IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON NEW ADVANCES IN BLOCKCHAIN-BASED WIRELESS NETWORKS

Received April 19, 2020, accepted May 4, 2020, date of publication May 14, 2020, date of current version June 23, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2994294

A Survey on Privacy Protection of Blockchain: The Technology and Application

DAN WANG, JINDONG ZHAO, AND YINGJIE WANG
School of Computer Science and Control Engineering, Yantai University, Yantai 264005, China
Corresponding author: Jindong Zhao (zhjdong@ytu.edu.cn)

This work was supported in part by the Shandong Key Research and Development Plan under Grant 2019JZZY010424.

ABSTRACT As a kind of point-to-point distributed public ledger technology, blockchain has been widely concerned in recent years. The privacy protection of blockchain technology has always been the core issue of people's attention. In this paper, some existing solutions to the current problems of user identity and transaction privacy protection are surveyed, including coin mixing mechanism, zero knowledge proof, ring signature and other technologies. Secondly, five typical applications of privacy protection technology based on blockchain are proposed and analyzed, which are mainly divided into technology applications based on coin mixing protocol, encryption protocol, secure channel protocol and so on. Finally, in view of the shortages of the existing blockchain privacy protection technology, we explore future research challenges that need to be studied in order to preserve privacy in blockchain system, and looks forward to the future development direction.

INDEX TERMS Blockchain, privacy protection, bitcoin, anonymity, security.

I. INTRODUCTION

Blockchain is the underlying technology behind digital cryptocurrencies such as bitcoin, ethereum and hyperledger. It originated by Satoshi Nakamoto (a pseudonym) on the bitcoin forum in 2008 – Bitcoin: A Peer-to-Peer Electronic Cash System [1], which has triggered a new round of technological revolution and industrial revolution, is one of the most cutting-edge and hottest technologies. With the help of distributed ledger, asymmetric encryption, intelligent contract, consensus mechanism and other core technologies, blockchain can achieve point-to-point, anonymity, traceability, tamper-proof and other features, and can guarantee the security and trust issues in the transaction process. In recent years, blockchain technology has been extended to digital finance [2], Internet of things (IoT) [3], [4], edge computing [5], Artificial Intelligence (AI) [6], Supply Chain Management (SCM) [7] and many other fields. Nowadays, many countries around the world are accelerating the development of block chain technology.

However, in order to reach a consensus, the nodes in the whole network need to disclose the transaction information on the chain, which brings serious privacy problems to users [8]. Therefore, it is of great significance to study targeted privacy protection methods. In recent years, there have been many technologies and typical applications for blockchain privacy protection, which can prevent attacks of stealing or tampering with privacy from different perspectives. In one word, while protecting the interests of users, privacy issues must not be ignored. For the purpose of providing some reference and help for current and future research, it is necessary to systematically analyze and summarize the privacy protection of blockchain.

The associate editor coordinating the review of this manuscript and approving it for publication was Yunchuan Sun.

II. BLOCKCHAIN PRIVACY PROTECTION

Privacy protection has been widely studied in distributed applications, mobile crowdsourcing [9], [10], IoT [11], [12], etc. As a type of distributed database, blockchain technology has significant advantages in privacy protection, such as information tamper-proof, anonymity and network stability [13], which can solve the privacy disclosure problems faced by some centralized services, such as the privacy protection intelligent parking system based on blockchain [14], the secret share voting system [15] and transparent voting platform [16]. However, the decentralized architecture and data storage mechanism adopted by blockchain technology also bring some adverse effects on privacy protection, among which the two main problems are user identity privacy challenge and user transaction privacy challenge [17], [18].

The rest of this paper is organized as follows: section II discusses the challenges of blockchain privacy protection from two aspects: user identity and user transaction; Section III proposes several key blockchain privacy protection technologies in view of the challenges, and makes a comparative analysis from the aspects of technical characteristics and anonymity; Section IV uses the privacy protection technology introduced in section III to put forward the corresponding technology application from five aspects. Finally, section V summarizes and anticipates the whole paper.

A. IDENTITY PRIVACY CHALLENGE

Identity privacy refers to the relationship between user's real identity and the blockchain address. The information on the blockchain cannot be changed. It is stored on the chain in the form of distributed ledger. Any node can obtain complete information from the chain. Although transactions on the blockchain have certain anonymity, with the develop of compute technology, anonymity cannot fully protect the privacy of user identity. An attacker can find out sensitive information by monitoring and analyzing the relevance of public data in the global ledger. For example, if there are stable related transactions between different addresses, the attacker can analyze the transaction relationship graph between different addresses and derive some data of user characteristic [19]. In addition, the attacker can obtain the corresponding transaction address by searching all possible transactions with approximate balance, and then can infer the user's identity information and location information [20].

B. TRANSACTION PRIVACY CHALLENGE

Transaction privacy refers to the transaction records stored in the blockchain and the potential information behind the transaction. The traditional information protection measure is to prevent the attacker from stealing or tampering by encrypting the information. However, in the process of encrypting transaction information in blockchain, on the one hand, it is necessary to ensure that the transaction information is not stolen by unauthorized nodes. On the other hand, it is necessary to verify the authenticity of the transaction without disclosing sensitive information, and the transaction content cannot be fully encrypted. There are contradictions between them, which are also difficulties and challenges in privacy protection technology.

To sum up, blockchain technology cannot provide absolute protection for users' privacy. It is necessary to introduce some privacy protection algorithms, protocols or other strategies to achieve blockchain privacy protection [21]. Thus, more focus should be put into blockchain privacy security issues.

III. KEY TECHNOLOGIES OF PRIVACY PROTECTION

Blockchain networks are open and tamper-proof, so they are vulnerable to network attacks. Although the transactions are anonymous, the attacker can still calculate the relationship between the two sides of the transaction by analyzing the transaction graph. The properties of public transparency of blockchain will threaten user privacy and transaction security. In order to increase the analysis difficulty of attackers, some privacy protection security mechanisms are proposed to solve this technical problem.

A. THE MECHANISM OF COIN MIXING

The mechanism of coin mixing was firstly proposed by Chaum in 1981 [22]. By adding intermediary transit information, it is difficult for attackers to analyze the communication information between the sender and the receiver, so the anonymity of communication is enhanced. As shown in Fig. 1, user A and B are the sender and receiver of the transaction, and C is the potential attacker. The mixing mechanism as a middleman to transfer transaction information, and attacker C cannot accurately analyze the correlation between the addresses of user A and B. Therefore, the connection between input address A and output address B of the transaction is hidden, which provides reliable privacy protection for transaction users without changing any blockchain foundational protocol.

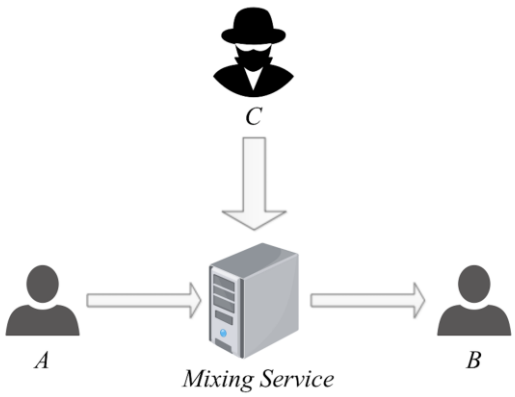

FIGURE 1. The principle of coin mixing mechanism.

The execution of the coin mixing process can be implemented by a trusted third-party or some protocols. According to whether there are trusted third-party nodes in the process of coin mixing, the existing coin mixing mechanisms can be divided into two types: the coin mixing mechanism based on central node and the decentralized coin mixing mechanism [23]. These two mechanisms have their own advantages and disadvantages in terms of efficiency, coin mixing effect, coin mixing cost, etc., and they are need to be improved in all these aspects. Besides, they are still vulnerable to some security issues, such as denial of service (DoS) attack, coin mixing process leak, etc.

1) THE COIN MIXING MECHANISM BASED ON CENTRAL NODE

The coin mixing method based on central node is implemented by the trusted third-party node. In order to blur the input address and output address of the transaction, the trusted

third-party mixes the currency through the corresponding algorithm to achieve the mixing of multiple currencies.

The principle of coin mixing mechanism based on central node is shown in Fig. 2. In order to prevent the potential attacker C from directly discovering the relationship between $A1$ and $B1$, user $A1$ transfers the funds to the third-party node D, and D can transfer to user $B1$ after receiving the funds, finally realizing the transfer of funds between $A1$ and $B1$. In a certain period of time, central node D may have completed the process of multi-user coin mixing, in part hiding the relationship between $A1$ and $B1$, which makes attacker C unable to find the address associated with $A1$ in different receivers $B1$, $B2$ and $B3$. However, through comprehensive analysis of the trading process of $A1$, $B1$ and D over a period of time, the attacker has a certain probability to guess that $B1$ is the real receiver who is corresponding to $A1$. For example, if D has n outputs in a certain amount of time, the probability that attacker C finds the correct transaction link is 1/n. Therefore, the more transactions are added in D, the lower the probability that the original transaction records will be found and the safer the data will be.

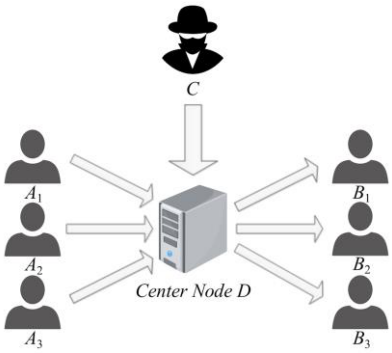

FIGURE 2. The principle of coin mixing mechanism based on center node.

The centralized coin mixing mechanism completely depends on the third-party nodes, it has the following disadvantages while bringing benefits.

(1) Higher fees and transaction delays. The coin mixing service node usually charges a certain amount of coin mixing fee, and with the increase of the number of coin mixing, the fee will rise in a straight line, and the coin mixing time will also increase. Generally, the delay of coin mixing is 48h, and the transaction cost is about $1\% \sim 3\%$.

(2) Third parties may steal money. If there is no appropriate supervision mechanism in the coin mixing service, the third-party node may break the contract after receiving the user's funds, do not perform the agreed operation, steal the user's funds, and the user does not have any effective remedial measures.

(3) Third parties may disclose coin mixing information. Because the third-party nodes master the whole process of coin mixing and user privacy, and understand the real transaction data. It cannot guarantee that the information of coin mixing will not be disclosed.

(4) Denial of Service (DoS) attack. Third-party nodes may reject coin mixing requests for certain addresses.

In view of the mentioned problems, there are many solutions to ensure the credibility of the third-party to provide coin mixing nodes, which will be discussed in the later part.

2) THE DECENTRALIZED COIN MIXING MECHANISM

The decentralized coin mixing mechanism cancels the participation of the third-party coin mixing providers and merges multiple one-to-one transaction records into a many to many transaction record. The attacker cannot directly find the relationship between them. Because the decentralized coin mixing mechanism does not depend on the credibility of the third-party node, it does not need to bear the moral risk of the central manager, which can effectively avoid the third-party theft and leakage of coin mixing information, and users do not need to spend extra fees for the coin mixing service. However, coin mixing users often need to organize their own negotiation and realize the process of coin mixing, thus exposing the following problems:

(1) Because coin mixing users cannot find other coin mixing users effectively, they need to rely on the third-party platform to help perform the process of finding coin mixing users. Therefore, some defects in centralized mixing currency are still inevitable.

(2) Users who participate in the process of mixing coin may expose their coin mixing information in the process of negotiation, which cannot guarantee that all participants are honest and trustworthy.

(3) It is vulnerable to denial of service (DoS) attack. In the process of coin mixing, multiple users need to participate at the same time. Once some users fail to mix coin due to illegal operations, the attacker may take the opportunity to launch a DoS attack.

(4) It is vulnerable to sybil attack. If an attacker has multiple addresses participating in the process of coin mixing, other users' coin mixing information in the process is threatened by leakage.

In view of these defects, there are many improved schemes. In the later part, we will continue to discuss the practical application scheme of decentralized coin mixing mechanism, and then deeply understand the principle and advantages of coin mixing mechanism.

B. ZERO KNOWLEDGE PROOF

Zero knowledge proof was firstly proposed by Goldwasser *et al.* [24] in the early 1980s. In a zero-knowledge proof system, the prover can make the verifier believe that a message is correct without providing any valid information to the verifier. Zero knowledge proof is essentially a protocol involving two or more parties, namely, a series of steps that two or more parties need to take to complete a task.

Zero knowledge proof can be classified into two groups: interactive and non-interactive. In the field of blockchain, the most widely used zero knowledge proof is non-interactive

zero knowledge proof (zk-SNARKs) [25]. Non-interactive means that the proof contains only a single message sent to the verifier from the prover, namely, there is no two-way communication between the prover and the verifier. Zcash, a privacy-protecting digital currency system [26], uses zk-SNARKs technology to completely hide transaction information, including transaction account number and transaction amount.

Zero knowledge proof has three properties:

(1) Completeness. If the argument is true, an honest prover can convince the honest verifier of the fact.

(2) Reliability. If the prover does not know the statement, then he can deceive the verifier only with a negligible probability.

(3) Zero knowledge. After the proof process is completed, the verifier only obtains the message ''the prover has this knowledge'' and cannot obtain any extra content.

By using zero knowledge proof technology, the privacy of blockchain is improved markedly. In addition to the validity of the statement, this verification method will not disclose any other information of the proved message. A large number of facts have proved that zero knowledge proof is very useful in blockchain and cryptography. If zero knowledge proof can be used to verify messages, many problems will be solved effectively.

C. RING SIGNATURE

Ring signature is a digital signature scheme proposed by Rivest *et al.* [27] in 2001. As shown in Fig. 3, a public key construction ring is used to hide the sender information. The output z of one calculation is the input v of the next calculation. After verification, if z and v are equal, it is determined that the signature is correct, that is, a public key in the key group corresponds to the corresponding private key [28].

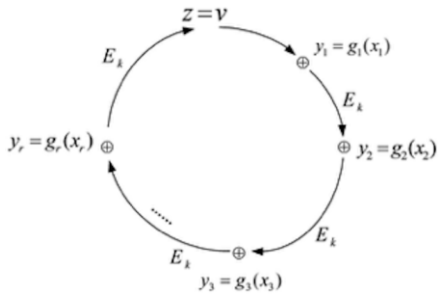

FIGURE 3. The principle of ring signature.

Ring signature is a kind of simplified special group signature [29]. There are only ring members in the ring signature, no trusted third-party and central manager, and no cooperation between ring members. Ring signature allows a ring member to sign other members with its own private key and other members' public key. The verifier cannot judge who is the real signer, but can confirm that the signer must be in the ring, which satisfies the complete anonymity of the signer. For example, based on the massive election of blockchain [30], one-time ring signature ensures the anonymity of voting transactions in blockchain. The unconditional anonymity, correctness and unforgeability of ring signature are very useful for the information that needs to be preserved for a long time in a special environment. While protecting the sender's privacy, ring signature brings difficulties to the supervision because it cannot reveal the signer.

D. HOMOMORPHIC ENCRYPTION

Homomorphic encryption (HE) is a method that allows for computations to be done on encrypted data, without requiring access to a secret (decryption) key. This concept was first proposed by Rivest *et al.* [31] in 1978. Homomorphic encryption is a form of encryption, and its principle is shown in Fig. 4. After plaintext x is encrypted, ciphertext $f(x)$ is obtained. After performing a specific algebraic operation on ciphertext $f(x)$, ciphertext $f(y)$ is obtained. The decryption of the result $f(y)$ is performed to obtain y. After performing the above algebraic operation on plaintext x, the same result y is obtained. That is to say, the operation can be carried out without knowing the original data x, and finally the same correct result y can be obtained.

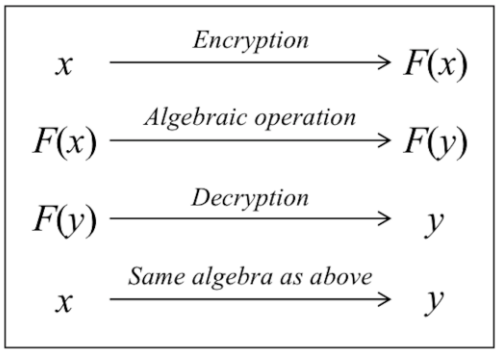

FIGURE 4. Homomorphic encryption.

Homomorphic encryption technology is of great significance in the field of blockchain. In terms of privacy protection, the distributed electronic voting and electronic bidding system [32] use homomorphic encryption technology to improve the anonymity of participants, the privacy of data transmission, and the reliability and verifiability of data. This technology can realize that the receiver can only get the final result, but cannot get every ciphertext message. It can improve the security of information, and does not need to decrypt every ciphertext at a high cost. However, the current homomorphic encryption technology still consumes a lot of computing time and memory in general, which is far from the level of large-scale application. Because of the advantages and disadvantages of homomorphic encryption technology in computing complexity, communication complexity and security, more and more research efforts are devoted to the exploration of its theory and application.

E. HIDDEN ADDRESS

The hidden address [33] is proposed by bitcoin developer Peter Todd and widely used in digital currency. Hidden address is to solve the problem of correlation between input address and output address. Using an address in the blockchain is easy to trace, so multiple addresses need to be used for confusion. In fact, when the sender initiates a transaction, first it uses the public key of the receiver to calculate a temporary intermediate address through the elliptic curve encryption algorithm, then puts the coin on the intermediate address, and finally the receiver finds the transaction according to its own public key, so as to spend. Due to the random uncertainty of this intermediate address, it is impossible to determine which transaction user the intermediate address belongs to, so that other users or attackers on the blockchain cannot determine the addresses of both sides of the transaction, protecting the privacy security of users and the authenticity of coin.

But the hidden address also has some disadvantages. By using transaction graph to analyze the relationship between a transaction from the sending end to the one-time address and then to the receiving end, we can break the privacy of transaction flow. Even using multiple one-time addresses in a transaction cannot avoid this vulnerability. Therefore, we need to further improve and develop the hidden address technology.

F. PEDERSEN COMMITMENT SCHEME

Pedersen commitment scheme [34] is one of the implementations of homomorphic commitment scheme. It supports homomorphic addition operation or multiplication operation of commitment. Similar to BGNO6 encryption scheme [35], it transforms the secrets on the number field group to the elliptic curve group. Before sending it to the receiver, it realizes the perfect hiding of real message through random blinding factor [36] to protect the block transaction privacy of the chain. In the Confidential Transaction (CT) scheme [37], the user signs the commitment when issuing the transaction. But in the RingCT scheme [38], the user only needs to prove whether he has the corresponding commitment key.

Pedersen commitment scheme has the ability of blindness and commitment, which is in line with the feature that the payee can directly confirm the transaction amount through ciphertext in blockchain transactions, without relying on additional amount transmission channel. In order to prevent information leakage and protect users' transaction privacy.

G. SECURE MULTI-PARTY COMPUTATION

Secure Multi-party Computing (SMC) [39] is a classic algorithm in cryptography, which is specially used to solve the cooperative computing problem of protecting privacy when multi entities do not trust each other, such as the famous millionaire problem (MP) [40], [41] and its application and implementation in secure electronic voting [42]. SMC has the characteristics of input privacy, computing correctness and decentralization, which can keep data privacy and be used safely.

SMC is also widely used in the area of blockchain. It plays a unique role in smart contract, key management, random number generation and other technologies. Blockchain focuses on the verifiability of calculation, and does not consider the confidentiality of input data in this process. But SMC is the opposite, emphasizes the confidentiality of the input data in the calculation process and does not ensure that the data is verifiable. Blockchain can improve its ability of data confidentiality by adopting SMC technology to adapt to more application scenarios. SMC can achieve redundant computing with the help of blockchain technology, thus obtaining verifiable characteristics. They complement each other and cooperate to achieve the purpose of privacy protection. Of course, due to the difficulty and low efficiency of secure multi-party computing technology itself, there is a bottleneck in practical application, and the performance improvement of this technology needs to be broken in the future [43].

H. TRUSTED EXECUTION ENVIRONMENT

Trusted Execution Environment (TEE) is a concept proposed by Global Platform (GP) in 2010. It can isolate the environment of software running from hardware, and provide a secure and confidential space for privacy data and sensitive computing in untrusted environment [44].

In blockchain, when it comes to complex cryptography problems such as secure multi-party computing, TEE can provide high-performance solutions that blockchain does not have. For example, IntelSGX [45] is a technology that uses hardware to implement a trusted black box for multi-party computing. In TEE, the use of isolation can protect sensitive data from malware and hackers. Compared with traditional security technology, it can actively defend against external security threats, and guarantee the security and integrity of data more effectively. At present, the development of this technology is mainly restricted by the cost of hardware platform and the difficulty of trusted application development [46].

Table 1 summarizes several classic blockchain privacy protection technologies, such as coin mixing mechanism, zero knowledge proof and ring signature, including the aspects of technical characteristics, anonymity, advantages and disadvantages.

IV. TYPICAL BLOCKCHAIN PRIVACY PROTECTION APPLICATIONS

Every transaction is public in the blockchain, so the attacker can query the transaction amount and transaction address of both sides of the transaction, and can obtain the corresponding information by analyzing the transaction content too. Therefore, the openness and transparency of the blockchain cause serious privacy problems to users. According to the key technologies of blockchain privacy protection introduced in Section III, the section puts forward the corresponding typical privacy protection application scheme from the aspects of

TABLE 1. Comparison of key technologies of blockchain privacy protection.

Name	Technology Features	Anonymity	Advantages	Disadvantages	Typical Application
Centralized coin mixing	Trusted third-party	Weak	Short Mixing time	High handling fee, theft of funds, and denial of service attack	Mixcoin, Blindcoin, Dash
Decentralized coin mixing	Multi-signature transaction	Medium	security, and no transaction fee	Leakage coin mixing information, and sybil attack	CoinShuffle, TumbleBit
Zero knowledge proof	Completeness, reliability, and zero knowledge	Strong	Hide transaction details and resist transaction graph analysis	High cost of computing and storage	Zerocoin, Zerocash
Ring signature	Unconditional anonymity, unforgeability, and correctness	Medium	Internal unlinkability	High cost and poor scalability	CryptoNote, Monero
Homomorphic encryption	Encrypted data can be operated without decryption	Strong	Resist transaction graph analysis	High cost of computing and storage	Confidential transaction (CT), Paillier encryption [47]
Hidden address	One-time middle address	Weak	Recipient anonymity	Sender is not anonymous	CryptoNote, Monero
Pedersen commitment	Preventing message leakage by random blinding factor	Strong	The transaction itself is anonymous	Sender and receiver are not anonymous	Confidential transaction (CT), RingCT, Monero
Secure multi-party computation	Input privacy, calculation correctness, and decentralization	Strong	Confidential input message	Message not verifiable	Millionaire Problem (MP)
Trusted execution environment	Have a trusted and secure independent environment	Strong	Ensure data security and integrity	High hardware cost and difficult development of trusted applications	IntelSGX

such as coin mixing protocol, encryption protocol, secure channel protocol, etc. [48]. Not only maintain the excellent characteristics of blockchain, but also protect the user's privacy.

A. TECHNOLOGY APPLICATION BASED ON COIN MIXING PROTOCOL

In Section 3.1, the advantages and disadvantages of different coin mixing mechanisms were analyzed by studying the principle of coin mixing mechanism, which is conducive to design a better coin mixing mechanism and provide evaluation basis for the selection of coin mixing mechanism in different scenarios. Subsequently, several practical privacy protection applications and the improvement aiming at their advantages and disadvantages are introduced.

1) THE COIN MIXING APPLICATION BASED ON THE CENTRAL NODE

The coin mixing application based on the central node relies on the third-party trusted node to hide the relationship between the input address and the output address of the transaction, so as to confuse the user's transaction relationship in the unrelated addresses and increase the difficulty of analyzing the identity of the attacker. For example, Mixcoin [49], Blindcoin [50], and CoinJoin [51] could realize privacy protection based on the central node.

a: MIXCOIN

Mixcoin [49] is the original centralized coin mixing system of bitcoin, which was proposed by Bonneau *et al.* Mixcoin uses the central mixing server to realize the mixing of transaction addresses and provide mixing services for transaction users to ensure external anonymity. The principle of Mixcoin design is shown in Fig. 5.

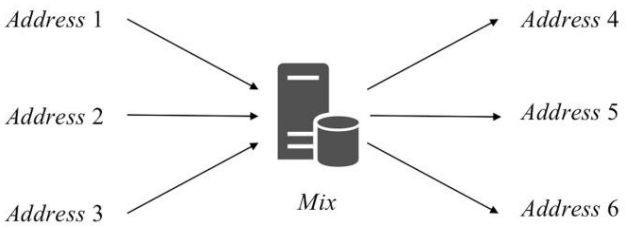

FIGURE 5. The principle of Mixcoin.

By processing the funds using mixing server, the connection between the input address and the output address of the transaction can be hidden, which improves the difficulty of the attacker to analyze the transaction content and ensures the privacy of the user's transaction.

However, this mixing method has considerable limitations. Providing coin mixing services as a third-party, Mixcoin knows the connection information between the user's input address and output address, which has the problem of disclosing the user's privacy. Therefore, in order to improve anonymity, Mixcoin has the following requirements:

a) Multiple users must use the same amount to mix currencies simultaneously. Users are not allowed to choose the number of matching transaction currencies.

b) The mixer must be honest enough to record the user's identity and the input and output information of the coin mixing; on the other hand, the system needs to prevent the mixer from stealing coin.

Aimed at resolving the above problems, Mixcoin added a reputation-based cryptographic accountability mechanism [52], which can expose the theft of mixers and damage the credibility of cheating institutions. However, the accountability mechanism cannot remove the threat of information disclosure from third parties at the root.

b: BLINDCOIN

Valenta and Rowan [50] further optimized the Blindcoin scheme by using blind signature technology [36] and an append only public log on the basis of Mixcoin. In the Blindcoin scheme, the MixCoin protocol is improved by using a blind signature to create an encrypted blind output address for user input and blind tokens. A successful blindcoin blending operation requires two additional transactions to issue and redeem the blind token. The Blindcoin scheme makes the third-party unable to obtain the real information of both parties in all transactions while providing coin mixing services normally, so as to avoid information disclosure and protect users' transaction privacy, thus realizing internal unlinkability.

The cost was the computation of the blind signatures and the extra time in the mixing phase, and the mixing amount of Blindcoin was still fixed. In the Blindcoin scheme, the user must send the output address to the public log anonymously and accept the verification and accountability of the third-party. However, it is still impossible to avoid the cheating of the third-party, which weakens the anonymity of Blindcoin. Blindcoin is likely to be successfully deanonymous.

c: DASH

Shentu and Yu [51] proposed a more efficient blind signature scheme, which uses elliptic curve encryption algorithm to improve the calculation efficiency. The anonymous digital currency Dash, which was launched in 2015, is a digital currency based on bitcoin technology and for the purpose of protecting users' privacy.

In addition to bitcoin, Dash adds a master node based coin mixing strategy, which can hide the flow of funds. In order to prevent the master node from cheating or being attacked, Dash introduced chain mixing [53] and the idea of blinding [54]. Chain mixing refers to that users can choose multiple master nodes randomly and autonomously to mix. Blind technology means that users do not need to send input and output to the transaction pool, but to specify the main node to transfer input and output to another main node. In this way, each master node only sees its own part in the execution process, so it is difficult to find the real identity of the user, avoiding the leakage of the user's privacy information when the central node is attacked.

Secondly, the master node must pay a high amount of deposit as a guarantee, otherwise it cannot get the right to provide coin mixing service. When the third-party node operates in violation of regulations, it must pay corresponding economic loss and reputation loss, so as to avoid the damage of the master node, improve the credibility of the trusted third-party node, and protect the privacy and property security of the coin mixing users.

Finally, in order to improve the anonymity of transactions, users can use multiple primary nodes to mix currencies, reducing the association between addresses. Dash's coin mixing process can effectively reduce the problems of stealing funds and leaking coin mixing process faced by similar coin mixing services. However, there is still a risk that the primary node of Dash is controlled and vulnerable to malicious primary node attacks, so a mixing encryption scheme that does not rely on the central node was proposed.

2) THE DECENTRALIZED COIN MIXING APPLICATION

In view of the high requirements of centralized mixing for mixing nodes, a decentralized mixing application scheme has gradually emerged. The following is a comparative analysis of several existing typical decentralized coin mixing applications.

a: CoinJoin

CoinJoin [55] proposed by Gregory Maxwell on the bitcoin forum is the earliest decentralized coin mixing scheme and the basis of decentralized coin mixing mechanism. However, the CoinJoin service is still difficult to implement without a central server. In general, CoinJoin needs a third-party server to match all the applicants of coin mixing for signature. In the CoinJoin transaction, each user completes the signature independently and dispersedly. Only when all signatures are provided and combined can the transaction be confirmed and accepted by the network.

Compared with Mixcoin, CoinJoin is a kind of distributed mixing service. It can automatically mix coins through a P2P mixing protocol, which is more suitable for the architecture of bitcoin system. The core idea of the scheme is to merge multiple transaction inputs into one transaction, and hide the corresponding relationship between input and output of both parties. As shown in Fig. 6, when there is only one input address and one output address in transaction 1, the attacker can directly observe the relationship between the two parties of the transaction. Under the CoinJoin mechanism, several single input single output transactions are combined into one multiple input multiple output transaction, and the two parties

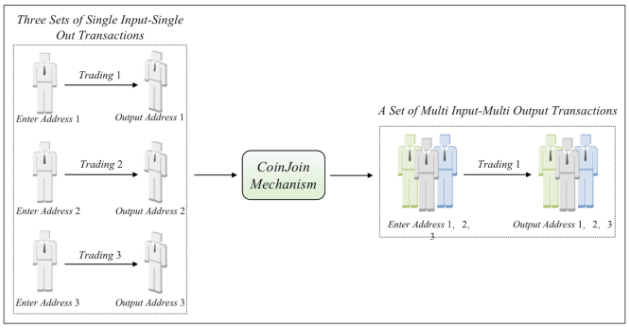

FIGURE 6. Schematic diagram of CoinJoin mechanism.

of the transaction change from two separate addresses to a set of two addresses.

In the view of outsiders, the scheme cannot determine the relevance of input and output through the input and output of transactions, so it provides the external unlinkability, and is not easy to have the problems of mixing costs and fund theft. However, for participants, the multiple input and multiple output transactions formed by CoinJoin scheme are all recorded in the global ledger, and users cannot deny that they have participated in the coin mixing, so the scheme does not provide internal unlinkability. Its anonymity also depends on the number of mixing participants and is vulnerable to DoS and sybil attacks. In addition, CoinJoin also has an important defect, that is, the coin mixing service cannot encrypt the amount of money involved in the coin mixing, and requires that each input amount is equal.

b: CoinShuffle

In view of the defects of CoinJoin scheme, there are many improved methods. Ruffing *et al.* [56] proposed a completely decentralized bitcoin mixing protocol, named CoinShuffle. On the basis of CoinJoin, CoinShuffle users use the key of other users in the coin mixing service to encrypt the output address, all participants shuffle the output address in order, and broadcast the output address list finally. Even the coin mixing participants cannot speculate the relationship between the transaction input and output address.

Compared with CoinJoin, the biggest technological innovation of CoinShuffle is the introduction of the picketing mechanism, which can find and eliminate malicious nodes every time the mixing fails. For example, theft will be found in the first time. An attacker cannot steal or destroy the coin of an honest user, and the user can also avoid malicious nodes for the next round of operations.

The decentralized scheme of CoinShuffle completely realizes the internal unlinkability, which can prevent users from stealing mixing funds. However, the scheme requires all participants to be online at the same time when implementing the coin mixing process, which is vulnerable to DoS attacks. The more participants, the greater the communication cost needed, which may face the problem that there are not enough users to participate in. CoinShuffle's anonymity is related to the size of anonymity set, which is low in anonymity, and it is also vulnerable to cross attacks [57] and sybil attacks.

c: XIM

Bissias *et al.* [58] designed a decentralized coin mixing protocol Xim that could anonymously discover participants of mixed currency mixed currency using the advertising information in the blockchain. Xim uses a multi-round two-party coin mixing protocol, and it has a controllable success rate. A Xim coin mixing can be divided into two steps: first, match other coin mixing users. You can anonymously find a mixing partner according to the advertisements placed on the blockchain. Fair Exchange is adopted as the exchange protocol to make the mixing process more flexible. Secondly, the two sides carry out the transaction of coin mixing amount, usually need to divide the capital of an address into many parts, then carry out multiple rounds of coin mixing at the same time, finally achieve the purpose of coin mixing.

Compared with other decentralized coin mixing application schemes, the cost of attack by malicious nodes in Xim scheme will increase linearly with the number of users participating in coin mixing and the number of times of coin mixing by a single user, and remain unchanged for honest participants. Xim does not change the block size of the blockchain during the coin mixing process and has no other special requirements. Besides, it can effectively resist Sybil attacks, inference attacks and other Dos attacks by charging transaction fees, and its privacy and security are better. There are also some problems in Xim. Compared with other schemes, coin mixing for a long time and coin mixing too many times and so on.

d: CoinParty

In 2015, Ziegeldorf *et al.* [59] proposed CoinParty protocol on CoinShuffle. CoinParty is a distributed coin mixing technology based on a combination of decryption mixnets with threshold signatures. By using of secure multi-party computing protocol [60], it simulates trusted third-party to realize safe and anonymous coin mixing among users. CoinParty can provide a single transaction of coin mixing, and allows the process of coin mixing to be still effective in the case of malicious operation or failure of some nodes involved in coin mixing, which increases the anonymity and security of users. Because the CoinParty protocol does not depend on the credibility of the third-party nodes, there is no mixing cost caused by the centralized coin mixing scheme, which improves the robustness and scalability of the protocol. Its defect is that it is easy to be attacked by DoS and needs more mixing time.

The coin mixing technology is easy to operate, widely applicable, so it is widely used in the blockchain digital currency, and there are many improved schemes. We make a comparative analysis on whether it depends on the third-party, whether it needs the coin mixing fee and their advantages

TABLE 2. Typical application comparison of coin mixing technology.

Technology Application	Need Third-Party	Technology Features	Advantages	Disadvantages	Coin Mixing Charges	Theft Risk	Denial of Service
Mixcoin	Yes	Use of accountability system	Unlinkability	Cannot customize mixing amount, high time cost	Yes	High	Low
Blindcoin	Yes	Using blind signature technology	Low risk of currency mixing process leakage	Cannot customize mixing amount, high calculation cost	Yes	High	Low
Dash	Yes	Using chain mixing and blinding techniques	Punishment mechanism to ensure anonymity	Depending on the master node, additional deposit is required, and the risk of coin mixing process leakage is high	Yes	Medium	Low
CoinJoin	No	Multisignature transaction	External unlinkability, high efficiency	Cannot customize mixing amount, vulnerable to DoS attack and sybil attack	No	Low	High
CoinShuffle	No	Using shuffle and picket mechanisms	Internal unlinkability	Need participants to be online at the same time, low efficiency	No	Low	High
Xim	No	Using a multi round and two-party coin mixing protocol	Internal unlinkability, resist multiple attacks	Long mixing time	Yes	Low	Low
CoinParty	No	Coin mixing network based on threshold signature and decryption	Robustness, scalability	Long mixing time	No	Low	Low

TYPICAL APPLICATION COMPARISON OF COIN MIXING TECHNOLOGY.

and disadvantages. As shown in Table 2, in the coin mixing protocols, most of the existing schemes mainly relies on the untrusted third-party platform to mix the transaction sets of multiple users and then output them to the corresponding address, so that the attacker cannot link the input and output addresses of the transaction, and the mixing service can greatly increase the difficulty for the attacker to obtain user privacy. However, with the development of data analysis algorithms, attackers can analyze the transaction anonymity set of the coin mixing protocol to associate the transaction address. Furthermore, untrusted third-party platforms may leak transaction information or refuse services. And all mixing schemes can't solve a problem: you can't customize the mixing amount, and all users participating in the mixing must conduct transactions of the same amount, which is caused by the blockchain's open transaction amount. Besides, the mixing scheme has the problem of overhead, and the system needs to consume more computer resources and communication resources to realize the mixing. Therefore, we need to study the encryption technology to ensure the security and anonymity of the coin mixing protocol, and the incentive mechanism to ensure the normal processing of transactions by the third-party platform, so as to achieve the privacy security of users.

B. TECHNOLOGY APPLICATION BASED ON ENCRYPTION PROTOCOL

Blockchain is currently mainly used for digital currency. In the process of asset transfer, user privacy is a very important issue. Bitcoin is the first application of blockchain technology in the field of digital currency, which has obvious defects in privacy protection. In view of the limitations of the mixing scheme, scholars have gradually shifted their research on the anonymity of digital currency from mixing to the introduction of other cryptography technologies, thus proposing different decentralized digital currencies, among which Monero [61], Zerocoin [62], Zerocash [26] are three of the most typical.

1) MONERO

Monero [61] is a new type of digital currency with privacy protection as its main feature. It uses ring signature [27] and hidden address [33] to hide the association between input and output addresses. CryptoNote [63], RingCT [38] and other

cryptography technologies are used to ensure the anonymity and privacy of users.

In Monero, users can mix a series of transactions with the same amount, using ring signature technology. In the process of mixing, no signature of other participants is needed, thus hiding their real identity in multiple outputs of the transaction. In this way, the external attacker cannot establish the association between addresses and achieve the unlinkability of transaction input and output [64].

Ring signature technology can protect the unlinkability of a single transaction, but it is not able to protect the relationship of multiple addresses and the association between multiple transactions. To solve this problem, Monroe proposed a solution of one-time random address. The sender of the transaction uses the public key of the receiver and the random parameters generated by the sender to encrypt and get a one-time random address. Because the random number is only controlled by the sender, no one else can find the relationship between the random address and the receiver. The random number also ensures that the output address of each transaction is different, and there is no correlation between them.

In Monero, ring signature is used in combination with hidden address, which is a one-time address and not related to any user. Transaction data and key profile are hidden to prevent double-spending attack [65]. However, the introduction of ring signature in CryptoNote will have a negative impact on scalability [66].

While Monero is able to make anonymous transactions and hide transaction amounts, there are still some problems: Monero have a ''key mirror'' mechanism (which records all the keys that have been used), and everyone can verify that the transaction is valid. On the side, Monero also uses other encryption technology to protect the amount of transactions, recipient information, and so on. Add some invalid addresses to every transaction to increase consumption of CPU time and memory.

In the ring signature, it needs mix the sender's private key with other users' public keys, which will hide the real transaction in the anonymous set. There may be malicious users who expose their privacy, so that the user's transaction address is associated, and when the user selects the anonymous set, the anonymous set is generally small. The attacker can connect the transaction information with the user's identity by analyzing the transaction information [67], [68]. Therefore, the concept of Zerocoin was put forward.

2) ZEROCOIN

Zerocoin is an encryption protocol based on zero knowledge proof [24] proposed by Miers and other scholars of Hopkins University [62], which can provide internal unlinkability and prevent user transaction address being exposed. Zerocoin is an extension protocol of bitcoin. Users can make transactions by casting bitcoin into Zerocoin, hide the transaction address of users, and can redeem Zerocoin into bitcoin. When using a Zerocoin transaction, user only knows whether the Zerocoin has been spent, but cannot get the other information of the transaction. However, zerocoin cannot be implemented in the original bitcoin system, so it needs bitcoin system to carry out soft forking.

Although Zerocoin can effectively protect the anonymity and privacy of users, it also has some limitations:

a) Zerocoin cannot realize any split and combination of amount, only can cast and exchange coin with fixed value, so it often needs to calculate many complex proofs.

b) Zerocoin cannot hide the transaction amount and the receiver's address. If the transaction amount is unique, other users can associate the Zerocoin with the original coin, thus destroying the user's unlinkability again.

c) Zerocoin does not support non-interactive transactions and the data used in zero knowledge proof is relatively large, the process is too tedious, and the efficiency of the generation process is too low. It needs to consume additional blockchain storage space and computing resources, which seriously affects the efficiency of digital currency.

For this reason, many new schemes have been proposed, and the Zerocash scheme proposed by Sasson *et al.* [26] is the most typical scheme.

3) ZEROCASH

Literature [26] proposed Zerocash on the basis of Zerocoin, which improved the encryption technology to a higher level and realized the highest degree of privacy and anonymity of current ''digital currency'' transactions.

Compared with Zerocoin, the Zerocash is completely independent with bitcoin, and is same as bitcoin in many aspects. They are all based on the ledger structure, and use proof-of-work mechanism to generate blocks, and the total amount of coins is 21 million. The difference is that Zerocash pays more attention to the privacy protection of users. The function of Zerocash is realized through two kinds of transactions: mint transaction and pour transaction. Same as bitcoin, Zerocash also uses blockchain as a decentralized transaction ledger, and the generated transactions will be broadcast and attached to the blockchain.

Different from other encrypted digital currencies, which will disclose all transaction records, Zerocash uses zk-SNARK [25] to protect transaction amount, sender's and receiver's addresses, supports any number of transaction amounts, and realizes full anonymity. zk-SNARK requires the sender to produce a zero knowledge proof that it has the ability to spend more than or equal to the transaction value. In addition to its simplicity, zk-SNARK has very good data-integrity and reliability. Its zero knowledge proof is polynomial time.

At present, although Zerocash obtains high anonymity and protects transaction privacy, but it requires expensive computing resources. Moreover, the scalability of Zerocoin and Zerocash is weak, and they have no smart contract function. The most important thing is that the process of using zk-SNARK algorithm to generate the proof is very slow. A common transaction may only take a few seconds, while the secret transaction of zk-SNARK takes 1 to 2 minutes. There is a

TABLE 3. Typical comparison of digital cryptocurrencies.

Encrypted Currency	Technology Features	Advantage	Disadvantages	Extensibility
Monero	Based on CrytoNote and RingCT cryptography protocol, anonymity is realized by ring signature and hidden address	Unlinkable, users can mix currencies by themselves	Depending on other public keys, extra computation storage	Weak
Zerocoin	Zero knowledge proof cryptography technology	Internal unlinkability, against theft, DoS attack	Can't realize any split and combination of amount, can't hide transaction amount and receiver address, data takes up a large amount of memory and takes a long time to verify	Weak
Zerocash	Simple non-interactive zero knowledge proof technology	Hide all transaction information, with the strongest anonymity	Anonymous transactions take a long time	Weak

bottleneck in the efficiency. Such a speed is absolutely not suitable for high-throughput transaction applications. Zcash is also making continuous improvements to address this problem, and some new schemes have been developed so far.

Table 3 analyzes the technical characteristics, advantages and disadvantages of the existing cryptocurrencies.

The mentioned new digital currency generally combines block chain structure and cryptography technology to solve the problem of anonymity. Compared with bitcoin, it can better protect the identity privacy and transaction privacy of users. In the encryption protocol, the existing technology mainly uses ring signature, zero knowledge proof and other cryptography technology to protect the privacy of users. However, since the mentioned schemes are all based on the bitcoin system, with the improvement of security, the efficiency of the system will inevitably be affected. In the future, we need to continue to study and improve the computing performance and storage performance of the schemes based on cryptography, and design encryption schemes with higher efficiency, better performance and stronger privacy.

C. TECHNOLOGY APPLICATION BASED ON SECURE CHANNEL PROTOCOL

As the number of transactions increases, blockchain applications will be delayed. Therefore, some schemes to fulfil off-chain transactions relying on third parties are proposed, which are also known as secure channel protocols [69]. Under the technical framework of secure channel protocol, Two-Way Micropayment Channel [70], Lightning Network [71], Sprites [72], Bolt [73], TumbleBit [74] and other technologies are committed to solving the privacy security problem when there is a third-party.

1) TWO-WAY MICROPAYMENT CHANNEL, LIGHTNING NETWORK, SPRITES AND OTHER OFF-CHAIN PAYMENT TECHNOLOGIES

The transaction of blockchain system needs to be verified by miners, and the whole network nodes reach consensus through consensus mechanism. Therefore, the number of transactions processed by the system per second is limited. In order to solve the scalability problem of blockchain system, a variety of security channel protocols are proposed [75]. Including Two-Way Micropayment Channel [70], Lightning Network [71], Sprites [72] and other chain payment technologies. Through the use of security channel, users only need to broadcast the first transaction amount and the last transaction amount to the blockchain, but will not make public the number of transactions between them. The details of transactions between users are executed in off-chain way. This fuzzy feature is conducive to ensuring that Privacy security of transaction information.

However, when there is no direct payment channel between the two parties, the relay nodes are allowed to complete the transaction as service providers. The relay node can obtain the transaction address and transaction amount of both parties, which puts the privacy of users at risk. In order to solve this problem, the current Lightning Network contains Sphinx [72] protocol which anonymously relays information on P2P network to hide all routing data from intermediate nodes.

2) BLOT

Blot is an anonymous payment channel technology proposed by Green *et al.* for the privacy protection of off-chain secure channel transaction technology [73]. Blot provides three off-chain payment schemes: one-way payment channel, two-way payment channel and third-party payment channel. Transactions between users can be conducted directly through the off-chain secure channel or rely on the untrusted third-party.

Bolt solution solves the problem of privacy protection in the context of micro payment channel by removing the contact of transactions in the payment channel. Bolt uses blind signature technology and zero knowledge proof to ensure that multiple payments under the same channel cannot be linked together, even between the individuals who conspire. And the payment occurs in milliseconds, without block confirmation. The receiver only needs to know that someone has made

TABLE 4. Comparison of typical secure channel technology applications.

Technology Application	Technology Features	Advantage	Disadvantages
Bi-directional Payment	Fast trading through off-chain trading channel	Transaction content is only visible to both parties, reducing verification time	Publish the user's last transaction status
Lightning Network	Fast trading through off-chain trading channel	Transaction content is only visible to both parties, reducing verification time	Release the final transaction status by relying on the third-party platform
Sprites	Fast transaction processing	Supporting partial withdrawals and deposits	Transactions can be linked
Blot	Using blind signature technology and zero knowledge proof technology	The transaction content is encrypted and cannot be linked	The third-party may obtain the transaction content, and the decentralization problem needs to be improved
TumbleBit	Fast anonymous off-chain channel transaction technology through RSA and ECDSA cryptography	The third-party verifies the authenticity of the transaction without knowing the transaction information, and cannot link the payment channel	The third-party may obtain the transaction content, at least two transactions are required

payment in the payment channel provided by him. Payment can also be arranged by a third-party to avoid the complexity of the transaction parties' switching on and off payment channels, which makes the third-party unable to obtain the user's transaction information, so as to prevent the third-party from doing evil. In the meantime, the transaction funds are also confidential to ensure the user's privacy. However, currently Bolt can only support single hop mediation network, and its decentralization problem also needs to be improved.

3) TumbleBit

For the privacy protection of the off-chain payment protocol, there have been some research achievement. Heilman *et al.* [76] proposed an off-chain anonymous payment scheme to enable users to realize anonymous transactions through a third-party, but the scheme assumes that the third-party is honest and trustworthy. Later, Heilman and Baldimtsi improved this scheme, and proposed a decentralized and untrusted off-chain channel mixing technology——TumbleBit [74].

TumbleBit scheme allows all parties to establish a payment channel for both parties through Tumber, an untrusted third-party platform, and to fulfil anonymous off-chain payment fastly using RSA and ECDSA cryptography technology. However, the payment channel information is hidden from the relay node Tumber, which can verify the authenticity of the user's transaction, but can't obtain the user's transaction information and don't know the identity of both parties. It realizes the unlinkability of user transactions to ensure user privacy. TumbleBit does not need block confirmation, which saves transaction time and keeps transaction funds confidential, so that multiple transactions under the same payment channel cannot be linked together. Furthermore, the TumbleBit scheme is fully compatible with bitcoin system, and does not need modify bitcoin protocol.

Nonetheless, TumbleBit like the previous secure channel protocols, allows relay nodes to complete transactions as service providers when there is no direct payment channel between the two parties. The relay node can obtain the transaction information of both sides of the transaction, which makes the user's privacy threatened.

Table 4 analyzes the technical characteristics, advantages and disadvantages of several existing off-chain secure channel trading applications.

In the existing off-chain secure channel protocols, anonymous communication between users is accomplish by untrusted third-party, and users without direct channel can also perform the transaction. For example, a personal data management platform [77] is built by combining blockchain and off-chain storage to ensure that users own and control their personal data. However, there are still many problems in the safety and reliability of the existing technologies. If there are errors in the transaction, it is necessary to disclose the transaction information of users to the whole network for verification. However, how to ensure the fairness of the transaction without disclosing users' privacy needs to be further improved.

D. TECHNOLOGY APPLICATION BASED ON RESTRICTED PUBLISH

Restricted publishing scheme is making public data selectively, which directly removes the data involving privacy from the public database. Compared with coin mixing mechanism and encryption mechanism, it can fundamentally guarantee the privacy of data. However, this method has many limitations on application scenarios, and requires a lot of modification and revision of blockchain protocol. Nowadays, there are two common schemes: Lightning Network [71], consortium blockchain and private blockchain [78].

1) LIGHTNING NETWORK

Lightning Network [71] is a micropayment technology in bitcoin, in which most transactions between users are stored off-chain, only the first and last transactions need to be recorded on the blockchain ledger, which reduces the storage load on the chain, consequently reduces the transaction cost of bitcoin significantly, and meets the requirements of small and fast payment. So it can effectively protect transaction privacy.

2) CONSORTIUM BLOCKCHAIN AND PRIVATE BLOCKCHAIN

Most of the traditional blockchain applications, such as bitcoin, ethereum and so on, are based on the public chain. Public blockchain is a highly decentralized distributed ledger, which makes it convenient for any node to access the blockchain network freely, but it also brings potential privacy threats. In order to prevent information leakage and attack, the public blockchain is gradually extended to the consortium chain and the private blockchain. Consortium blockchain means the blockchain is managed by multiple industry organizations. Only members of the consortium can read and write and send data, while other unauthorized nodes cannot access the blockchain data. Private blockchain is a non-public ''chain'' that is suitable for the application within the enterprise. Only authorized users can access the blockchain data. These two new chains close the access to data of unauthorized nodes fundamentally, and reduce the risk of blockchain privacy disclosure significantly.

E. TECHNOLOGY SCHEME BASED ON CASE APPLICATION

All of the above proposals are for privacy protection of the identity and transaction amount of both parties. Blockchain also proposes some privacy protection schemes in other fields, such as Hawk framework based on smart contract [79], Quorun based on Ethereum [80], IntelSGX based on Trusted Execution Environment (TEE) [45].

1) HAWK

Kosba *et al.* [79] proposed a smart contract framework to protect users' privacy: Hawk. Unlike Zerocash, which uses zero knowledge proof for coin transactions, hawk cleverly combines zero knowledge proof [24] and multi-party computing [39] or TEE [44] to protect the privacy of blockchain contract content.

Generally, the blockchain smart contract is open and transparent, but Hawk divides the smart contract into public and private parts [81]. Public contracts store public information, private contracts store private data, transaction amount and other information. These operations achieve the data privacy on the chain and ensure that the private data is hidden out of the public view.

In addition, Hawk also guarantees the fairness of the contract participants, and any participant who terminates the agreement maliciously will be subject to financial penalty. However, it is worth noting that Hawk can only guarantee the privacy of the input code in the contract, but not the privacy of the code itself. In fact, the contract code will also disclose user information. In the blockchain smart contract, although Hawk protects the user's privacy, its scalability is not very strong, and it is not completely decentralized.

2) QUORUM

Quorum is an enterprise level blockchain platform launched by J.P. Morgan (a financial institution in the United States). Starting from the actual operation of the financial system, Quorum is a consortium blockchain system based on Ethereum, and is different from the previous consideration of privacy from the perspective of public chain.

Ethereum is the underlying protocol for Quorun, where the code and logic are almost completely inherited (which reduces the probability of bugs) and provides additional services. Quorun added a privacy field to the smart contract and changed ethereum's consensus mechanism from PoW to Raft or smart contract voting, so it was more efficient. The introduction of Privatefor syntax allows users to specify the visible side of an encrypted transaction, thus enabling a flexible and clear privacy policy [80]. Quorun also added permission functions to the previously unrestricted P2P transmission mode, such as read and write permissions, user sending messages, miner node processing data, etc., so that P2P messages can only be transmitted between mutually allowed nodes.

Quorum is similar to Hawk in some aspects. It divides the transaction data into two parts: public and private. The difference is that Quorum does not rely on zero knowledge proof or secure computing to protect user privacy. By default, each node in Quorum is honest, and public and private data will be recorded on multiple nodes in the form of encryption and supervised, which can be traced back to responsibility afterwards. Therefore, quorum is more practical to solve the privacy problem in the blockchain, and its scope of application is relatively limited.

3) IntelSGX

In 2013, Intel Corporation, the world's largest CPU manufacturer, launched a new security technology SGX [45] when it released Skylake processor. SGX is a specific implementation of trusted execution environment (TEE). TEE provides a completely isolated environment to prevent other applications, operating systems, and host owners from querying or even compiling application content. So that malware cannot access these data, but also prevent some forms of hardware attacks. We call the memory space corresponding to the tee environment protected by SGX as Enclave [82]. Therefore, the operation of isolation in SGX can be regarded as an ideal model to ensure the privacy and integrity of users' key code and data.

SGX, as an important research in the field of security, can not only enhance the security of the system, but also solve the problem of data privacy protection in the blockchain after it is combined with the blockchain technology,

without affecting the decentralization and tamper-proof properties of the blockchain. It not only preserves the advantages of blockchain, but also improves the disadvantages of blockchain technology. At present, SGX technology has been widely used in the implementation of data privacy protection in distributed systems [83].

V. SUMMARY AND PROSPECT

With the rapid development of blockchain technology and its extensive applying in various fields such as finance [84], cloud computing [85], big data [86], IoT [3], [4], privacy protection has been severely challenged. However, bitcoin, Ethereum and other fully open ledgers have been unable to meet people's perfect demand for privacy protection in application scenarios. For this reason, researchers need to devote themselves to study and constantly improve the privacy protection of blockchain.

Based on the latest research results, this paper focuses on the key technologies and typical applications of privacy protection in blockchain. Among them, the eight privacy protection key technologies proposed in this paper have made a detailed comparison and analysis of blockchain privacy protection from the aspects of technical characteristics and anonymity. It is concluded that the centralized coin mixing mechanism and the hidden address have the weakest privacy protection for users, followed by the decentralized coin mixing mechanism and ring signature. The remaining four privacy protection technologies have stronger anonymity in the blockchain field than before, and are also the key technologies that have been studied and applied most. They are applied to various digital currency and other application scenarios, such as Zerocoin, Zerocash, Hawk, and IntelSGX. One common feature of them is decentralization, which avoids the attack of the third-party malicious nodes and achieves anti-transaction graph analysis. Therefore, blockchain privacy protection must be put in an important position to enhance the system's anti-attack in the future.

Nowadays, there have been a lot of achievement of blockchain security and privacy protection, but the known blockchain privacy protection technologies are not perfect, there are still many problems to be discussed and improved, hoping to design a more secure and efficient privacy protection scheme. Among them, the most representative is to provide privacy protection and trust mechanism by combining blockchain and trusted computing technology [87]. For example, VANETs based on blockchain [88] can establish distributed trust management mechanism while protecting vehicle privacy. This field has become a new research direction in the future. Although, the existing applications of digital currency have been more mature, such as bitcoin, Monroe, Zerocoin and so on. But the research of blockchain in other fields is just beginning. As a new network technology, blockchain still needs to be studied by researchers to provide technical foundation for further development of blockchain.

Finally, privacy protection should not be the protection technology of lawbreakers, especially the emerging digital currency similar to bitcoin, which is more severe in the face of privacy protection and regulatory issues [89]. Therefore, it is necessary to introduce appropriate supervision mechanism or audit mechanism in the blockchain to realize the functions of governance and error correction in the process of blockchain transaction, so as to reduce the possibility of criminals using the blockchain platform. How to supervise the illegal and criminal behaviors in the blockchain under the condition of providing privacy protection has become the development direction of the government and financial institutions in the next stage.

REFERENCES

[1] U. Rajput, F. Abbas, R. Hussain, H. Eun, and H. Oh, "A simple yet efficient approach to combat transaction malleability in bitcoin," in *Proc. Int. Workshop Inf. Secur. Appl.* Cham, Switzerland: Springer, 2015, pp. 27–37.

[2] J. Zhu, "Blockchain: The cornerstone of digital finance," (in Chinese), *Informatization Construct.*, no. 7, pp. 1–56, 2019.

[3] P. Fremantle, B. Aziz, and T. Kirkham, "Enhancing IoT security and privacy with distributed Ledgers—A position paper," in *Proc. 2nd Int. Conf. Internet Things, Big Data Secur.*, Apr. 2017, pp. 344–349.

[4] M. S. Ali, K. Dolui, and F. Antonelli, "IoT data privacy via blockchains and IPFS," in *Proc. 7th Int. Conf. Internet Things (IoT)*. New York, NY, USA: Association for Computing Machinery, 2017, pp. 1–7.

[5] J. Xu, S. Wang, B. K. Bhargava, and F. Yang, "A blockchain-enabled trustless crowd-intelligence ecosystem on mobile edge computing," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3538–3547, Jun. 2019, doi: 10.1109/TII.2019.2896965.

[6] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and open research challenges," *IEEE Access*, vol. 7, pp. 10127–10149, 2019.

[7] X. He, J. Yi, and A. Chen, "Application progress and development trend of block chain technology," *World Sci.-Tech. RD*, vol. 40, no. 6, pp. 615–626, Aug. 2018, doi: 10.16507/j.issn.1006-6055.2018.12.007.

[8] A.-D. Liu, X.-H. Du, N. Wang, and S.-Z. Li, "Research progress of blockchain technology and its application in information security," *Ruan Jian Xue Bao/J. Softw.*, vol. 29, no. 7, pp. 2092–2115, Apr. 2018, doi: 10.13328/j.cnki.jos.005589.

[9] Y. Wang, Z. Cai, G. Yin, Y. Gao, X. Tong, and G. Wu, "An incentive mechanism with privacy protection in mobile crowdsourcing systems," *Comput. Netw.*, vol. 102, pp. 157–171, Jun. 2016, doi: 10.1016/j.comnet.2016.03.016.

[10] Y. Wang, Z. Cai, X. Tong, Y. Gao, and G. Yin, "Truthful incentive mechanism with location privacy-preserving for mobile crowdsourcing systems," *Comput. Netw.*, vol. 135, pp. 32–43, Apr. 2018, doi: 10.1016/j.comnet.2018.02.008.

[11] X. Zheng, Z. Cai, and Y. Li, "Data linkage in smart Internet of Things systems: A consideration from a privacy perspective," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 55–61, Sep. 2018, doi: 10.1109/MCOM.2018.1701245.

[12] Z. Cai and X. Zheng, "A private and efficient mechanism for data uploading in smart cyber-physical systems," *IEEE Trans. Netw. Sci. Eng.*, early access, Apr. 24, 2018, doi: 10.1109/TNSE.2018.2830307.

[13] Y. Deng, X. Chen, Z. Wang, and D. Wang, "Blockchain-based privacy security protection feasibility analysis," (in Chinese), *Softw. Guide*, vol. 18, no. 1, pp. 166–168, Jun. 2019, doi: 10.11907/rjdk.181917.

[14] W. A. Amiri, M. Baza, K. Banawan, M. Mohamed, W. Alasmary, and K. Akkaya, "Privacy-preserving smart parking system using blockchain and private information retrieval," Apr. 2019, *arXiv:1904.09703*. [Online]. Available: https://arxiv.org/pdf/1904.09703.pdf

[15] S. Bartolucci, P. Bernat, and D. Joseph, "SHARVOT: Secret SHARe-based VOTing on the blockchain," in *Proc. 1st Int. Workshop Emerg. Trends Softw. Eng. Blockchain (WETSEB)*, Gothenburg, Sweden, Mar. 2018, pp. 30–34, doi: 10.1145/3194113.3194118.

[16] N. Faour, "Transparent voting platform based on permissioned blockchain," M.S. thesis, Dept. Soft. Eng., Nat. Res. Univ., Moscow, Russia, 2018.

[17] X. Han, Y. Yuan, and F. Wang, "Security problems on blockchain: The state of the art and future trends," *Acta Automat. Sinica*, vol. 45, no. 1, pp. 206–225, Jan. 2019, doi: 10.16383/j.aas.c180710.
[18] L. Zhu, F. Gao, M. Shen, Y. Li, B. Zheng, H. Mao, and Z. Wu, "Survey on privacy preserving techniques for blockchain technology," *J. Comput. Res. Develop.*, vol. 54, no. 10, pp. 2170–2186, Jun. 2017, doi: 10.7544/issn1000-1239.2017.20170471.
[19] D. Ron and A. Shamir, "Quantitative analysis of the full bitcoin transaction graph," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, vol. 7859, Nov. 2013, pp. 6–24, doi: 10.1007/978-3-642-39884-1_2.
[20] M. Fleder, M. S. Kester, and S. Pillai, "Bitcoin transaction graph analysis," Feb. 2015, *arXiv:1502.01657*. [Online]. Available: https://arxiv.org/abs/1502.01657
[21] Z. Liu, D. Wang, and B. Wang, "Privacy preserving technology in blockchain," *Comput. Eng. Des.*, vol. 40, no. 6, pp. 1567–1573, Jun. 2019, doi: 10.16208/j.issn1000-7024.2019.06.012.
[22] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Commun. ACM*, vol. 24, no. 2, pp. 84–90, Feb. 1981, doi: 10.1145/358549.358563.
[23] X. Li, Y. Niu, L. Wei, C. Zhang, and N. Yu, "Overview on privacy protection in bitcoin," *J. Cryptol. Res.*, vol. 6, no. 2, pp. 133–149, Apr. 2019, doi: 10.13868/j.cnki.jcr.000290.
[24] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems," *SIAM J. Comput.*, vol. 18, no. 1, pp. 186–208, Feb. 1989, doi: 10.1137./ 0218012.
[25] S. Hu, C. Cai, Q. Wang, C. Wang, X. Luo, and K. Ren, "Searching an encrypted cloud meets blockchain: A decentralized, reliable and fair realization," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Honolulu, HI, USA, Apr. 2018, pp. 792–800, doi: 10.1109/INFOCOM.2018.8485890.
[26] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in *Proc. IEEE Symp. Secur. Privacy*, San Jose, CA, USA, May 2014, pp. 459–474, doi: 10.1109/SP.2014.36.
[27] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Proc. 7th Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, 2001, pp. 552–565.
[28] G. Dong, Y. Chen, J. Fan, Y. Hao, and F. Li, "Research on privacy protection strategies in blockchain application," *Comput. Sci.*, vol. 46, no. 5, pp. 29–35, May 2019, doi: 10.11896/j.issn.1002-137X.2019.05.004.
[29] D. Chaum and V. H. Eugène, "Group signatures," in *Advances in Cryptology*. Berlin, Germany: Springer, 1991, pp. 257–265.
[30] B. Wang, J. Sun, Y. He, D. Pang, and N. Lu, "Large-scale election based on blockchain," *Procedia Comput. Sci.*, vol. 129, pp. 234–237, Mar. 2018, doi: 10.1016/j.procs.2018.03.063.
[31] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms," *Found. Secure Comput.*, vol. 4, no. 11, pp. 169–180, Jan. 1978.
[32] R. Tso, Z.-Y. Liu, and J.-H. Hsiao, "Distributed E-voting and E-bidding systems based on smart contract," *Electronics*, vol. 8, no. 4, p. 422, Apr. 2019, doi: 10.3390/electronics8040422.
[33] P. Todd. *Stealth Addresses*. Accessed: Jan. 6, 2014. [Online]. Available: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2014-January/004020.htm
[34] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Proc. 11th Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 1991, pp. 129–140.
[35] Z. Wang, J. Liu, Z. Zhang, and H. Yu, "Full anonymous blockchain based on aggregate signature and confidential transaction," *J. Comput. Res. Develop.*, vol. 55, no. 10, pp. 2185–2198, Oct. 2018, doi: 10.7544/issn1000-1239.2018.20180430.
[36] D. Chaum, "Blind signatures for untraceable payments," in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 1982, pp. 199–203.
[37] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *J. Netw. Comput. Appl.*, vol. 126, pp. 45–58, Jan. 2019, doi: 10.1016/j.jnca.2018.doi:.10.020.
[38] S. Noether and A. Mackenzie, "Ring confidential transactions," *Ledger*, vol. 1, pp. 1–18, Dec. 2016, doi: 10.5195/LEDGER.2016.34.
[39] T. Wang, "A review of the study of secure multi-party computation," *Cyberspace Secur.*, vol. 5, no. 5, pp. 41–44, May 2014.
[40] J. Zhang, Z. He, B. Ge, Y. Tang, and Q. Ye, "An efficient millionaire problem protocol and application," *Comput. Eng.*, vol. 126, pp. 1–13, Mar. 2020, doi: 10.19678/j.issn.1000-3428.0057131.
[41] A. C. Yao, "Protocols for secure computations," in *Proc. 23rd Annu. Symp. Found. Comput. Sci. (SFCS)*, Chicago, IL, USA, Nov. 1982, pp. 160–164.
[42] J. Yu, "Secure multiparty compution and Private electronic voting system," M.S. thesis, Dept. Soft. Eng., Jilin Univ., Jilin, China, 2016.
[43] X. Liu, "Global blockchain technology and application innovation status, trend and inspiration," (in Chinese), *China Sci. Technol. Bus.*, no. 1, pp. 27–31, Jan. 2020.
[44] N. Zhenyu, Z. Fengwei, and S. Weisong, "A study of using TEE on edge computing," *J. Comput. Res. Develop.*, vol. 56, no. 7, pp. 1441–1453, Jan. 2019.
[45] J. Wang, C.-Y. Fan, Y.-Q. Cheng, B. Zhao, T. Wei, F. Yan, H.-G. Zhang, and J. Ma, "Analysis and research on SGX technology," *J. Softw.*, vol. 29, no. 9, pp. 2778–2798, Sep. 2018, doi: 10.13328/j.cnki.jos.005594.
[46] G. Fan and P. Dong, "Research on trusted execution environment building technology based on TrustZone," *Netinfo Secur.*, vol. 16, no. 3, pp. 21–27, Mar. 2016, doi: 10.3969/j.issn.1671-1122.2016.03.004.
[47] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. Eurocrypt*, vol. 99, 1999, pp. 223–238.
[48] Z. Wang, S. Zhang, S. Jin, and H. Wang, "Survey on privacy preserving techniques for blockchain," *Chin. J. Internet Things*, vol. 2, no. 3, pp. 71–81, Sep. 2018.
[49] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, "Mixcoin: Anonymity for bitcoin with accountable mixes," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, in Lecture Notes in Computer Science, 2014, pp. 486–504.
[50] L. Valenta and B. Rowan, "Blindcoin: Blinded, accountable mixes for bitcoin," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Berlin, Germany: Springer, 2015, pp. 112–126.
[51] Q. Shentu and J. Yu, "A blind-mixing scheme for Bitcoin based on an elliptic curve cryptography blind digital signature algorithm," Oct. 2015, *arXiv:1510.05833*. [Online]. Available: https://arxiv.org/abs/1510.05833
[52] S. Fu, H. Xu, P. Li, and T. Ma, "A survey on anonymity of digital currency," *Chin. J. Comput.*, vol. 42, no. 5, pp. 1045–1062, Sep. 2019, doi: 10.11897/SP.J.1016.2019.01045.
[53] M. Bellare, J. Kilian, and P. Rogaway, "The security of cipher block chaining," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer-Verlag, 1994, pp. 341–358.
[54] M.-J. O. Saarinen, "Arithmetic coding and blinding countermeasures for lattice signatures: Engineering a side-channel resistant post-quantum signature scheme with compact signatures," *J. Cryptograph. Eng.*, vol. 8, no. 3, pp. 1–14, Jan. 2017, doi: 10.1007/s13389-017-0149-6.
[55] G. Maxwell. (Oct. 5, 2018). *CoinJoin: Bitcoin Privacy for the Real World*. [Online]. Available: https://bitcointalk.org/index.php
[56] T. Ruffing, P. Moreno-Sanchez, and A. Kate, "CoinShuffle: Practical decentralized coin mixing for bitcoin," in *Proc. Eur. Symp. Res. Comput. Secur.* Cham, Switzerland: Springer, 2014, pp. 345–364.
[57] G. Danezis and A. Serjantov, "Statistical disclosure or intersection attacks on anonymity systems," in *Proc. 6th Int. Conf. Inf. Hiding*. Berlin, Germany: Springer-Verlag, 2004, pp. 293–308.
[58] G. Bissias, A. P. Ozisik, B. N. Levine, and M. Liberatore, "Sybil-resistant mixing for bitcoin," in *Proc. ACM Workshop Privacy Electron. Soc.*, Scottsdale, AZ, USA, Nov. 2014, pp. 149–158.
[59] J. H. Ziegeldorf, F. Grossmann, M. Henze, N. Inden, and K. Wehrle, "CoinParty: Secure multi-party mixing of bitcoins," in *Proc. 5th ACM Conf. Data Appl. Secur. Privacy*, 2015, pp. 75–86.
[60] I. Damgård, M. Geisler, M. Krøigaard, and J. B. Nielsen, "Asynchronous multiparty computation: Theory and implementation," in *Proc. 12th Int. Conf. Pract. Theory Public Key Cryptogr.* Irvine, CA, USA: Springer-Verlag, Mar. 2009, pp. 160–179.
[61] A. Mackenzie, S. Noether, and M. C. Team, "Improving obfuscation in the CryptoNote protocol," Tech. Rep. MRL-0004, Jan. 2015. [Online]. Available: https://www.docin.com/p-2122152949.html
[62] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed e-cash from bitcoin," in *Proc. IEEE Symp. Secur. Privacy*, Berkeley, CA, USA, May 2013, pp. 397–411.
[63] S. N. Van. (Sep. 12, 2017). *CryptoNote, Version 2.0*. [Online]. Available: https://whitepaperdatabase.com/wp-content/uploads/2017/09/Monero-whitepaper.pdf
[64] L. Zhu, H. Dong, and M. Shen, "Privacy protection mechanism for blockchain transaction data," *Big Data Res.*, vol. 4, no. 1, pp. 46–56, Jan. 2018, doi: 10.11959/j.issn.2096-0271.2018005.
[65] N. T. Courtois and R. Mercer, "Stealth address and key management techniques in blockchain systems," in *Proc. Int. Conf. Inf. Syst. Secur. Privacy*, Porto, Portugal: SciTePress, 2017, pp. 559–566.

[66] T. Ruffing and P. Moreno-Sanchez, "ValueShuffle: Mixing confidential transactions for comprehensive transaction privacy in bitcoin," in *Sliema: Financial Cryptography and Data Security*. Cham, Switzerland: Springer, 2017, pp. 133–154.
[67] A. Miller, M. Möeser, K. Lee, and A. Narayanan, "An empirical analysis of linkability in the Monero blockchain," Apr. 2017, *arXiv:1704.04299v1*. [Online]. Available: https://arxiv.org/abs/1704.04299v1
[68] A. Kumar, C. Fischer, S. Tople, and P. Saxena, "A traceability analysis of Monero's blockchain," in *Proc. Eur. Symp. Res. Comput. Secur.* Cham, Switzerland: Springer, 2017, pp. 153–173.
[69] L. Zhang, B. Liu, R. Zhang, B. Jing, and Y. Liu, "Overview of blockchain technology," *Comput. Eng.*, vol. 45, no. 5, pp. 1–12, Mar. 2019, doi: 10.19678/j.issn.1000-3428.0053554.
[70] C. Decker and R. Wattenhofer, "A fast and scalable payment network with bitcoin duplex micropayment channels," in *Proc. Symp. Self-Stabilizing Syst.* Cham, Switzerland: Springer, 2015, pp. 3–18.
[71] J. Poon and T. Dryja. (Jan. 14, 2016). *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments DRAFT Version 0.5.9.2*. [Online]. Available: http://lightning.network/lightning-network-paper.pdf Draft Version 0.5
[72] A. Miller, I. Bentov, S. Bakshi, R. Kumaresan, and P. McCorry, "Sprites and state channels: Payment networks that go faster than lightning," in *Proc. 23rd Int. Conf. Financial Cryptogr. Data Secur.*, Frigate Bay, St. Kitts and Nevis, 2019, pp. 508–526.
[73] M. Green and I. Miers, "Bolt: Anonymous payment channels for decentralized currencies," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2017, pp. 473–489.
[74] E. Heilman, L. Alshenibr, F. Baldimtsi, A. Scafuro, and S. Goldberg, "Tumblebit: An untrusted bitcoin-compatible anonymous payment hub," in *Proc. NDSS*, 2017, pp. 1–15.
[75] P. McCorry, M. Möser, S. F. Shahandasti, and F. Hao, "Towards bitcoin payment networks," in *Proc. Australas. Conf. Inf. Secur. Privacy*. Cham, Switzerland: Springer, 2016, pp. 57–76.
[76] E. Heilman, F. Baldimtsi, and S. Goldberg, "Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Berlin, Germany: Springer, 2016, pp. 43–60.
[77] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Secur. Privacy Workshops*, San Jose, CA, USA, 2015, pp. 180–184.
[78] X. Yu, "Research and application of privacy preserving techniques and blockchain technology," M.S. thesis, Dept. Comput. Sci., Nanjing Univ. Posts Telecommun., Jiangsu, China, 2019.
[79] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *Proc. IEEE Symp. Secur. Privacy (SP)*, San Jose, CA, USA, May 2016, pp. 839–858.
[80] X. Zhang, Y. Jing, and Y. Yan, "A glimpse at blockchain: Form the perspective of privacy," *J. Inf. Secur. Res.*, vol. 3, no. 11, pp. 981–989, Nov. 2017.
[81] H. Wang, F. Zhang, T. Li, M. Gao, and X. Du, "Security and privacy-protection technologies in smart contract," *J. Nanjing Univ. Posts Telecommun., Natural Sci. Ed.*, vol. 39, no. 4, pp. 63–71, Jul. 2019, doi: 10.14132/j.cnki.1673-5439.2019.04.009.
[82] W. Nan, "A study on SGX-based traceable anonymous scheme for permissioned blockchain," M.S. thesis, Dept. Comput. Sci., Nanjing Univ., Jiangsu, China, 2019.
[83] J. Wang, Y. Jing, Q. Li, and Y. Yang, "Survey of research on SGX technology application," *J. Netw. New Media*, vol. 6, no. 5, pp. 3–9, Sep. 2017.
[84] H. Jing, "Research on the application mode of blockchain in financial industry," M.S. thesis, Dept. Econ., Zhejiang Univ., Zhejiang, China, 2018.
[85] D. Chen, "Research on key technologies and applications of cloud computing based on blockchain," Xidian Univ., Xi'an, China, 2018.
[86] T. Chen, "Research on financial big data authentication model based on block chain technology," *Mod. Electron. Techn.*, vol. 43, no. 6, pp. 171–174, Mar. 2020, doi: 10.16652/j.issn.1004-373x.2020.06.042.
[87] H. G. Zhang, "Research and development of trusted computing in China," in *Proc. 3rd Asia–Pacific Trusted Infrastruct. Technol. Conf. (APTC)*. New York, NY, USA: IEEE Computer Society, 2008, pp. 1–3.
[88] Z. Lu, Q. Wang, G. Qu, and Z. Liu, "BARS: A blockchain-based anonymous reputation system for trust management in VANETs," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun., 12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, New York, NY, USA, Aug. 2018, pp. 98–103.
[89] B. Qin, L. Chen, Q. Wu, Y. Zhang, L. Zhong, and H. Zheng, "Bitcoin and digital fiat currency," *J. Cryptol. Res.*, vol. 4, no. 2, pp. 176–186, Apr. 2017, doi: 10.13868/j.cnki.jcr.000172.

DAN WANG was born in Shandong, China, in 1996. She received the B.S. degree from Jining Medical University, in 2019. She is currently pursuing the M.S. degree with Yantai University. Her main studies include privacy protection and scalability of blockchain.

JINDONG ZHAO was born in Yangxin, Shandong, China, in 1974. He received the B.S. degree in applied mathematics from Yantai University, in 1997, the M.S. degree in computer software and theory from Jilin University, in 2004, and the Ph.D. degree in computer architecture from the University of Science and Technology Beijing, in 2011.

From 1997 to 2006, he was an Engineer with the Network Center, Yantai University. Since 2006, he has been a Lecture with the School of Computer, Yantai University. Since 2013, he has also been an Assistant Professor with the School of Computer and Control Engineering, Yantai University. He is the author of two books and more than 15 articles. His research interests include the Internet of Things technology, bigdata process technology, and blockchain technology, He is currently an Associate Editor of *Wireless Personal Communications* Journal.

YINGJIE WANG received the Ph.D. degree from the College of Computer Science and Technology, Harbin Engineering University.

She visited Georgia State University, from September 2013 to September 2014, as a Visiting Scholar. She is currently an Associate Professor with the School of Computer and Control Engineering, Yantai University. She is a Postdoctoral Researcher with the South China University of Technology. Her research interests are mobile crowdsourcing, privacy protection, and trust computing. She has published more than 40 articles in well-known journals and conferences in her research field, which include an ESI high cited paper. In addition, she has presided one National Natural Science Foundation of China Project, two China Postdoctoral Science Foundation Projects, and joined three National Natural Science Foundation of China Projects and one Natural Science Foundation of Shandong Province Project.