Journal of Network and Computer Applications 126 (2019) 45–58

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Review

A survey on privacy protection in blockchain system

Qi Feng [a], Debiao He [a,*], Sherali Zeadally [b], Muhammad Khurram Khan [c], Neeraj Kumar [d]

[a] Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan, China
[b] College of Communication and Information at the University of Kentucky, USA
[c] Center of Excellence in Information Assurance (CoEIA), King Saud University, Saudi Arabia
[d] Department of Computer Science and Engineering, Thapar University, Patiala, India

ARTICLE INFO

Keywords:
Privacy
Anonymity
Blockchain
Cryptography
Cryptocurrency

ABSTRACT

Blockchain, as a decentralized and distributed public ledger technology in peer-to-peer network, has received considerable attention recently. It applies a linked block structure to verify and store data, and applies the trusted consensus mechanism to synchronize changes in data, which makes it possible to create a tamper-proof digital platform for storing and sharing data. It is believed that blockchain can be utilized in diverse Internet interactive systems (e.g., Internet of Things, supply chain systems, identity management, and so on). However, there are some privacy challenges that may hinder the applications of blockchain. The goal of this survey is to provide some insights into the privacy issues associated with blockchain. We analyze the privacy threats in blockchain and discuss existing cryptographic defense mechanisms, i.e., anonymity and transaction privacy preservation. Furthermore, we summarize some typical implementations of privacy preservation mechanisms in blockchain and explore future research challenges that still need to be addressed in order to preserve privacy when blockchain is used.

1. Introduction

Marking the new dawn of a new era, blockchain is a groundbreaking innovation in decentralized information technology. Originally invented as the underlying infrastructure of (Bitcoin) (the first decentralized cryptocurrency which develops extremely rapidly since its release in 2009), blockchain's potential application has reached far beyond cryptocurrency and financial assets. As the technology gained wider recognition in recent years, there has been a flurry of advancements, new use cases and applications. The range of potential applications of blockchain is endless, from cryptocurrencies to Internet of thing (IoT), supply chain management (SCM) and so on.

In the area of digital currency, blockchain constitutes the basic underlying infrastructure, which allows the monetary operation to be performed in a distributed way without the need of some central entities. Built upon blockchain, (Bitcoin) and other altcoins such as (Ethereum project, Litecoin, Monero project and Zerocash), have grown into a new surprisingly robust ecosystem. According to the statistics (BitInfoCharts, 2017), The market capitalization (as of July 2018) of Bitcoin is over $112 billions and Ethereum is over $47 billions. Not less than 60 thousands blockchain transactions per hour can be confirmed all over the world.

Although cryptocurrency is the most paradigmatic application of blockchain, there are other applications far beyond it, e.g., blockchain makes it attractive for the Internet of Things (IoT) environment which is equipped with a decentralized topology and many Internet-enabled devices. By using blockchain, device management could be automated and data synchronization could be easier and faster among IoT devices (as discussed in (Huh et al., 2017; Dorri et al., 2016; Conoscenti et al., 2016)). Moreover, blockchain can also enhance the transparency and traceability of ownership for the supply chain management system (as discussed in (Kim and Laskowski, 2016; Korpela et al., 2017; Abeyratne and Monfared, 2016)). Furthermore, the decentralized feature of blockchain can inherently ease the pressure on centralized servers, such as in public key infrastructure or identity management system (as discussed in (Ali et al., 2016; Fromknecht et al., 2014; Ebrahimi, 2017; Qin et al., 2017)).

* Corresponding author.
E-mail addresses: fq.whu@whu.edn.cn (Q. Feng), hedebiao@163.com (D. He), szeadally@uky.edu (S. Zeadally), mkhurram@ksu.edu.sa (M.K. Khan), nehra04@yahoo.co.in (N. Kumar).

https://doi.org/10.1016/j.jnca.2018.10.020
Received 1 May 2018; Received in revised form 17 September 2018; Accepted 29 October 2018
Available online 13 November 2018

Although blockchain can provide a powerful abstraction for the design of distributed systems, privacy issues (e.g., the leakage of user real identity and transaction amount) should not be ignored from the protection of users' interests. For example, when the blockchain is integrated into supply chain management (SCM) system, if the buyer-supplier relations during the blockchain communication or the extra information for each communication are not protected, it may leak trade secrets of the suppliers. For example, the price of products from different suppliers can be estimated by analyzing transaction records. As a result, the suppliers' incentives to apply this blockchain-based system will be diminished for their interests are compromised, which seriously limits the widely applications of blockchain in SCM system. From the above indications, it is necessary to conduct a systematic summary and evaluation on the privacy preservation of blockchain.

1.1. Our contributions

As far as we know, most of the review articles (Li et al., 2017; Zheng et al., 2016; Halim et al., 2017; Bonneau et al., 2015) are emphasizing the comprehensive overview on the security issues and challenges of blockchain. Other surveys are focusing on the privacy challenges on the decentralized cryptocurrencies (Genkin et al., 2018; Meiklejohn and Orlandi, 2015; Ylihuumo et al., 2016).

The first objectives of our surveys is to give a critical comparative analysis of cryptographic defense mechanisms for the privacy of blockchain. Originality of the survey is multifold: 1) redefines the concept of privacy in blockchain, not just the user's privacy, but also the transaction-related privacy, 2) introduces existing threats on the presented two concepts of privacy in blockchain, 3) introduces several technologies, especially cryptographic techniques, which have be used to protect privacy of blockchain, 4) presents a step-by-step analysis in order to help the readers to better understand the origin, objective, and drawback of each protection approach, 5) compares the impact of various privacy preserving methods in current practical projects, and finally, 6) identities future research directions on privacy protection for blockchain.

Furthermore, the present survey brings several attractive advantages. First, it leads the users and researchers to understand the management challenges and opportunities in the privacy of blockchain. Second, it helps a security designer to specify, validate and implement adaptive privacy preservation policies in blockchain applications. Finally, this survey conveys to the reader the ability to conduct science investigation mission to analyze privacy attacks against blockchain.

1.2. Paper organization

We organize the remainder of this paper as follows. Section 2 presents an overview on the basic architecture and characteristics of blockchain. Section 3 provides a detailed analysis of the privacy requirements and existing threats. We discuss different techniques for identity privacy preservation in Section 4. Section 5 classifies and compares cryptographic protocols that are used for transaction privacy of blockchain. Furthermore, we summarize these techniques and discuss future research directions that need to be explored further to mitigate privacy concerns of blockchain in Section 6. Finally, Section 7 concludes this paper.

2. Overview of blockchain

Blockchain was originally introduced by S. Nakamoto (2008) to record all the transactions of Bitcoin and avoid misbehaving or cheating. To better understand the core concept and technology of blockchain, we will overview some knowledge about blockchain in this section, i.e., the fundamental structure of blockchain, how many types of blockchain there are, as well as what the main characteristics of blockchain are.

2.1. Structure of blockchain

Basically, blockchain is an append-only database maintained by the nodes of a peer-to-peer (P2P) network. As shown in Fig. 1, the basic structure of the blockchain may consist of three levels, i.e., underlying P2P network, databases and its various applications.

The P2P network is responsible to ensure the freely communication among the blockchain nodes, where the nodes are geographically dispersed but being equally privileged participants in the application. There is no centralized server in P2P network, and each nodes is an information consumer, but also an information provider. Each node engages in the routing process of the entire network, the discovering and maintaining of connections to neighboring peers, the propagation and verification of transactions, as well as the synchronization of data blocks (transaction and block are both the data structure of blockchain, which will be introduced in the subsequent content). This "flat" topology of P2P network is the key reflection and basis of the blockchain's decentralized feature.

The global ledger is responsible for the core mission of blockchain, i.e., transmitting message reliably and trustfully between account addresses. The account address is an unique digital pseudonym when users engaging in the blockchain, which is normally generated with the public key cryptography (e.g., elliptic curve cryptography) by the user. Each communication between two or more addresses are carried out through a transaction, which is indeed a record including senders' addresses, receivers' addresses, messages, and of course, signatures from related participants and so on. There is a special and flexible message exchanging mode in blockchain, i.e., smart contract. There are various definitions about it, for example: in Bitcoin, it is an script executing during the confirmation of cryptocurrency; in Ethereum, it is extended to be a Turing-complete language and can achieve more complex functions; in (Hyperledger projects), it directly executes the blockchain functions. All of the related messages will be eventually recorded in blockchain global ledger.

When confirming a transaction or smart contract, the global ledger will record it in a continuously growing list of blocks, where each block carries a hash pointer as a link to the previous one, a timestamp and some transactions or smart contracts organized in the form of a Merkle Hash Tree. These blocks are linked together from the genesis block to the latest block in the chronological order, which is why blockchain be named. Note that the genesis block is the **Block #0** of the blockchain and has no previous block. Every transaction and block will eventually be broadcast through the entire P2P network, and an agreed-on consensus mechanism (e.g., proof of work (POW) (Nakamoto, 2008), proof of stake (POS) (Siim), practical byzantine fault tolerance (PBFT) (Castro Liskovet al., 1999) and etc) will be carried out to determine what blocks get added to the ledger and what the current state is. Finally, this global ledger will then be synchronized among the peers of blockchain and therefore, cannot be modified easily by malicious entities.

The applications of blockchain provides application program interfaces (APIs) for various scenarios. Users directly interact with each other via these APIs with no need to think about details of underlying technologies. As introduced in Section 1, the most widely application of blockchain is still in financial fields. Furthermore, the project of Hyperlegder incubates and promotes a range of blockchain businesses, including distributed ledger frameworks, smart contract engines, client libraries, graphical interfaces and so on. Based on the immutability and integrity of blockchain, some other applications such as digital document management platform (Factom), copyright protection system (Binded), distributed data network (Maidsafe), autonomous decentralized P2P telemetry ADEPT for IoT (Cohn et al., 2017) and so on have been released for different scenarios.

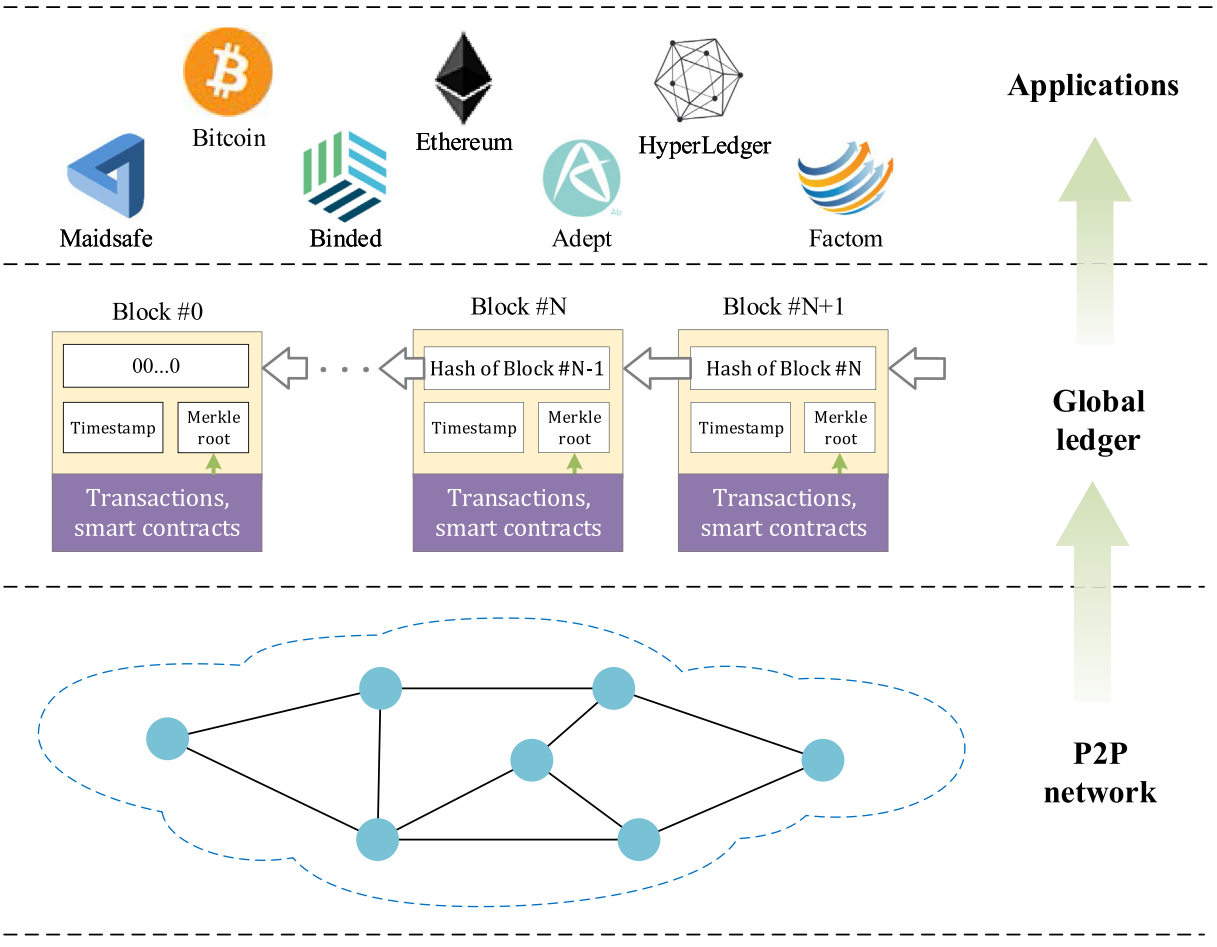

Fig. 1. The basic structure of blockchain.

2.2. Classification of blockchain

Based on the permissioning, there are three options of blockchain: i.e., public blockchain, private blockchain and consortium blockchain. Most projects today rely on the public blockchain, which grants access to a large number of users, network nodes, and markets. However, there are still reasons to prefer a private blockchain or consortium blockchain (among a group of trusted participants). For example, a number of companies in verticals, like banking, are looking to private blockchain as their own data exchanging platform. Here, we explains the difference between these three style:

- *Public blockchain*: a public blockchain (e.g., Bitcoin or Ethereum) is a blockchain that any participant can read, submit transactions to and expect to see them included if they are valid, as well as engage in the consensus process. As a substitute for centralized or quasi-centralized trust, public blockchain are secure by cryptoeconomics (the merge of economic incentives and cryptographic verification), where following a general principle that the degree to which someone can have an influence in the consensus process is proportional to the quantity of economic resources that they can bring to bear. A public blockchain is, therefore, a completely transparent and decentralized database of the transactions on an open network.
- *Consortium blockchain*: a consortium blockchain (e.g., the HyperLedger) is a blockchain where the consensus process is controlled by a pre-selected set of nodes. For example, one might imagine a consortium of 15 institutions each of which operates a node and of which 10 must confirm a block in order for the block to be valid. The right to read the blockchain may be public, or restricted to specific participants. There are also hybrid routes such as providing an public API that allows members to make a limited number of queries and get back the root hashes of blocks along with the cryptographic proofs on the blockchain states. A consortium blockchain is, therefore, considered to be partially decentralized.
- *Private blockchain*: a private blockchain is, essentially, the inverse of public blockchain in all key attributes, where the write permission is kept centralized to one organization in a fully private blockchain and the read permissions may be public or restricted with an arbitrary extent. Ultimately, private blockchain is a catch-all term for anything that is not completely public. There is broad flexibility for governance and management within it.

2.3. Key characteristics of blockchain

Here, we will conclude from several research efforts (e.g., (Nakamoto, 2008; Swan, 2015; Pilkington, 2016; Underwood, 2016; Tapscott and Tapscott, 2016)) four attributes which describe a basic blockchain architecture as a general decentralized ledger offering data integrity and traceability. We describe these characteristics next.

1. *Autonomous:* One significant property of blockchain is that there is no single entity controlling or governing the network. In particular, in a public setting, any node can sign and publish transactions to the blockchain and reviews them at any time if they are accepted by other nodes of the decentralized network. Besides, everyone could join in the consensus process so as to expand new blocks into the blockchain.
2. *Distributed:* Blockchain system is built on the P2P network, where every signed transaction will be broadcast by the source node to its one-hop peers. Then, the neighboring peers verify these incoming

transactions: valid ones will be relayed further and invalid ones will be discarded. Eventually, these transactions can spread across the entire P2P network. A newly generated block will be treated in the same way in terms of its notification and synchronization in the network.

3. *Immutability:* All the valid blocks and transactions recorded on the global ledger are practically immutable due to the need for verification by other nodes and traceability of changes. Furthermore, the whole global ledger will be synchronized among the blockchain nodes following the consensus mechanism, such that users are provided with a higher degree of confidence that the data in blockchain is unaltered and accurate.
4. *Contractual:* The consensus process (e.g., mining or voting) depends on the status of the data. Consensus is achieved by executing the rules (i.e., smart contract) of the blockchain without any central authorization. These code-defined rules ensure that any monetary actions will be executed timely and correctly without human intervention.

These characteristics bring several benefits that are derived from the blockchain architecture (e.g., durability, transparency, verifiability, and process integrity (Abeyratne and Monfared, 2016)).

3. Privacy requirements and threats for blockchain

Next, we present two analyses that extract the privacy requirements and threats which arise from the network environment, transactions, and applications. The first analysis is based on the fundamental characteristics of blockchain, and the second analysis describes the various threats in detail.

3.1. Privacy requirements for blockchain

To protect privacy, the blockchain needs to satisfy the following requirements: (1) the links between transactions should not be visible or discoverable, and (2) the content of transactions is only known to their partakers. As we mentioned earlier, the private or permissioned blockchain could set an access control policy to satisfy the privacy requirements of blockchain, which means the complete transparency of the blockchain data is not a problem. However, in the case of a public setting, everyone can have access to the blockchain with no restrictions, the privacy requirements should be considered on the following two factors:

1. *Identity Privacy*: which means intractability between the transaction scripts and the real identities of their partakers, as well as the transactional relationships between users. Even if users apply random addresses (or pseudonyms) when acting in the blockchain, they can only provide limited identity privacy. By monitoring the unencrypted network and traversal through the public blockchain, some behavioral analysis strategies (e.g., anti-money laundering (AML) regulation (Schott, 2006) or know your customer (KYC) policy (Gill and Taylor, 2004)) may reveal some information about who is using blockchain, or for what.
2. *Transaction Privacy*: which means that the transaction contents (e.g., amount or transacting patterns) can only be accessed by specified users, and kept unknown to the public blockchain network. Transaction privacy is desired in many blockchain-based applications, e.g., electrical health record management or big data's anonymous authentication and authorization, where users may wish for increased levels of privacy and avoid revealing their sensitive information to any curious blockchain entities.

3.2. Privacy threats for blockchain

As described previously, a transaction of blockchain contains the addresses of its participants, trade values, timestamp and signature of its sender. Due to the public nature of the blockchain network, it is possible to trace the flow of transactions to extract the users' physical identities or other additional information by data mining. In this section, we refer to the Bitcoin (Nakamoto, 2008) system as a typical instance to analyze the privacy threats for the blockchain network.

3.2.1. De-anonymization

Bitcoin provides a limited form of unlinkability: users always create pseudonyms when they connect to the bitcoin system. However, due to the public and openness of blockchain, it is possible to perform a static analysis of the blockchain or actively listening for network information to unmask users, i.e., de-anonymization. Here, we list several attacks that may work for de-anonymizing users' real identities.

1. *Network Analysis*: as we mentioned in Section 2, the blockchain is based on the P2P network architecture which means that a node will leak its IP address when broadcasting transactions. Koshy et al. (2014) identified three anomalous relay patterns for network analysis which could be used to map bitcoin addresses to IP addresses (i.e., multi-relayer & non-rerelayed transaction, single-relayer transactions and multi-relayer & rerelayed transactions). Reid and Harrigan (2013) conducted network analysis via publicly available information from the bitcoin faucets which give out a small amount of bitcoin freely. These sites sometimes publish the IP addresses of recipients to prevent abuse.
2. *Address Clustering*: there are inherent properties of the transaction in blockchain could be applied to link addresses controlled by the same user:
   (a) According to the structure of blockchain (Nakamoto, 2008), all the inputs in a transaction are normally signed by the sender, therefore the addresses of inputs involved in one transaction may be controlled by the same entity (user or organization).
   (b) The change address (Bitcoinwiki) is the one that receives the price difference between the outputs and the actual value the user intends to pay. Thus in a transaction, the change address and input addresses always point to the same party. The change address is normally created by the wallet and will unlikely to be re-used for accepting payments, e.g., in bitcoin.
   (c) Some transactions does not contain an origin-destination pair. For example, coinbase blocks (Wiki. coinbase) have no origin address (i.e., no inputs) and points to one destination address (i.e., one output). This is indeed the origin of a transaction list and the only destination address always points to a miner or a mining pool.
   (d) To speed up the confirmation process of a transaction, the approaches presented in (Vornberger, 2012; Vandervort, 2014) add some typical markers aiming to leverage existing trust relationships (e.g., identification information or certificates).

   Based on these knowledge and other side information, the users could partition the network into different clusters of addresses. After being tagged via data collection technology, some of the addresses can be discovered to be corresponded to the same user. These approaches may not be easy in practice but still cannot be ignored. Researches in (Reid and Harrigan, 2013; Liao et al., 2016; Spagnuolo et al., 2014) has utilized this knowledge as heuristics for address clustering.

3. *Transaction Fingerprinting*: Another threat to anonymity is a transaction's user-related features. Androulaki et al. (2013) summarized six attributes that may characterize some aspects of transaction behaviors, i.e., Random time-interval (RTI), hour of day (HOD), time of hour (TOH), time of day (TOD), coin flow (CF) and input/output balance (IOB). Extra consideration on these attributes may increase the probability to de-anonymize an individual user. Androulaki et al. (2013) conducted an experiment in an university, where students uses Bitcoin as the daily transaction currency. By utilizing cluster

analysis based on the transaction fingerprints, the researches finally could recover the profiles of approximately 40% of the users, even when users adopt a new address for every transaction.

4. *DoS Attacks*: a denial-of-service attack is a cyber attack where the malicious attacker seeks to make a machine or network resource unavailable to its clients by disrupting services of the host connected to the Internet. One of the hiding approaches for IP addresses in P2P network is using anonymity networks (e.g., TOR), however, Biryukov et al. (Biryukov and Pustogarov, 2015) pointed out that the DoS attack may disconnect a TOR node from the blockchain network.
5. *Sybil Attacks*: a Sybil attack is a cyber attack where the malicious attacker subverts the reputation system of a P2P network by creating a large number of pseudonymous identities, using them to gain a disadvantageous influence. As for the de-anonymization in the blockchain, Bissias et al. (2014) analyzed that Sybil attacks could break or block the decentralized anonymity protocols and will increase the possibility to find out the users' real identities.

3.2.2. Transaction pattern exposure

Except for some personally identifiable information, other transaction information flows to the public network can be used to extract statistical distributions, which may reveal some new regulation within the applications of blockchain.

1. *Transaction graph analysis*: This type of analysis focuses on discovering some overall transaction features (e.g., daily turnover, exchange rate or transaction pattern) over time. For example, in bitcoin, Ron and Shamir (2013) identified all the largest transactions in the transaction graph and found out four characteristic transaction patterns in the bitcoin network. These features may have the chance of discovering someone's financial history when used in conjunction with de-anonymization methods (see Section 3.2).
2. *AS-level deployment analysis*: This technique aims to crawl the bitcoin network by recursively connecting to clients, requesting and collecting their lists of other peer's IP addresses. In this way, one can obtain concrete information on size, structure and distribution of the bitcoin's core network. These parameters can be used to impact at least the vitality and resilience of bitcoin's ecosystem. For example, Feld et al. (2014) analyzed the size and distribution of the bitcoin system among autonomous systems (AS) and found out that more than 30% of all nodes belong to 10 AS while over 900 AS contain just one single node.

4. Methodology for identity privacy preservation

This section presents a comprehensive overview of solutions that have been recently proposed by researchers aimed at preserving privacy of the blockchain. In a public setting such as in the cryptocurrency (Decred) or the blockchain-based electric vehicle charging system (Knirsch et al., 2018), it is suggested that the users' addresses needed to be changed by generating a new key pair for each session. Except that, there are three frequently-used mechanisms for protecting anonymity in the blockchain and they include: mixing services, ring signature, and non-interactive zero-knowledge proof.

4.1. Mixing services

In the blockchain, it is linkable between senders and receivers of a transaction, therefore, by analyzing the public content (i.e., analytical attack), one can infer some privacy information. One of the solutions to mitigate this attack is to obfuscate the transaction's relationships with the help of *mixer* (aka *tumbler* or *laundry*). A mixing service, first presented by Chaum (1981), allows users to hide who a participant communicates with as well as the content of the communication. We present the concepts in (Chaum, 1981) below (with the basic

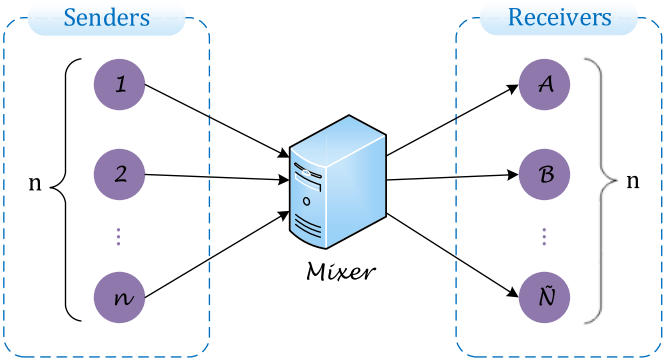

Fig. 2. Basic architecture of mixing services.

architecture shown in Fig. 2):

Assume that one entity prepares a message M for delivery to another entity at address R. What he/she need to do is encrypting M with the receiver's public key K_R, appending the address R, and then encrypting the result with the intermediary's public key K_I. The left-hand of the following expression denotes the ciphertext, which is transferred to an intermediary:

$$K_I(r_0, K_R(r_1, M), R) \rightarrow K_R(r_1, M), R$$

The symbol $\rightarrow$ denotes the transformation of the ciphertext by the intermediary into another ciphertext shown on the right-hand side. This transformation performs a decryption on the original ciphertext by the intermediary with its private key. Then the intermediary delivers the sub-ciphertext to R who then decrypts it with his/her own private key. It is to note that r_1 and r_0 are random numbers which ensure that no message is transferred more than once.

When the intermediary gets many inputs and outputs, this mechanism will hide the correspondences between each message's origin and destination. The order of arrival is hidden by outputting the uniformly sized items in random patterns. Additionally, to minimize the danger of the single intermediary being the attacker, multiple intermediaries can be linked together thereby creating a mix cascade.

Over the last few years, these services have been integrated into the blockchain network to obfuscate the transaction history and reduce the risk of de-anonymization. The research efforts mainly focus on two aspects: (i) centralized mixing and (ii) decentralized mixing.

4.1.1. Centralized mixing services

There are multiple mixing websites available (Onionbc; Bitcoin fog; Bitmixer; Helix by grams; Bitlaundry; Send shared; Bitblender). All of them offer the functionality to mix transactions anonymously at the cost of some service fees. These websites act as online mixers and swap the transactions among different users in order to hide the relationship between their incoming and outgoing transactions. In addition, most of them are reachable only via the TOR network (Tor project) which enables anonymous communications through a free, worldwide, volunteer overlay network.

There are two disadvantages behind these sites: (1) A possible attacker could be the service provider who would steal users' assets by not transferring them to the receivers analyzed by (Meiklejohn et al., 2013); (2) The service providers are in the middle and therefore they always keep logs for a certain time in order to route the transactions through the system whilst users cannot ensure that their personal data is not be disclosed.

To solve the first problem, one of the solutions is conditional execution, which means that *if and only if* the mixer operates correctly, it can get reward, otherwise it gets nothing. For example, Gregory Maxwell introduced a third party-based mixing protocol for the bitcoin system called CoinSwap (Maxwell, 2013a). The general flow of this protocol is

that many senders deliver transactions to many receivers with a mixer acting as the intermediary. All the transactions between the sender & mixer and the mixer & receiver are escrow transactions that are protected by hash-lock and can only be spent by corresponding redeeming transactions. This lock mechanism ensures that no one can steal the user's assets. However, the transactions are sent in plaintext, the mixer can still track all the transaction pairs and all the transactions' information between them.

Another attempt to address the first problem is to audit the misbehaved mixer which means using undeniable evidence for supervising the mixer's activities. For example, Mixcoin, proposed by Bonneau et al. (2014), adds a signature-based accountability mechanism to expose theft so that users are able to unambiguously prove if the mixer has misbehaved. Malicious operations will quickly have the mixer's reputation destroyed. Like CoinSwap, there is no way to prove that the mixer is not storing records sufficient to de-anonymize its users.

For the second question, the blind signature scheme is a common and advantageous tool for preserving privacy at the mixer side. A blind signature is such a digital signature wherein the message is blinded before it is signed. This approach generally consists of three procedures, i.e., blinding (covering the original message together with a random "blinding factor"), signing (signing the blinded message following the standard sign algorithm) and unblinding (removing the "blinding factor" to get a valid signature on the actual message). The resulting signature can be publicly verified while the signer will never know the connection between the message and the one he/she signed. Thus this can be used in protocols where anonymity is required. For example, Blindcoin (Valenta and Rowan, 2015), introduced by Valenta et al., combines the blind signature scheme with an append-only public log to keep the mixing process accountable and provides evidence against misbehaved mixer. Heilman et al. (2016) applies blind signature and smart contract to ensure anonymity and fairness during the mixing process.

One of the first attempts to provide anonymity in practical digital currency was Dash (released in 2014) (Dash is digital cash). In this project, a coin-mixing service called *PrivateSend* is created to remove all the unique information about the users from the blockchain network. The mixing network consists of a set of specific nodes (called master nodes) instead of a single website and restricts the mixing process to only accept certain denominations. Furthermore, every master node must pay 1000 Dash (the cryptocoin in Dash network) as a deposit that can increase the cost with master nodes' violations. However, the process of mixing is limited by the number of online participants (i.e., just three parties per round in Dash private transaction).

TumbleBit (Heilman et al., 2017) is the first approach to simultaneously achieve full unlinkability and avoids coin theft. The method is based on a centralized service but utilizes secure two-party computation and zero-knowledge proof in order to protect the user's privacy and the fairness of the transaction (includes enforcement on the mixing server to execute the protocol honestly). The mixing is done in three main steps: firstly, the payee engages the Tumbler (i.e., mixer in TumbleBit protocol) in the "Puzzle-Promise Protocol" and the later will set up an escrow transaction with one crypto-coin and return a puzzle (RSA encrypted version of the escrow cash-out transaction) to the payee. Secondly, the receiver gives the blinded puzzle to the payer who will then pay the Tumbler one crypto-coin to decrypt the puzzle, here they utilize the cut-and-choose protocol to enhance honest behavior among payer, payee and Tumbler. Finally, after the payer returns the blinded answer to the payee, the later will unblinds it and broadcasts the transaction. However, researchers in (Kuan and Chen, 2017) pointed out that there are several issue need to be noticed: 1) the hash-locks take up a lot of transaction space, which will lead to extra blockchain storage, network bandwidth and transaction fee, 2) it cannot support multiple payments in one single transaction, furthermore, 3) the multi-round cut-and-choose protocol takes a heavy execution time, which cannot satisfy real-time application requirements.

In conclusion, the centralized mixing services mainly suffer from three limitations: (i) the delay incurred when waiting for enough online participants to be mixed or executing the interactive process for fairness exchange is quite high; (ii) the centralized mixing server still remains a single point of failure, which may be vulnerable to denial of service (DOS) attacks and it also becomes the bottleneck of the distributed blockchain network; (iii) users always need to pay a fairly high mixing fees or deposits in practice.

4.1.2. Decentralized mixing services

To mitigate the DOS threat caused by the centralized services, a decentralized mixing pattern is proposed to enable a set of mutually untrusted peers to publish their messages simultaneously and anonymously without the need of a third-party anonymity proxy. Another major benefit of this approach is the elimination of the need for mixing fees. Furthermore, it is closer and more compatible to the decentralized structure of blockchain compared to the centralized mixing pattern. So far, there are mainly two methods to achieve the decentralized mixing process, i.e., CoinJoin and multi-party computation (MPC).

CoinJoin (Maxwell, 2013b) is a special transaction first described in the Bitcoin Forum by Gregory Maxwell. The core idea of CoinJoin is "When you want to make a payment, find some one else who also wants to make a payment and make a joint payment together.". For example, as illustrated in Fig. 3, there are two transactions: one is from User $\boldsymbol{A}$ to User $\boldsymbol{C}$ and another is from User $\boldsymbol{B}$ to User $\boldsymbol{D}$. These two independent transactions can be combined together into one CoinJoin transaction while inputs and outputs are unchanged. The resulting joint transaction mixes the link between inputs and outputs so that the exact direction of data flow will be kept unknown to the other peers.

This method provides perfect compatibility with Bitcoin-like blockchain, while ensuring that even malicious nodes can get nothing about transaction relationships. An alpha version of this sort of mixing technology has been implemented in Dark Wallet (Greenberg, 2014), (Joinmarket - coinjoin tha, 2015), and so on. However, CoinJoin suffers from three significantly drawbacks:

1. It lacks internal unlinkability which means that participants will know the details about the joint transaction, including the destinations of the transactions with which the senders' addresses are paired. This increases the likelihood of a Sybil attack as the number of available participants increases.
2. It is susceptible to the Denial-of-Service (DoS) attack proven in (Bissias et al., 2014). Assume that an attacker can create enough separate virtual entities which are associated with unique IP addresses and blockchain addresses. This attack may block the mixing process by refusing to sign the CoinJoin transactions.
3. A practical issue with CoinJoin is that the number of participants n has a maximum. One of the reasons for this maximum is because of the increased vulnerability to DoS attacks, and another reason is the exponential increasing communication overhead. On the other hand, when n is small, the effect of anonymity and unlinkability will be lower.

To achieve the internal unlinkability, CoinShuffle, proposed by Ruffing et al. (2014), utilizes an anonymous group communication protocol to hide the participants' identities from each other. This method achieves the internal unlinkanility by the simple trick of layered encryption, and the cost of high communication and computation overhead. Bissias et al. (2014) proposed a totally different approach, i.e., XIM, to support large anonymity sets. This protocol is based on the fair-exchange mixer in (Barber et al., 2012) as a secure method for partnering mix users without leaving evidence. Moreover, XIM mitigates the effects of Sybil attacks by an additional participating fee. However, it requires a significant waiting time in the whole mixing time, typical be in the order of hours.

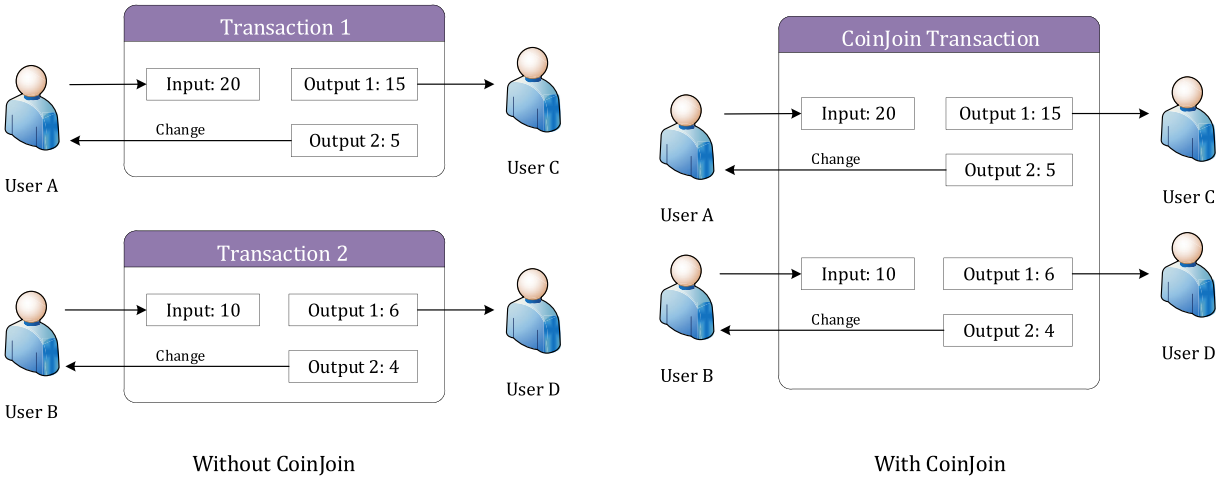

Fig. 3. An example of CoinJoin's core idea.

MPC (also known as secure multi-party computation) is a cryptographic method that ensures input privacy and jointly correct computation. In MPC, given a number of participants $P_1, P_2, \ldots, P_N$ with each of them having private data $d_1, d_2, \ldots, d_N$, respectively. Participants compute the value of a public function on the private data: $F(d_1, d_2, \ldots, d_N)$ while keeping their own inputs private. After the computation, all that the parties can learn is what they can learn from the output and their own input. The main operation of this method is playing over distance without requiring a trusted party which is suitable for decentralized tasks. Thus, (Ziegeldorf et al., 2015) proposed an ECDSA-based threshold scheme to achieve MPC and introduced the CoinParty protocol wherein users are allowed to generate a escrow address using multiple private keys and a threshold transaction is required to redeem its funds, i.e., only when a majority of participants agree to do so.

Table 1, which is largely based on a similar comparison from (Genkin et al., 2018), concludes and compares the main mixing services in blockchain in terms of five aspects as follows:

1. Whether the protocol can fully hide the identities of users.
2. Whether there is a centralized party involved in the mixing process.
3. Any fee for mixing services.
4. The risk of being blocked by Sybil attack.
5. Whether there is any possibility of coin-theft.
6. The number of participants per mixing round.
7. The delay incurred waiting to be mixed.

In short, mixing services are relatively simple methods for privacy protection in blockchain. Most of them are compatible with existing blockchain networks without any particular consensus mechanism, which means they need less resources to be implemented. Furthermore, combined with a proper defensive technique, mixing services can provide an acceptable privacy protection.

4.2. Ring signature

Although the decentralized mixing techniques (Maxwell, 2013b; Ruffing et al., 2014; Bissias et al., 2014; Ziegeldorf et al., 2015) offer "spontaneous" mixing in the blockchain, they still require a delay while participants discover their partners for their transactions to be mixed. The ring signature enables a user (also a member of a set) to sign a message on behalf of the "ring" of members but no way to tell which is the real one who signed. The core idea of this technology is the choice of a set without any central manager, which will significantly improve privacy in blockchain. In this section, we first present the basic idea behind the ring signature. Then, we present two existing ring implementations that achieve anonymity in blockchain.

4.2.1. Ring signature

Ring signature was initially designed by Rivest et al. in (Rivest et al., 2001) as a digital signature that could be used to produce a valid but anonymous signature from a group of possible signers without telling which member actually produced the signature (as illustrated in Fig. 4).

As shown in Fig. 4, in a ring architecture, User $\mathcal{A}$ chooses a set of participants including himself/herself and creates a ring $\{User_0, User_1, \ldots, User_n\}$. Each participant has a public key from a standard signature scheme (e.g., RSA, ECDSA). User $\mathcal{A}$ signs a message with his/her private key (SK_s) and all the public keys ($PK_0, \cdots, PK_s, \cdots, PK_n$) of the members in the ring. The verifier can tell that one of the set has signed the message but does not know who is the actual signer. Therefore, this signature provides complete anonymity for the signer.

One of the modified versions of ring signatures is the traceable ring signature (Fujisaki and Suzuki, 2007; Fujisaki, 2011). This type of ring signature can detect if two signatures were produced by the same user. Each traceable ring signature has a tag $T = (issue, \mathbf{PK})$, where $\mathbf{PK}$ denotes the public keys of the members (e.g., $PK_0 \cdots PK_n$ in the Fig. 4) of the set and *issue* is a label of a specific election or survey. In this case, $\mathcal{A}$ signs his/her message with SK_s and T. The verifier also checks the resulting signature with tag T instead of just $\mathbf{PK}$. There are two interesting statements on this signature:

1. If $\mathcal{A}$ signed one message twice using the same T, the two signatures can be linked by a public procedure while the identity of $\mathcal{A}$ remains concealed (i.e., linkability).
2. If $\mathcal{A}$ signed two different messages using the same T, then the two messages are from the same signer, and the anonymity of $\mathcal{A}$ will be revealed (i.e., traceability).

It is worth noting that any two signatures produced by two distinct tags are always unlinkable.

4.2.2. CryptoNote & Monero

The properties of anonymity and linkability have led to the development of several ring-based privacy preservation protocols for blockchain (e.g., (van Saberhagen, 2013; Noether Mackenzieet al., 2016; Sun et al., 2017)).

Table 1
Summary of mixing services in blockchain.

Protocol	Anonymity	Centralized party	Mix cost	Dos resistance	Sybil resistance	Theft resistance	Mixing scale	Waiting delay
Mixing website (Onionbc) ~ (Bitblender)	Linkable at mixer	Needed	Yes	Low	High	High	Limited to access	High
CoinSwap (Maxwell, 2013a)	Linkable at mixer	Needed	Yes	Low	High	Protected	No limitation	High
Mixcoin (Bonneau et al., 2014)	Linkable at mixer	Needed	Yes	Low	High	Accountable	No limitation	High
Blindcoin (Valenta and Rowan, 2015)	Unlinkable	Needed	Yes	Low	High	Accountable	No limitation	high
Blindly Signed Contracts (Valenta and Rowan, 2015)	Unlinkable	Needed	Yes	Low	High	Protected	No limitation	High
TumbleBit (Heilman et al., 2017)	Unlinkable	Needed	Yes	High	High	Protected	Limited by transaction space	High
Dash (Dash is digital cash)	Unlinkable	Needed, multiple	Yes	High, multi-ple mixers	High	Prevented with deposit	Small, up to three	Middle
CoinJoin (Maxwell, 2013b)	Internal Unlinkable	Decentralized	No	Low	Low	High	Small, same transaction value	High
CoinShuffle (Ruffing et al., 2014)	Unlinkable	Decentralized	No	Middle, blame	High	High	Small, same transaction value	High
XIM (Bissias et al., 2014)	Unlinkable	Decentralized	No	Middle with fees	Middle with fees	Low	Large	High
CoinParty (Ziegeldorf et al., 2015)	Unlinkable	Decentralized	No	High	High, MPC	Need 2/3 honest	Large	High

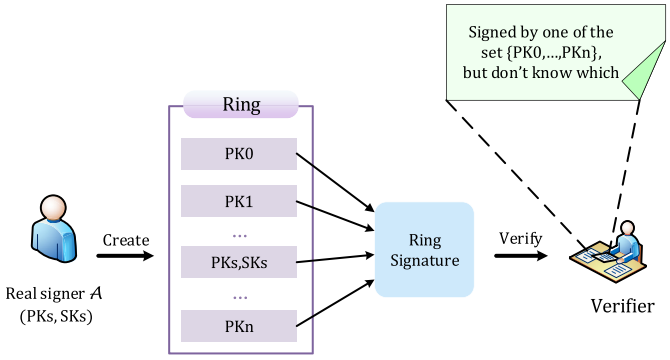

Fig. 4. Ring signature anonymity.

Saberhagen (van Saberhagen, 2013) implemented a slight modification of the traceable ring signature which allows a user to sign only one valid transaction with one private key. In his solution (called CryptoNote), the tag is replaced with a key image computed from the user's one-time private key to mitigate the double-spending attack. The identity of the signer is indistinguishable from the other users whose public keys are in the set until the owner produces a second signature using the same key pairs (see Fig. 5).

At the receiver's end, CryptoNote uses a one-time key pair for each asset transformation even for the same sender and receiver. Fig. 6 illustrates the basic idea of this technology. The destination of each CryptoNote output is a public key derived from receiver's one-time address and sender's random data. This ensures that every destination address is unique (unless the sender uses the same data for each of his/her transaction to the same receiver).

A standard transaction sequence is as follows: before sending a transaction, the sender $\mathcal{A}$ calculates a new destination address based on the public key of the receiver $\mathcal{B}$. The matching one-time keys can by recovered only by using the private key of $\mathcal{B}$. To transfer this transaction again, the output is signed with the one-time ring signatures by one-time keys, the key image and the anonymous public key set. In this sense, an incoming transaction for the same receiver is sent to a one-time address (instead of a unique address) and only the real receiver can spend the funds involved in this transaction. Furthermore, the traceable ring signature ensures unlinkable payments while precents double-spending when signing the transaction.

The CryptoNote protocol is vulnerable to analysis attacks based on the transaction amount. Another security drawback is that it requires

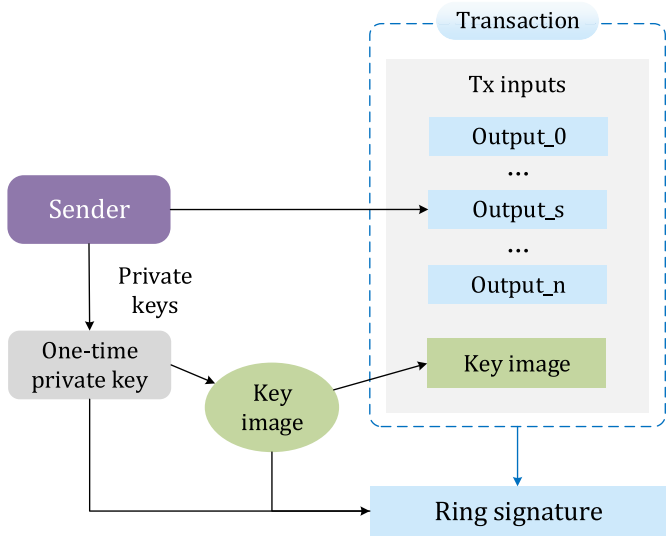

Fig. 5. Ring signature anonymity in CyrptoNote.

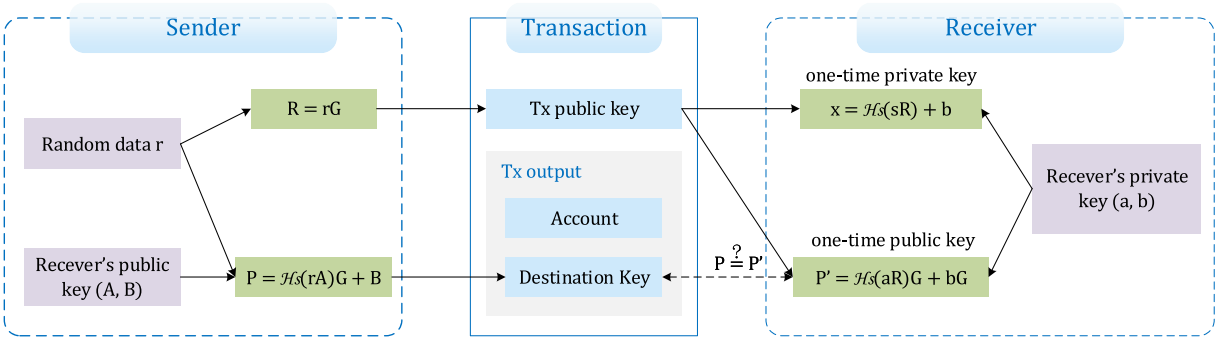

Fig. 6. One-time payment of CyrptoNote.

a specific set of public keys having the same amount involved in a ring signature which will lead to a smaller anonymity set than may be desired. These security weaknesses are discussed in depth in (Noether Mackenzieet al., 2016).

An improvement of the CryptoNote is Ring Confidential Transaction (RingCT) proposed by (Noether Mackenzieet al., 2016). The key innovation of this approach is hiding the amount using Greg Maxwell's Confidential Transaction (Maxwell, 2015) and the ring signature on the hidden amount is placed in the bottom row of the multilayered linkable spontaneous anonymous group signature (MLSAG) (Liu et al., 2004). Their solution can provide identity privacy and transaction privacy simultaneously. The most successful implementation of this approach to date is the cryptocurrency named Monero (Monero project) (first released in 2014).

Although the ring signature provides strong anonymity, it suffers from three limitations:

1. The size of its transactions (especially RingCT transactions) are very large, almost thousands of bytes per transaction. It will increase the storage space for the entire blockchain records.
2. The inherent drawback of ring signature is that a signature's size is directly proportional to the number of participants. Thus in practice, there are only a limited number of foreign outputs in each transaction (e.g., 4 outputs per Monero transaction by default).
3. The hidden amount will make it difficult for auditing, i.e., to verify if new cryptocurrencies have been generated secretly during the transaction or to determine the extra amount at some point.

4.3. Non-interactive zero-knowledge proof

Zero-knowledge proof (ZKP) is a cryptographic method with the goal to prove a given statement without leaking any additional information. Non-interactive zero-knowledge proof (NIZK) is a variant of ZKP where the interaction between the prover and the verifier is missing which is suitable in blockchain to verify the message anonymously and in a distributed way. Therefore, in this section, we present a general overview of the NIZK cryptography and two examples of its usage in preserving privacy of blockchain.

4.3.1. Non-interactive zero-knowledge proof

The concept of NIZK proof was proposed by (Blum et al., 1988). The ability to prove the correctness of an assertion independently without leaking additional information makes NIZK proof well suitable for creating privacy preserving protocols.

A formal definition of the NIZK proof system is: Let a pair of probabilistic polynomial time algorithms (P, V) be the prover and verifier, respectively. For language $\mathcal{L} \subseteq NP$ (with a security parameter κ), (P, V) is called the NIZK proof system for language $\mathcal{L}$ if it meets the following properties.

1. Completeness: for any input $x \in \mathcal{L}$, its witness w and polynomial $p(\cdot)$,

$$Pr[V(R, x, P(R, x, w)) = 1] \geq 1 - \frac{1}{p(|x|)}$$

2. Soundness: for any input $x \notin \mathcal{L}$, any probabilistic polynomial time algorithms P^* and polynomial $p(\cdot)$,

$$Pr[V(R, x, P^*(R, x)) = 1] < \frac{1}{p(|x|)}$$

3. Zero knowledge: for any $x \in \mathcal{L}$ and its witness w, there is a probabilistic polynomial time simulator S such that the two distributions are computationally indistinguishable:

$$\{R, x, P(R, x, w)\} \approx \{R, x, \pi\} \leftarrow S(x)$$

which means that all the information obtained by the verifier during the interaction with the proofer can also be computed by a probabilistic polynomial time simulator.

It is worth noting that R is a public random reference string.

4.3.2. Zerocoin & zerocash

Owing to the properties of completeness, soundness and zero knowledge, Zerocoin (Miers et al., 2013) employs NIZK proof cryptography to prevent transaction graph analysis. The main ideas behind this projects is analogous to decentralized mixing, where a coin is minted first and later redeemed with a totally new one that has no history information. NIZK proof cryptography is used to authenticate the validity of the minted coin so that an equal-priced new coin will be paid back.

In Zerocoin, all the valid coins with fixed denomination are maintained in the public ledger (i.e., the blockchain). A transaction with some amounts in Zerocoin consists of three steps, i.e., mint → publish → redeem. For example, if User $\mathcal{A}$ will pay a coin to User $\mathcal{B}$, $\mathcal{A}$ first needs to mint a coin by computing a random serial number sn and committing it with a trapdoor r. The resulting commitment cm can only be opened by (sn, r) while neither of them can be obtained by cm. Then $\mathcal{A}$ publishes cm with a mint transaction, which will be later verified and recorded in the public ledger through the consensus algorithms. When $\mathcal{B}$ wants to redeem this coin, he/she needs to send a spend transaction which contains the serial number sn and a NIZK proof π for the statements as follows:

1. He/She knows a commitment cm in the public ledger.
2. He/She knows the secret trapdoor r with which cm opens to sn.

If cm is correct and sn has not been spent previously, a new coin will be redeemed back; otherwise the transaction will be rejected and discarded. In this scenario, $\mathcal{A}$'s minted coin cannot be linked to $\mathcal{B}$'s retrieved funds because the proof π is zero-knowledge: there is no information about the exact mint transaction corresponding to the spend

transaction; r is unknowable from the sn revealed. Therefore, the origin of the transaction is anonymous.

Although Zerocoin provides strong anonymity guarantee, there are three main limitations that need to be considered:

1. Since $\mathcal{A}$ knows the sn, he/she may redeem it before $\mathcal{B}$ does so, or if $\mathcal{B}$ transferred this coin to $\mathcal{C}$, $\mathcal{A}$ will find out when $\mathcal{C}$ redeems with sn.
2. The fixed denomination of coins may be a major obstacle in its deployment in future applications.
3. Its public transaction lists cannot protect transaction privacy in terms of the amount or other metadata.

Zerocash (Sasson et al., 2014) made an improvement by providing identity and transaction privacy simultaneously to address some of the above limitations and achieved a high level of privacy protection for blockchain. A more detailed description of Zerocash is given in Section 5.1.

In addition to the mentioned methodologies, i.e., mixing, ring signature and NIZK, there are also some other mechanisms such as cryptographic commitment that can be used to protect user's sensitive information. Normally, a commitment is such a cryptographic primitives including "commit" and "reveal" phases, where values will be hidden by committing on it, and revealed later by the legal user. A general commitment scheme satisfies "binding" that the committed values are unaltered to any one including the one who commits on it. The research of Delmolino et al. (2016) utilized commitment scheme to protect the inputs of participants instead of being in plaintext, where the observers learns nothing about the other input choice even after revealing commitment. Similarly to (Delmolino et al., 2016), Knirsch et al. (2017) combined commitment and embedding mechanism to ensure that the embedded information remain completely private even after the revealing commitment. Furthermore, they also utilize the mixing approach to shuffling the relationships between ends of communication.

5. Methodology for transaction privacy preservation

This section discusses all the critical elements among the existing protocols that support transaction privacy in the blockchain. There are two main approaches for preserving transaction privacy of the blockchain, i.e., NIZK proof and homomorphic cryptosystem.

5.1. Non-interactive zero-knowledge proof

The basic idea behind the NIZK proof is described in Section 4.3. However, due to the fixed denomination (as we discussed before), Zerocoin provides strong anonymity but is unable to protect transaction privacy.

Therefore, Session et al. (Sasson et al., 2014) presented and issued a new cryptocurrency Zerocash aiming to achieve anonymity and transaction privacy simultaneously. In contrast to Zerocoin, Zerocash addresses the aforementioned issues via following technologies.

1. Zerocash makes use of zero-knowledge succinct non-interactive arguments of knowledge (zk-SNARKs) proof and a commitment scheme to hide a payment's original address. Furthermore, the coin value is added in the commitment and zero-knowledge proof so that the value is arbitrary and publicly verifiable.
2. Zerocash modifies the deviation of a coin commitment and serial number for each target payment. When the coins are spent, totally fresh serial numbers sn will be issued using the receiver's new private key. This mechanism ensures that even if the sender knows the previous sn, he/she still be unable to track or re-spend the coins.
3. The sender encrypts the transaction amounts and other metadata using the receiver's public key before spending the coins, and appends the ciphertext in the spending transaction. This type of transaction does not leak paid amounts and destination addresses because of the security of public-key encryption scheme.

Zerocash achieves the highest level of anonymity and transaction privacy protection for the blockchain but at the expense of high computational costs it requires when it generates the transaction proofs.

In contrast, as other technology such as smart contract has emerged where users can arbitrarily define programs running in the blockchain, it is important to consider the programmability aspect without exposing transactions and data in cleartext to the public (i.e., any party not involved in the contract). Hawk presented by Kosba et al. (2016) is the first work to simultaneously provide transactional privacy and programmability in the blockchain. This method is based on the idea of Zerocash and the smart contract system, users send encrypted and committed information to the smart contract, and rely on the NIZK proofs to enforce the correctness of contract execution and funds' transfer. While the result of smart contract can be publicly verifiable, the entire sequence of transaction actions taken in the contract are kept confidential from the public.

A more in-depth discussion of smart contract system is out of scope of the survey, but is presented in (Szabo, 1997; Wood, 2014).

5.2. Homomorphic cryptosystem

A homomorphic cryptosystem (HC) is such a cryptographic encryption methodology that satisfies homomorphism so as to preserve arithmetic operations carried out on ciphertexts. It allows any party to perform computation on the ciphertexts while preserving the privacy of digital data.

Consider the following scenario, $\mathcal{A}$ has secret values $\{x_1, x_2, \ldots, x_n\}$ and $\mathcal{B}$ has a function $f(\cdot)$. $\mathcal{A}$ and $\mathcal{B}$ wants to calculate $f(x_1, \ldots, x_n)$ together without leaking secret values or algorithm details. We define $E(\cdot)/D(\cdot)$ to be a set of the homomorphic encryption system. Then $\mathcal{A}$ can send encrypted inputs $\{E(x_1), \ldots, E(x_n)\}$ to $\mathcal{B}$ who later performs the normal computations on the ciphertexts, randomizes and outputs the result to $\mathcal{A}$. After decryption, $\mathcal{A}$ will learn $f(x_1, \ldots, x_n)$ securely.

In general, homomorphic cryptography performs as black box, when given n ciphertexts and operations, it outputs the encrypted result of the same operations on the corresponding original data. This attractive feature makes homomorphic cryptography well suited for hiding and performing timely update of the amount and other medatata of a transaction. Typical homomorphic cryptographic schemes which could be used to protect privacy of blockchain include the Pedersen commitment scheme (Pedersenet al., 1991) and Paillier cryptosystem (Paillieret al., 1999).

5.2.1. Pedersen commitment scheme

The Pedersen commitment scheme (Pedersenet al., 1991) is one of the implementations of the homomorphic commitment scheme. It supports homomorphic operations (i.e., addition or multiplication) on the commitments and can provide perfect hiding of real message with the same trapdoor.

The Confidential Transaction (CT), conceptualized by Gregory Maxwell (Maxwell, 2015), was first implemented with the range proof scheme to protect the transaction privacy of the blockchain. In CT, the transaction amounts are committed by random blinding factors before sent to the recipients and later notarized by the recipients. As a result of the homomorphism property of Pederson commitment scheme, all the encrypted inputs and outputs of a transaction can be added up, respectively. The two encrypted sums are then compared to ensure trade-off when verifying the transaction. This process does not reveal the real amounts or other metadata of the transaction.

RingCT (described in Section 4.2.2) is a variant of CT used in Monero. In order to support the ring signature that provides sender's anonymity, RingCT verifies the transaction by added all the commitments on inputs and outputs up to a commitment on zero. Furthermore, users sign for the commitment when publishing transaction in original

CT scheme, whereas in the RingCT scheme users just need to prove that he/she has the corresponding secret key of the commitment.

5.2.2. Paillier cryptosystem

The Paillier cryptosystem (Paillieret al., 1999) is an efficient additive homomorphic encryption system that is based on the composite residuosity class problem. This means that given only the ciphertexts on m_1 and m_2 along with the same public key, anyone can calculate the ciphertext on $m_1 + m_2$. This method works very well for privacy preservation for financial scenarios where the transactions are mainly related to addition or subtraction operations on the amount or balance.

Therefore, considering the transaction privacy problem for blockchain, Wang et al. (2017) designed a framework where the Paillier cryptosystem is used to hide the real amount of each transaction, and Commitment Proof is used for checking the validity of the encrypted amount (i.e., ensures that the amount is positive and verifies the trade-off between inputs and outputs). These encrypted transactions are like sealed asset envelopes which can be merged, separated, or used while keeping the amount invisible. However, this method cannot support auditing requirement when using in some fields that need to be regulated and/or supervise.

6. Discussion and future research directions

In this section, we summarize and discuss the methodologies described above. We focus our comparison on the their impact on privacy protection, main disadvantages and their existing implementations. Finally, we discuss some future research directions in the area of privacy preservation of blockchain.

6.1. Summary and discussion

Table 2 summarizes the privacy-preserving methodologies in Section 4 and Section 5 in terms of their security goal, main disadvantages and their practical implementations.

As described above, centralized mixing and decentralized mixing aim to protect the relationship between the sender address and the receiver address with a mixing service. The difference is that the former needs a centralized mixer to do this task while the latter accomplishes the mixing jointly among the participants. However, there are some common disadvantages including: additional delay for waiting to be mixed and no protection for the transaction's content (due to the fixed denomination requirement in a mixing session), and some unique limitations such as the centralized mixer will charge for mixing services and may also be vulnerable in terms of being a single point failure, or in the decentralized one, some participants may destroy the mixing process by rejecting to execute the protocols. Furthermore, the frequency of communications between participants in decentralized mixing will cause high transmission overheads on the network channel, which may limit the scalability of a mixing session.

The ring signature is a typical anonymous signature which can be used to hide the signer's identity. However, as a signature scheme, it does not purposely hide the message to be signed. Furthermore, another limitation for this scheme is the size of signature is proportional to the number of participants, which means the more participants, the more storage and communication costs. Thus, when applied to blockchain, CryptoNote utilizes ring signature, one-time payment and confidential transaction together to protect the sender's (i.e., the signer's) privacy, the receiver's privacy as well as the transaction's content, respectively. Furthermore, in order to keep the size of the transaction within a reasonable range, only a limited number of participants are allowed to engage in the signing stage which may reduce the difficulty of data mining on senders' addresses.

NIZK cooperates with the commitment scheme to provide a comprehensive privacy protection structure for the blockchain such as Zcash. NIZK proof proves the ownership of the coins with an anonymous and unlinkable way. The commitment scheme can hide the transaction content with non-repudiation and non-modifiability. Thus, with these two technologies, Zcash can provide strong anonymity for the users and the highest preservation on transaction content simultaneously without any bound on the size of anonymity set per transaction. However, the NIZK protocol incurs high computation overheads specially in the proof generation phase of zk-SNARKs protocol used in Zcash.

The homomorphic cryptosystem (HC) is a valuable methodology to protect the contents of a transaction, even while computing on the protected data. The Confidential Transaction (CT), used in Bitcoin and Monero, is indeed an homomorphic commitment. The Paillier encryption, an additive homomorphic cryptographic technique, has attracted a lot of interest in the academic world but unfortunately it has not be implemented in practical projects. It may need some time to be applied to blockchain implementations.

As summarized as above, we note that there have been many efforts for protecting privacy in blockchain. These efforts focused mainly on the following aspects:

- Obfuscation on the transaction relationships to resist linking or tracing analysis.
- Hiding the identities of the sender and the receiver via complicated cryptographic primitives.
- Blinding the transaction content whilst retaining the verifiability and computability.

6.2. Future research directions

From a practical perspective, blockchain can consider all the cryptocurrencies (such as Bitcoin, Ethereum) and open source platforms (such as HyperLedger) as a huge incubator, from which it can adapt to different requirements of a range of application areas. However, privacy preservation approaches that have been developed to date are still far from meeting the requirements of some important applications. Hence, we present a few research directions that need further investigation in the future.

1. **Scalable and economy**: As shown in Table 2, both centralized and decentralized mixing methodologies incur an additional waiting delay. The complex cryptographic primitives (e.g., NIZK or MPC used in decentralized mixing methodologies) normally bring about heavy computation and communication overheads. For example, the average running time for proof generation in Zcash is approximately 2 min. Furthermore, we can see that the size of an anonymous transaction signature in CryptoNote is proportional to the number of participants, which means that as the number of participants increases, the storage and communication costs also increase. These high costs limit the scalability of an anonymity set. Therefore, one possible direction is to solve the combinatorial optimization problem among the existing or novel cryptographic primitives and their possible configurations.
2. **Stronger privacy under weaker assumptions**: Another challenge for the methodologies presented above is achieving strong privacy preservation under milder assumptions. For example, the zk-SNARKs protocol used in ZCash inherently requires a trusted third party for setup and initialization of the system; a certain percentage of the participants in decentralized mixing protocols are assumed to be honest so as to resist or mitigate the Sybil attack; the homomorphic cryptosystem assumes that the executives, who use the encrypted or committed data for further computing or verifying, is semi-honest, i.e., they are curious about the contents under the cipher texts but will follow the protocol honestly; for every different smart contract, the Hawk will re-initialized a separate trusted setup process to generate it. From an optimization perspective, one of the potential research directions is to enhance the privacy preservation but without or with only a few trust assumptions.

Table 2
Summary of privacy-preserving methodologies in Section 4 and Section 5.

Methodologies	Security Objectives	Main Disadvantages	Existing Projects
Centralized mixing in Section 4.1.1	Obfuscating transaction relationship	1. Waiting delay 2. Single failure 3. Service fees 4. No protected on transaction content	Mixing Websites, Dash, etc
Decentralized mixing in Section 4.1.2	Decentralized Obfuscating transaction relationship	1. Waiting delay 2. Sybil attack 3. Heavy communication overhead 4. No protected on transaction content	CoinJoin, CoinShuffle, etc
Ring signature in Section 4.2	Hiding tradition origin	1. Limited size of anonymity set 2. Heavy storage overhead 3. No protected on data to be signed 4. No protected on transaction target	⊥
CryptoNote in Section 4.2.2	Hiding tradition relationship and content	1. Limited size of anonymity set 2. Heavy storage overhead	Monero
NIZK in Section 4.3 and Section 5.1	Hidding transaction relationship and content	Heavy computation overhead	Zcoin, Zcash, etc
Commitment in Section 4.3 and Section 5.2.1	Non-repudiation on protected transaction content	Need additional ways for anonymity	Confidential Transaction (CT)
HC in Section 5.2.2	Hidding transaction contents	No support for auditing	⊥

3. **Compatibility**: There are several transaction structures that exist for different application scenarios and requirements, e.g., Bitcoin's Unspent Transaction Outputs (UTXO) architecture and the Ethereum's ACCOUNT architecture. More details are presented in (Nakamoto, 2008; Wood, 2014). Basically, the former is the vital component of cryptocurrency that will be linked by a chain of digital signatures, which is the mostly used structure implemented for the transactions protected by the above methodologies. Although the latter works in a similar way as in the traditional banking world, i.e., addresses' accounts are maintained as a global state and the transactions just independently affect the state these accounts. Unfortunately, none of the existing schemes consider privacy preservation under this transaction structure. Due to its programmable system, Ethereum is considered to be an ideal platform for decentralized applications and is therefore valuable but is a challenge for the privacy preservation methodologies to be compatible with the ACCOUNT architecture.
4. **Legal traceability and accountability**: Privacy protection in the blockchain is a "double-edge sword". On one hand, a well-behaved user would like to maintain his/her identity and action privately. On the other hand, a malicious entity may abuse the privacy protection mechanism for some illegal transaction. Therefore, privacy preservation in blockchain may need to be conditional such that a trusted authority (e.g., Public Security Bureau or Court) can find a way to track a targeted user and collect all the messages he/she has disseminated, while the user's sensitive information is still protected from the public.

7. Conclusion

Recently, blockchain has received considerable attention in decentralized information systems because of its decentralized nature and security feature. It provides a completely different way for storing, sharing and updating data and will play a crucial role in future Internet interactive system (e.g., Internet of Things or supply chain systems). However, the growing need for privacy protections may be a hindrance to emerging blockchain's real applications.

In this context, this survey reviews the existing privacy issues associated with the blockchain network. Then, we present a comprehensive analysis of cryptographic protection mechanisms in terms of both anonymity and transaction privacy. Based on the review and discussions for these mechanisms that achieve privacy protection in the blockchain, we identity future research directions for blockchain's privacy protection.

Acknowledgments

The work was supported in part by the National Key Research and Development Program of China under Grant 2017YFB0802500, in part by the National Natural Science Foundation of China under Grant 61501333, Grant 61572379, Grant 61472287, and Grant 61772377, and in part by the Natural Science Foundation of Hubei Province of China under Grant 2017CFA007 and Grant 2015CFA068. We thank the anonymous reviewers for the valuable comments and suggestions which helped us improve the content, organization, and presentation of this paper.

References

Abeyratne, S.A., Monfared, R.P., 2016. Blockchain Ready Manufacturing Supply Chain Using Distributed Ledger.
Ali, M., Nelson, J.C., Shea, R., Freedman, M.J., 2016. Blockstack: a global naming and storage system secured by blockchains. In: USENIX Annual Technical Conference, pp. 181–194.
Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T., Capkun, S., 2013. Evaluating user privacy in bitcoin. In: International Conference on Financial Cryptography and Data Security. Springer, pp. 34–51.
Barber, S., Boyen, X., Shi, E., Uzun, E., 2012. Bitter to betterhow to make bitcoin a better currency. In: International Conference on Financial Cryptography and Data Security. Springer, pp. 399–414.
Binded - copyright made simple. https://binded.com/.
Biryukov, A., Pustogarov, I., 2015. Bitcoin over tor isn't a good idea. In: Security and Privacy (SP), 2015 IEEE Symposium on. IEEE, pp. 122–134.
Bissias, G., Ozisik, A.P., Levine, B.N., Liberatore, M., 2014. Sybil-resistant mixing for bitcoin. In: the Workshop on Privacy in the Electronic Society, pp. 149–158.
Bitblender. https://bitblender.io/.
Bitcoin fog. http://bitcoinfog.com.
Bitcoin. https://bitcoin.org/en/.
BitInfoCharts, 2017. Bitcoin (Btc) Price Stats and Information. Website. https://bitinfocharts.com/bitcoin/.
Bitlaundry. http://app.bitlaundry.com.
Bitmixer. https://bitcointalk.org/index.php?topic=415396.160.
Bitcoinwiki. change. https://en.bitcoin.it/wiki/Change.
Blum, M., Feldman, P., Micali, S., 1988. Non-interactive zero-knowledge and its applications. In: Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing. ACM, pp. 103–112.
Bonneau, J., Narayanan, A., Miller, A., Clark, J., Kroll, J.A., Felten, E.W., 2014. Mixcoin: anonymity for bitcoin with accountable mixes. In: International Conference on Financial Cryptography and Data Security. Springer, pp. 486–504.
Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J.A., Felten, E.W., 2015. Sok: research perspectives and challenges for bitcoin and cryptocurrencies. In: Security & Privacy, pp. 104–121.
Castro, M., Liskov, B., et al., 1999. Practical byzantine fault tolerance. In: OSDI, vol. 99, pp. 173–186.
Chaum, D.L., 1981. Untraceable electronic mail, return addresses, and digital pseudonyms. Commun. ACM 24 (2), 84–90.
Cohn, J.M., Finn, P.G., Nair, S.P., Panikkar, S.B., Pureswaran, V.S., 2017. Autonomous Decentralized Peer-to-peer Telemetry.

Conoscenti, M., Vetrò, A., De Martin, J.C., 2016. Blockchain for the Internet of Things: a Systematic Literature Review.
Dash is digital cash. https://www.dash.org//.
Decred - autonomous digital currency. https://www.decred.org/.
Delmolino, K., Arnett, M., Kosba, A., Miller, A., Shi, E., 2016. Step by step towards creating a safe smart contract: lessons and insights from a cryptocurrency lab. In: International Conference on Financial Cryptography and Data Security. Springer, pp. 79–94.
Dorri, A., Kanhere, S.S., Jurdak, R., 2016. Blockchain in Internet of Things: Challenges and Solutions. arxiv:1608.05187.
A. Ebrahimi, "Identity Management Service Using a Blockchain Providing Certifying Transactions between Devices," Aug. 1 2017. US Patent 9,722,790.
Ethereum project. https://www.ethereum.org/.
Factom - making the world's systems honest. https://www.factom.com/.
Feld, S., Schönfeld, M., Werner, M., 2014. Analyzing the deployment of bitcoin's p2p network under an as-level perspective. Proced. Comput. Sci. 32, 1121–1126.
Fromknecht, C., Velicanu, D., Yakoubov, S., 2014. A decentralized public key infrastructure with identity retention. IACR Cryptol. ePrint Arch. 2014, 803.
Fujisaki, E., 2011. Sub-linear size traceable ring signatures without random oracles. In: CT-RSA, vol. 11. Springer, pp. 393–415.
Fujisaki, E., Suzuki, K., 2007. Traceable ring signature. In: Public Key Cryptography, vol. 4450. Springer, pp. 181–200.
Genkin, D., Papadopoulos, D., Papamanthou, C., 2018. Privacy in decentralized cryptocurrencies. Commun. ACM 61 (6), 78–88.
Gill, M., Taylor, G., 2004. Preventing money laundering or obstructing business? financial companies' perspectives on know your customerprocedures. Br. J. Criminol. 44 (4), 582–594.
Greenberg, A., 2014. Dark Walletis about to Make Bitcoin Money Laundering Easier than Ever. http://www.wired.com/2014/04/darkwallet.
Halim, N.S.B.A., Rahman, M.A., Azad, S., Kabir, M.N., 2017. Blockchain security hole: issues and solutions. In: International Conference of Reliable Information and Communication Technology, pp. 739–746.
Heilman, E., Baldimtsi, F., Goldberg, S., 2016. Blindly signed contracts: anonymous on-blockchain and off-blockchain bitcoin transactions. In: International Conference on Financial Cryptography and Data Security. Springer, pp. 43–60.
Heilman, E., Alshenibr, L., Baldimtsi, F., Scafuro, A., Goldberg, S., 2017. Tumblebit: An untrusted bitcoin-compatible anonymous payment hub. In: Network and Distributed System Security Symposium.
Helix by grams. https://grams7enufi7jmdl.onion.link/helix.
Huh, S., Cho, S., Kim, S., 2017. Managing iot devices using blockchain platform. In: Advanced Communication Technology (ICACT), 2017 19th International Conference on. IEEE, pp. 464–467.
Hyperledger projects. https://www.hyperledger.org/.
Joinmarket - Coinjoin that People Will Actually Use, 2015. Bitcoin Talk, https://bitcointalk.org/index.php?topic=919116.msg10096563.
Kim, H.M., Laskowski, M., 2016. Towards an Ontology-driven Blockchain Design for Supply Chain Provenance.
Knirsch, F., Unterweger, A., Eibl, G., Engel, D., 2017. Pprivacy-preserving smart grid tariff decisions with blockchain-based smart contracts. Sustain. Cloud Energy Serv. 85–116.
Knirsch, F., Unterweger, A., Engel, D., 2018. Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions. Comput. Sci. Res. Dev. 33 (1–2), 71–79.
Korpela, K., Hallikas, J., Dahlberg, T., 2017. Digital supply chain transformation toward blockchain integration. In: Proceedings of the 50th Hawaii International Conference on System Sciences.
Kosba, A., Miller, A., Shi, E., Wen, Z., Papamanthou, C., 2016. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts. In: Security and Privacy (SP), 2016 IEEE Symposium on. IEEE, pp. 839–858.
Koshy, P., Koshy, D., McDaniel, P., 2014. An analysis of anonymity in bitcoin using p2p network traffic. In: International Conference on Financial Cryptography and Data Security. Springer, pp. 469–485.
Kuan, H.-H., Chen, R.-J., 2017. Denial of Service Resistance for Bitcoin Mixing Method Tumblebit. http://hdl.handle.net/11536/142102.
Li, X., Jiang, P., Chen, T., Luo, X., Wen, Q., 2017. A survey on the security of blockchain systems. Future Generat. Comput. Syst., https://doi.org/10.1016/j.future.2017.08.020.
Liao, K., Zhao, Z., Doupé, A., Ahn, G.-J., 2016. Behind closed doors: measurement and analysis of cryptolocker ransoms in bitcoin. In: Electronic Crime Research (ECrime), 2016 APWG Symposium on, IEEE, pp. 1–13.
Litecoin - open source p2p digital currency. https://litecoin.org/.
Liu, J.K., Wei, V.K., Wong, D.S., 2004. Linkable spontaneous anonymous group signature for ad hoc groups. In: ACISP, vol. 4. Springer, pp. 325–335.
Maidsafe - the New Decentralized Internet. https://www.maidsafe.net/.
Maxwell, G., 2013a. Coinswap: Transaction Graph Disjoint Trustless Trading. CoinSwap: Transactiongraphdisjointtrustlesstrading (October 2013).
Maxwell, G., 2013b. Coinjoin: bitcoin privacy for the real world. In: Post on Bitcoin Forum.
Maxwell, G., 2015. Confidential transactions. https://people.xiph.org/%7egreg/confidential%20values.txt. (Accessed 9 May 2016).
Meiklejohn, S., Orlandi, C., 2015. Privacy-enhancing Overlays in Bitcoin. Springer Berlin Heidelberg.
Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M., Savage, S., 2013. A fistful of bitcoins: characterizing payments among men with no names. In: Proceedings of the 2013 Conference on Internet Measurement Conference. ACM, pp. 127–140.
Miers, I., Garman, C., Green, M., Rubin, A.D., 2013. Zerocoin: anonymous distributed e-cash from bitcoin. In: IEEE Symposium on Security and Privacy, pp. 397–411.
Monero project. https://getmonero.org/.
Nakamoto, S., 2008. Bitcoin: a Peer-to-peer Electronic Cash System.
Noether, S., Mackenzie, A., et al., 2016. Ring confidential transactions. Ledger 1, 1–18.
Onionbc. http://6fgd4togcynxyclb.onion/.
Paillier, P., et al., 1999. Public-key cryptosystems based on composite degree residuosity classes. In: Eurocrypt, vol. 99. Springer, pp. 223–238.
Pedersen, T.P., et al., 1991. Non-interactive and information-theoretic secure verifiable secret sharing. In: Crypto, vol. 91. Springer, pp. 129–140.
Pilkington, M., 2016. 11 Blockchain Technology: Principles and Applications. Research handbook on digital transformations, p. 225.
Qin, B., Huang, J., Wang, Q., Luo, X., Liang, B., Shi, W., 2017. Cecoin: a decentralized pki mitigating mitm attacks. Future Generat. Comput. Syst., https://doi.org/10.1016/j.future.2017.08.025.
Reid, F., Harrigan, M., 2013. An analysis of anonymity in the bitcoin system. In: Security and Privacy in Social Networks. Springer, pp. 197–223.
Rivest, R., Shamir, A., Tauman, Y., 2001. How to leak a secret. In: Advances in CryptologyASIACRYPT 2001, pp. 552–565.
Ron, D., Shamir, A., 2013. Quantitative analysis of the full bitcoin transaction graph. In: International Conference on Financial Cryptography and Data Security. Springer, pp. 6–24.
Ruffing, T., Moreno-Sanchez, P., Kate, A., 2014. Coinshuffle: practical decentralized coin mixing for bitcoin. In: European Symposium on Research in Computer Security, pp. 345–364.
Sasson, E.B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M., 2014. Zerocash: decentralized anonymous payments from bitcoin. In: IEEE Symposium on Security and Privacy, pp. 459–474.
Schott, P.A., 2006. Reference Guide to Anti-money Laundering and Combating the Financing of Terrorism. World Bank Publications.
Send shared. https://blockchain.info/de/wallet/send-shared.
J. Siim, "Proof-of-stake,".
Spagnuolo, M., Maggi, F., Zanero, S., 2014. Bitiodine: extracting intelligence from the bitcoin network. In: International Conference on Financial Cryptography and Data Security. Springer, pp. 457–468.
Sun, S.-F., Au, M.H., Liu, J.K., Yuen, T.H., 2017. Ringct 2.0: a compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero. In: European Symposium on Research in Computer Security. Springer, pp. 456–474.
Swan, M., 2015. Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc.
Szabo, N., 1997. Formalizing and securing relationships on public networks. Clin. Hemorheol. and Microcirc. 2 (9).
Tapscott, D., Tapscott, A., 2016. Blockchain Revolution: How the Technology behind Bitcoin Is Changing Money, Business, and the World. Penguin.
Tor project. https://www.torproject.org/.
Underwood, S., 2016. Blockchain beyond bitcoin. Commun. ACM 59 (11), 15–17.
Valenta, L., Rowan, B., 2015. Blindcoin: blinded, accountable mixes for bitcoin. In: International Conference on Financial Cryptography and Data Security. Springer, pp. 112–126.
van Saberhagen, N., 2013. Cryptonote V 2. 0.
Vandervort, D., 2014. Challenges and opportunities associated with a bitcoin-based transaction rating system. In: International Conference on Financial Cryptography and Data Security. Springer, pp. 33–42.
Vornberger, J., 2012. Marker addresses: adding identification information to bitcoin transactions to leverage existing trust relationships. In: GI-jahrestagung, pp. 28–38.
Wang, Q., Qin, B., Hu, J., Xiao, F., 2017. Preserving transaction privacy in bitcoin. Future Generat. Comput. Syst., https://doi.org/10.1016/j.future.2017.08.026.
Wiki. coinbase. https://en.wikipedia.org/wiki/Coinbase.
Wood, G., 2014. Ethereum: a Secure Decentralised Generalised Transaction Ledger. Ethereum Project Yellow Paper, vol. 151.
Ylihuumo, J., Ko, D., Choi, S., Park, S., Smolander, K., 2016. Where is current research on blockchain technology?a systematic review. PloS One 11 (10), e0163477.
Zerocash — zerocash. http://zerocash-project.org/.
Zheng, Z., Xie, S., Dai, H.N., Wang, H., 2016. Blockchain Challenges and Opportunities: a Survey.
Ziegeldorf, J.H., Grossmann, F., Henze, M., Inden, N., Wehrle, K., 2015. Coinparty: Secure multi-party mixing of bitcoins. In: Proceedings of the 5th ACM Conference on Data and Application Security and Privacy. ACM, pp. 75–86.

Qi Feng received the Bachelor degree in 2016 and the Master degree in 2018, both from the School of Computer Science, Wuhan University, China. She is currently working toward a Ph.D. degree at with the Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan, China. Her research interests include cryptographic protocols.

Debiao He received his Ph.D. degree in applied mathematics from School of Mathematics and Statistics, Wuhan University in 2009. He is currently a professor of the Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University. His main research interests include cryptography and information security, in particular, cryptographic protocols.

Sherali Zeadally received his Bachelor degree from the University of Cambridge, Cambridge, England in 1991, and the Doctorate degree from the University of Buckingham, Buckingham, England in 1996, both in computer science. He is an Associate Professor in the College of Communication and Information, University of Kentucky, Lexington, KY, USA. He is a Fellow of the British Computer Society and the Institution of Engineering Technology, England.

Muhammad Khurram Khan is one of the Founding Members of the Center of Excellence in Information Assurance (CoEIA) and has served as the Manager of research and development from 2009 to 2012. He developed and successfully managed the research program of CoEIA, which transformed the center as one of the best centers of research excellence in Saudi Arabia as well as in the region. He is currently a Full Professor with CoEIA, King Saud University, Saudi Arabia. Khurram Khan has been the Editor-in-Chief of a well-esteemed ISI-indexed international journal Telecommunication Systems (Springer-Verlag) since 1993 with an impact factor of 1.542 (JCR, 2016). He is a Founding Editor of the Bahria University Journal of Information and Communication Technology. Furthermore, he is also a full-time Editor/Associate Editor of several ISI-indexed international journals/magazines, including the IEEE Communications Surveys and Tutorials, IEEE Communications Magazine, the Journal of Network and Computer Applications (Elsevier), the IEEE Transactions on Consumer Electronics, the IEEE Access, Security and Communication Networks, IEEE Consumer Electronics Magazine, the Journal of Medical Systems (Springer), PLOS One, Computers & Electrical Engineering (Elsevier), IET Wireless Sensor Systems, Electronic Commerce Research (Springer), the Journal of Computing and Informatics, the Journal of Information Hiding and Multimedia Signal Processing, the International Journal of Biometrics (Inderscience), and so on. He is also an Adjunct Professor with the Fujian University of Technology, China, and an Honorary Professor with IIIRC, Shenzhen Graduate School,Harbin Institute of Technology, China. He received the Outstanding Leadership Award from the IEEE International Conference on Networks and Systems Security, Australia, in 2009. He has been included in the Marquis Who's Who in the World 2010 edition. Besides, he has received certificate of appreciation for outstanding contributions in Biometrics & Information Security Research at the AIT international Conference, Japan, in 2010. He received the Gold Medal for the Best Invention and Innovation Award at the 10th Malaysian Technology Expo 2011, Malaysia. Moreover, his invention recently received the Bronze Medal at the 41st International Exhibition of Inventions, Geneva, Switzerland, in 2013. In addition, he received the Best Paper Award from the Journal of Network and Computer Applications (Elsevier) in 2015. He has played a leading role in developing the B.S. Cybersecurity Degree Program and the Higher Diploma in cybersecurity with King Saud University. He has secured several national and international research grants in the domain of information security. He has edited seven books/proceedings published by Springer-Verlag and the IEEE. He has published over 300 research papers in the journals and conferences of international repute. In addition, he is an inventor of 10 U.S./PCT patents. His research areas of interest are cybersecurity, digital authentication, biometrics, multimedia security, and technological innovation management. He is a fellow of IET (U.K.), BCS (U.K.), FTRA (South Korea), and a member of the IEEE Technical Committee on Security and Privacy and the IEEE Cybersecurity Community. He was a recipient of the King Saud University Award for Scientific Excellence (Research Productivity) in 2015, and the King Saud University Award for Scientific Excellence (Inventions, Innovations, and Technology Licensing) in 2016.

Neeraj Kumar received his Ph.D. in CSE from Shri Mata Vaishno Devi University, Katra, India in 2009. He is currently an Associate Professor in the Department of Computer Science and Engineering, Thapar University, Patiala, India. He has guidedmany students leading to M.E. and Ph.D. He has more than 200 technical research papers in leading journals such as IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, the IEEE TRANSACTIONS ON POWER SYSTEMS, IEEE Transactions on Cloud Computing, IEEE Transaction on Information Forensics and Security, IEEE Transactions on Smart Grid, IEEE SYSTEMS JOURNAL, IEEE Communications Magazine, IEEE Wireless Communications Magazine, the IEEE Network Magazine, and conferences including IEEE ICC, IEEE Globecom etc. His research is supported by Department of Science and Technology, Tata Consultancy Services, and University Grants Commission. His research interests include mobile computing, parallel/distributed computing, multiagent systems, service oriented computing, routing, and security issues in mobile ad hoc, sensor, and mesh networks. He is associate editor of JNCA, Elsevier, IJCS, Wiley and Security and Privacy, Wiley.