AID_s}\left(V_{out2}, b_2\right) \tag{12}$$

To ensure the legality of the transaction, it is necessary to calculate them. Moreover, we can define the public key of the transaction and calculate the private key of the transaction. Making use of the ECC to sign the transaction, we get the relevant results:

$$V_{in1} + V_{in1} = V_{out1} + V_{out2} + V_{fee} \tag{13}$$

$$\left(P_{in1} + P_{in2}\right) - \left(P_{out1} + P_{out2} + P_{fee}\right) = \left(a_1 + a_2 - b_1 - b_2\right)H \tag{14}$$

$$Pk_{T_z} = \left(a_1 + a_2 - b_1 - b_2\right)H \tag{15}$$

$$Sk_{T_z} = a_1 + a_2 - b_1 - b_2 \tag{16}$$

$$M_{T_z} = \left\{P_{in1}, P_{in2}, \left(P_{out1}, C_{out1}\right), \left(P_{out2}, C_{out2}\right), V_{fee}\right\} \tag{17}$$

$$Sig_{T_z} = ECC.Sign_{Sk_{Tx}}\left(M_{T_X}\right) \tag{18}$$

In addition, it is necessary to prove the range of transaction amount to avoid negative value. It can be realized through Bulletproofs Zero-Knowledge Proof, which exists as an assistive technology in the blockchain. It means that the verifier cannot obtain any additional information other than the result of the judgment (wrong or right). In the late 1980s, Blum and others further proposed the concept of "Bulletproofs Zero-Knowledge Proof," replacing the interactive process with a short random string and realizing zero-knowledge proof [30,37]. Therefore, the final transaction can be expressed as follows:

$$T_x = \left\{M_{T_x}, Sig_{T_x}, P_{range}\right\} \tag{19}$$

where P_{range} is the relevant content of the proof of transaction amount range. Broadcast T_x through the network to the outside world. After the miners verify its legitimacy, it is packaged into blocks and recorded on the blockchain ledger through the consensus mechanism. The receiver can confirm receipt of the transaction according to AID_r and then use the private key Sk_r decrypts C_{out1} and obtains the transaction information. In summary, we have completed the entire transaction process while hiding the transaction amount. The legality of the transaction amount is verified in two aspects by miners: the input and output amounts are equal and the output amount is within the valid range.

5. EXPERIMENTAL ANALYSIS AND DISCUSSION

A thorough experimental and analytical analyses were carried out on the proposed model. Specifically, privacy tests on the blockchain model and analyzes the privacy protection capabilities of the proposed scheme and compares it with the existing blockchain privacy protection transaction schemes.

5.1. The Ability of Privacy Protection

For users' identity information, AID_u privacy users' real information ID_u, if AID_u is used frequently (e.g., in a transaction), set AID_u as the transaction input and output address at the same time, it is easy to infer that this is the change information given by traders. In order to improve privacy, this paper uses BG so that different seed s_0 can be randomly selected for each encryption, the same ID_u can generate countless anonymous AID_u addresses and AID_u cannot be distinguished from each other. Therefore, the user can generate AID_u in batches by regulators without changing ID_u, and replace the AID_u in each transaction. The third party cannot recognize the changes of output in a trading and track the whole process of trading, or even speculate any effective information, so this scheme can realize the strong ability of privacy protection.

5.2. Baselines Schemes

In this subsection, we compare the performance using 8 baseline models to test our proposed scheme.

- **Bitcoin:** Public key is used to realize identity anonymity and transaction amount is disclosed.
- **Ethereum:** Public key is used to realize identity anonymity and transaction amount is disclosed.
- **Dash:** The scheme is simple and mainly depends on the master node.
- **Monero:** The ring signature relies on other public keys and the verification is complicated.
- **Zcash:** Strong anonymity, but the parameter initialization is complicated, and the proof generation is time-consuming.
- **Beam/Grin:** Using MimbleWimble protocol, the implementation is simple, but requires an interactive process.
- **Literature 22:** With the multi-chain architecture, the node communication is more complicated, and the decentralization characteristic is lost.
- **Literature 23:** The double-chain structure is adopted to ensure the privacy of transactions. The chain structure is more complicated.
- **Our model:** The solution is simple to implement, but requires initial user authentication.

5.3. Comparison and Analysis

This subsection compares and analyzes the proposed regulatable blockchain anonymous transaction scheme in this paper with the existing blockchain transaction scheme, as shown in Table 1. At the same time, in order to observe the performance of all methods more intuitively, Figure 6 shows them in the form of images.

Table 1 Performance comparison of blockchain technology.

Blockchain Technology	Main Technologies	Privacy Protection	Regulatable Function	Protection Against Identification Attack	Low Storage Usage	Independence
Bitcoin	ECDSA, SHA256	×	×	√	×	√
Ethereum	ECDSA, Keccak	×	×	√	×	√
Dash	CoinJoin	√	×	×	√	√
Monero	Hidden address, Ring signature, Pedersen commitment	√	×	×	×	√
Zcash	zkSNARKs, Pedersen commitment	√	×	×	×	√
Beam/Grin	Pedersen commitment, Aggregate signature	√	×	×	√	√
Literature 22	Multi-chain	×	√	√	×	√
Literature 23	Alliance chain and public chain technology	√	√	√	×	√
Our model	-	√	√	√	√	√

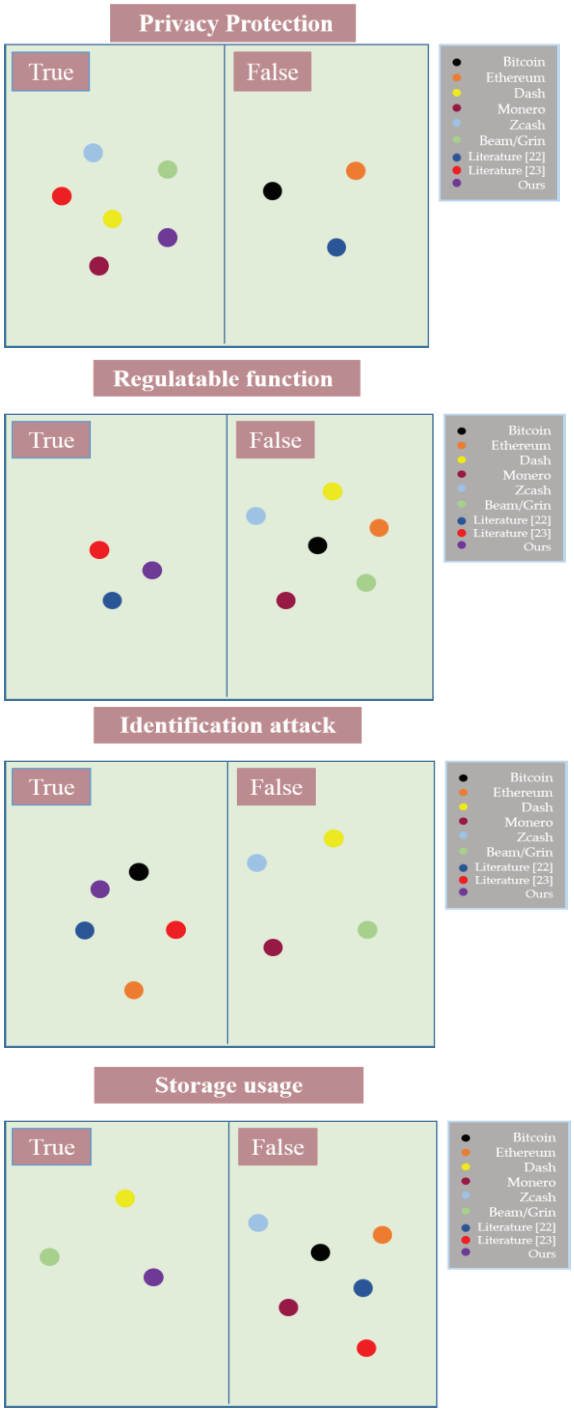

Figure 6 Intuitive schematic diagram of the models' performance.

Different colors represent different baseline models, and we classify them according to their performance. To further verify the performance of the solution proposed in this article, we have added three additional indicators, namely, protection against Identification attack, low storage usage and independence. They are used to verify the sender and receiver's identity protection and the storage size of privacy protection models. Among the existing cryptocurrencies, Bitcoin and Ethereum have a weak realization of the anonymity of identities, and the transaction amount has been completely disclosed to the outside world without privacy protection. Dash uses hybrid coin technology to mix the input and output of multiple transactions through the master node, but there is a risk of centralization, it may lead to the disclosure of user privacy. Therefore, when the Dash model faces an identity attack, it is difficult to avoid the risk. However, Monero adopts hidden address and ring signature technology, which no longer relies on centralized nodes, but needs to be mixed with other users' public keys and verification is relatively complicated. Zcash adopts the zkSNARKs Zero-Knowledge Proof scheme, which can achieve very strong anonymous privacy protection and make the model unable to be effectively supervised and has certain supervision loopholes. Moreover, the zkSNARKs scheme is very complicated to implement and requires initial trusted parameter settings. The generation of the proof is very time-consuming, which affects the practical efficiency. This feature of zkSNARKs makes it require higher storage usage. Both Beam and Grin use Pedersen commitment and aggregate signature technology to use the MimbleWimble protocol, which makes the implementation of the two simple, but requires an interactive process between the two parties, so it is more inconvenient to use. The above features make the two parties unable to deal with identity attacks. None of the above blockchain transaction privacy protection schemes have regulatable functions, which is indispensable in the transaction model and can greatly reduce risks. Therefore, a trading plan with regulatory functions is an indispensable indicator for us. Literature [22] proposed a multi-chain model suitable for supervision, but the communication between chain nodes is more complicated, and the super chain structure also makes it lose the decentralization characteristics and cannot protect the privacy of transactions. Literature [23] proposed a digital currency supervision model that adopts a double-chain structure, which combines alliance chains and public chains to ensure the privacy of transactions through secret sharing, while providing regulatable features, but the realization of the double-chain structure is more complicated. Both the model and the method proposed in this article are used to improve the privacy protection and supervision of blockchain transactions, which allows them to obtain basically satisfactory results. However, the solution we proposed is simpler in comparison, and has low storage characteristics, which can be conveniently applied to physical places such as health monitoring and bank transactions. Through comparison, it can be found that our proposed method is superior to other traditional methods, which fully verifies the validity of the above argument and the superiority of our scheme. As far as independence is concerned, the abovementioned baseline method and our scheme have this characteristic, but their degree of independence is slightly different.

By comparing with the existing schemes, it can be seen that the scheme proposed in this paper does not need to rely on a centralized master node, does not need to introduce other public keys for ring signatures, does not need to implement a complex zkSNARKs certification process, does not require a cumbersome interaction process and no complex multi-chain structure is required. Through the use of probabilistic public-key encryption, IBC cryptosystem and Pedersen commitments, the scheme have both privacy protection and regulatable functions, which make regulators do not need to store users' real identity and key information and greatly reduces the storage and calculation pressure. The abovementioned features make it possible to protect the user's identity, thereby avoiding attacks. Nowadays, more and more researchers are committed to the

development of lightweight models, which are not only convenient, but also have certain application value. The scheme proposed in this paper has this characteristic, so it has great application prospects.

6. CONCLUSIONS AND FUTURE WORK

The application of blockchain technology not only protect the privacy of user transactions, but also ensure the legality of user transactions. Therefore, it is necessary to achieve a balance between privacy protection and regulatory requirements. While providing convenience to users, it strictly combats certain illegal transactions. Therefore, we integrate a variety of cryptographic techniques, using probabilistic public-key cryptography, IBC cryptography, Pedersen commitment, Bulletproofs Zero-Knowledge Proof, etc., to form a blockchain transaction model with privacy and supervision functions. With the advantages of probabilistic public-key encryption, the users' real identity information can be hidden and transaction anonymous identities can be generated, and the same real identity can be encrypted for unlimited times to generate different anonymous identities, which is convenient for users to realize the privacy protection of user transaction identity information by changing their anonymous identities. Pedersen promise and Bulletproofs technology are used to verify the legality of blockchain transactions. Regulators can use decryption to obtain the user's real identity information, and obtain the transaction amount through IBC cryptography, which satisfies the requirements of transaction privacy protection and supervision functions.

The blockchain transaction model proposed in this paper can be used as an independent module in the existing blockchain technology. Security performance analysis shows that the blockchain transaction scheme in this paper is simple and practical, and has a wide range of applications in the fields of digital assets and energy transactions.

Based on the above analysis, we find that the method proposed in this article can well balance privacy protection and supervision. We also believe that a lot of research is needed to enhance security and privacy protection. Typical network attacks and privacy issues can be used to undermine the stability of the blockchain system. Currently, all evolving solutions may slightly improve security and privacy, but usually accompanied by price increases make users suspicious of using such systems. However, with the help of this method to optimize the decision-making of users and regulators, further improvements are needed to realize the application. The fuzzy decision algorithm can evaluate the algorithm well and successfully capture the uncertainty, which is of great significance to improve the performance of the algorithm, and thus is applied to many industries [38]. Combining the solution proposed in this article with Pythagorean fuzzy uncertain environments will be our main research direction in the future.

CONFLICTS OF INTEREST

The authors declare they have no conflicts of interest.

AUTHORS' CONTRIBUTIONS

Conceptualization, Zhiyuan Xue and Miao Wang; methodology, Zhiyuan Xue, Peide Liu; software, Zhiyuan Xue and Miao Wang; writing—original draft preparation, Zhiyuan Xue; writing—review and editing, Miao Wang and Qiuyue Zhang; visualization, Miao Wang and Qiuyue Zhang; supervision, Yunfeng Zhang and Peide Liu.

ACKNOWLEDGMENTS

This research was funded by the National Natural Science Foundation of China (Grant Nos. 61972227), the Natural Science Foundation of Shandong Province (Grant Nos. ZR2019MF051 and ZR201808160102) and in part by the Fostering Project of Dominant Discipline and Talent Team of Shandong Province Higher Education Institutions.

REFERENCES

[1] S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system, Online, https://bitcoin.org/bitcoin.pdf, 2008.
[2] Ministry of Industry and Information Technology, White paper for China blockchain technology and application development [EB/OL], 2016. http://5li08.cn/a4tzE
[3] M.U. Hassan, M.H. Rehmani, J. Chen, Differential privacy in blockchain technology: a futuristic approach, J. Parallel Distr. Comput. 145 (2019), 50–74.
[4] M. Conti, E.S. Kumar, C. Lal, S. Ruj, A survey on security and privacy issues of bitcoin, IEEE Commun. Surv. Tut. 20 (2018), 3416–3452.
[5] A. Sigh, R. Parizi, Q. Zhang, K. Choo, A. Dehghantanha, Blockchain smart contracts formalization: approaches and challenges to address vulnerabilities, Comput. Secur. 88 (2020), 101654.
[6] V. Aleksieva, H. Valchanov, A. Huliyan, Application of smart contracts based on ethereum blockchain for the purpose of insurance services, in Proceeding of International Conference Biomedical Innovations and Applications, Varna, Bulgaria, 2019, pp. 8–9.
[7] L.H. Zhu, F. Gao, M. Shen, Y.D. Li, B.K. Zheng, H.L. Mao, Z. Wu, Survey on privacy preserving techniques for blockchain technology, J. Comput. Res. Dev. 54 (2017), 2170–2186.
[8] P. Koshy, D. Koshy, P. McDaniel, An analysis of anonymity in bitcoin using p2p network traffic, in 18th International Conference Financial Cryptography and Data Security, Christ Church, Barbados, 2014, pp. 469–485.
[9] D. Ron, A. Shamir, Quantitative analysis of the full bitcoin transaction graph, in 17th International Conference Financial Cryptography and Data Security, Okinawa, Japan, 2013, pp. 6–24.
[10] Y. Li, G. Yang, W. Susilo, Y. Yu, D. Liu, Monero: anonymous cryptocurrency with enhanced accountability, IEEE Trans. Depend. Secure Comput. 18 (2020), 679–691.
[11] E.B. Sasson, A. Chiesa, C. Garman, M. Green, L. Miers, E. Tormer, M. Virza, Zerocash: decentralized anonymous payments from bitcoin, in Proceeding of the IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 2014, pp. 459–474.

[12] V. David, M.I. Ana, F. Vias, J. Emilio, Herding in the cryptocurrency market: CSSD and CSAD approaches, Finance Res. Lett. 30 (2019), 181–186.
[13] G. Fuchsbauer, M. Orrù, Y. Seurin, Aggregate cash systems: A Cryptographic Investigation of Mimblewimble, in: Y. Ishai, V. Rijmen (Eds.), Advances in Cryptology – EUROCRYPT, Lecture Notes in Computer Science, Springer, Cham, Switzerland, 2019.
[14] J. Garay, A. Kiayias, N. Leonardos, The bitcoin backbone protocol: analysis and applications, in 34th Annual International Conference Theory and Applications of Cryptographic Techniques, Berlin, Germany, 2015, pp. 281–310.
[15] N. Zhang, S. Zhon, Mechanism of personal privacy protection based on blockchain, J. Comput. Appl. 37 (2017), 2787–2793.
[16] A. Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for IOT security and privacy: the case study of a smart home, in IEEE International Conference Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 2017.
[17] R. Horgan, Dash for the cash, in: New Civil Engineer, Metropolis, London, United Kingdom, 2019, pp. 42–43.
[18] F.K. Maurer, T. Neudecker, M. Florian, Anonymous coin-Join transactions with arbitrary values, in IEEE Trustcom/BigDataSE/ICESS, Sydney, Australia, 2017, pp. 1–4.
[19] I. Miers, C. Garman, M. Green, A.D. Rubin, Zerocoin: anonymous distributed e-cash from bitcoin, in 2013 IEEE Symposium on Security and Privacy (SP), Berkeley, CA, USA, 2013, pp. 19–22.
[20] E. Ben-Sasson, A. Chiesa, D. Genkin, E. Tromer, M. Virza, Snarks for c: verifying program executions succinctly and in zero knowledge, in Proceeding of 33rd Annual Cryptology Conference in Advances in Cryptology (CRYPTO 2013), Santa Barbara, CA, USA, 2013, pp. 90–108.
[21] G. Betarte, M. Cristiá, C. Luna, A. Silveira, D. Zanarini, Towards a formally verified implementation of the mimblewimble cryptocurrency protocol, in Applied Cryptography and Network Security Workshops, Rome, Italy, arxiv-2104.00822, 2020.
[22] S. He, H. Mao, X. Bai, Z. Chen, Y. Wei, Multi-blockchain model for central bank digital currency, in International Conference on PDCAT, Taipei, Taiwan, 2017.
[23] J. Zhang, Z. Wang, Z. Xu, Y. Ouyang, T. Yang, A regulatable digital currency model based on blockchain, J. Comput. Res. Dev. 55 (2018), 2219–2232.
[24] Z. Kuo, X. Yongheng, Research review on internet of things security driven by blockchain technology, Inf. Netw. Secur. 17 (2017), 1–6.
[25] O. Attia, I. Khoufi, A. Laouiti, C. Adjih, An IoT-blockchain architecture based on hyperledger framework for healthcare monitoring application, in NTMS 2019 – 10th IFIP International Conference on New Technologies, Mobility and Security, Jun 2019, Canary Islands, Spain, pp. 1– 5
[26] C. Dwork, M. Naor, Pricing via processing or combatting junk mail, in Proceeding of 12th Annual International Cryptology Conference Advances in Cryptology (CRYPTO'92), Santa Barbara, CA, USA, 1992, pp. 139–147.
[27] S. Lande, M. Bartoletti, A.S. Podda, A proof-of-stake protocol for consensus on bitcoin subchains, in International Conference Financial Cryptography and Data Security, Sliema, Malta, 2017, pp. 568–584.
[28] C. Miguel, L. Barbara, Practical byzantine fault tolerance and proactive recovery, ACM Trans. Comput. Syst. 20 (2002), 398–461.
[29] S. Goldwasser, S. Micali, Probabilistic encryption, J. Comput. Syst. Sci. 28 (1984), 270–229.
[30] M. Blum, S. Goldwasser, An efficient probabilistic public-key encryption scheme which hides all partial information, in Workshop on the Theory and Application of Cryptographic Techniques, Santa Barbara, CA, USA, 1984. pp. 289–302.
[31] D.R. Stinson, Principles and Practices of Cryptography, third ed., Electronic Industry Press, Beijing, China, 2009.
[32] A. Shamir, Identity-based cryptosystems and signature schemes, *In*: Blakley G.R., Chaum D. (eds) Advances in Cryptology. CRYPTO 1984. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 1984.
[33] W. Diffie, M.E. Hellman, New directrions in cryptography, IEEE Trans. Inf. Theory. 22 (1976), 644–654.
[34] D. Boneh, The decision Diffie-Hellman problem, in Proceeding of 3rd International Symposium on Algorithmic Number Theory, Lecture Notes in Computer Science, Springer-Verlag, 1998, pp. 48–63.
[35] B. Dan, X. Boyen, Short signatures without random oracles, in International Conference Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, 2004. pp. 56– 73.
[36] D. Boneh, M.K. Fran, Identity-based encryption from the Weil pairing, SIAM J. Comput. 32 (2000), 586–615.
[37] B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, G. Maxwell, Bulletproofs: short proofs for confidential transactions and more, in IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2018, pp. 315–334.
[38] L. Wang, H. Garg, N. Li, Pythagorean fuzzy interactive Hamacher power aggregation operators for assessment of express service quality with entropy weight, Soft Comput. 25 (2020), 973–993.