Fang *et al. EURASIP Journal on Wireless Communications and Networking* (2020) 2020:56
https://doi.org/10.1186/s13638-020-01665-w

EURASIP Journal on Wireless Communications and Networking

REVIEW Open Access

Digital signature scheme for information non-repudiation in blockchain: a state of the art review

Weidong Fang[1,2], Wei Chen[3*], Wuxiong Zhang[1,2,4], Jun Pei[1], Weiwei Gao[1,2] and Guohui Wang[1]

Abstract

Blockchain, as one of the most promising technology, has attracted tremendous attention. The interesting characteristics of blockchain are decentralized ledger and strong security, while non-repudiation is the important property of information security in blockchain. A digital signature scheme is an effective approach to achieve non-repudiation. In this paper, the characteristics of blockchain and the digital signature to guarantee information non-repudiation are firstly discussed. Secondly, the typical digital signature schemes in blockchain are classified and analyzed, and then the state-of-the-art digital signatures are investigated and compared in terms of application fields, methods, security, and performance. Lastly, the conclusions are given, and some future works are suggested to stir research efforts in this field. Our works will facilitate to design efficient and secure digital signature algorithms in blockchain.

Keywords: Blockchain, Cyber security, Non-repudiation, Digital signature

1 Introduction

Currently, as the key technology behind Bitcoin, the blockchain has been widely researched and deployed [1]. It provides a decentralized mechanism and infrastructure in different fields [2–5] and maintains a chronologically continuous, non-tamperable data record. Meanwhile, it is also a research hotspot [6–9]. When assets in the real or digital world can generate digital digests, the blockchain becomes the perfect vehicle for the application of the assertion class, to provide digital evidence of ownership and timestamps. Hence, the blockchain can be applied in many fields [10], which involve online payment, stock exchange, trade management, and IoT. Blockchain technology not only serves as the technical basis for all digital cryptocurrencies, but also extends broader developments and applications in traditional finance and trade. Furthermore, it also opens the door to new technologies such as smart contracts [11].

With the development of blockchain, the issues of hard fork and double payment [12], which are caused by block conflicts, will directly impact on the validity and integrity of E-commerce transactions. The essence of these issues is information security, in short, whether it is the consensus process in the face of 51% attack [13, 14], the Byzantine failures or in the future on the asymmetric encryption algorithm, as well as those attacks from outside rivals and transaction information forgery, or there are the personal privacy leakage and the software design flaws. The non-repudiation of information is very important for the security in blockchain. In order to guarantee the non-repudiation of information in the blockchain system, some security technologies, such as digital signature [15], identity authentication, and time stamping [16] are studied and applied.

Digital signatures can be used to verify the integrity of a file or a message. It is non-repudiation. In Fig. 1, a typical digital signature process is given basic on RSA. It is one of the digital signature algorithms, which are widely used [17]. Digital signature technology can be well adapted to its characteristics in the blockchain system. It will be more secure and applicable than the traditional application field and has the

* Correspondence: chenwdavior@163.com
[3]School of Computer Science and Technology, China University of Mining and Technology, Xuzhou 221116, China
Full list of author information is available at the end of the article

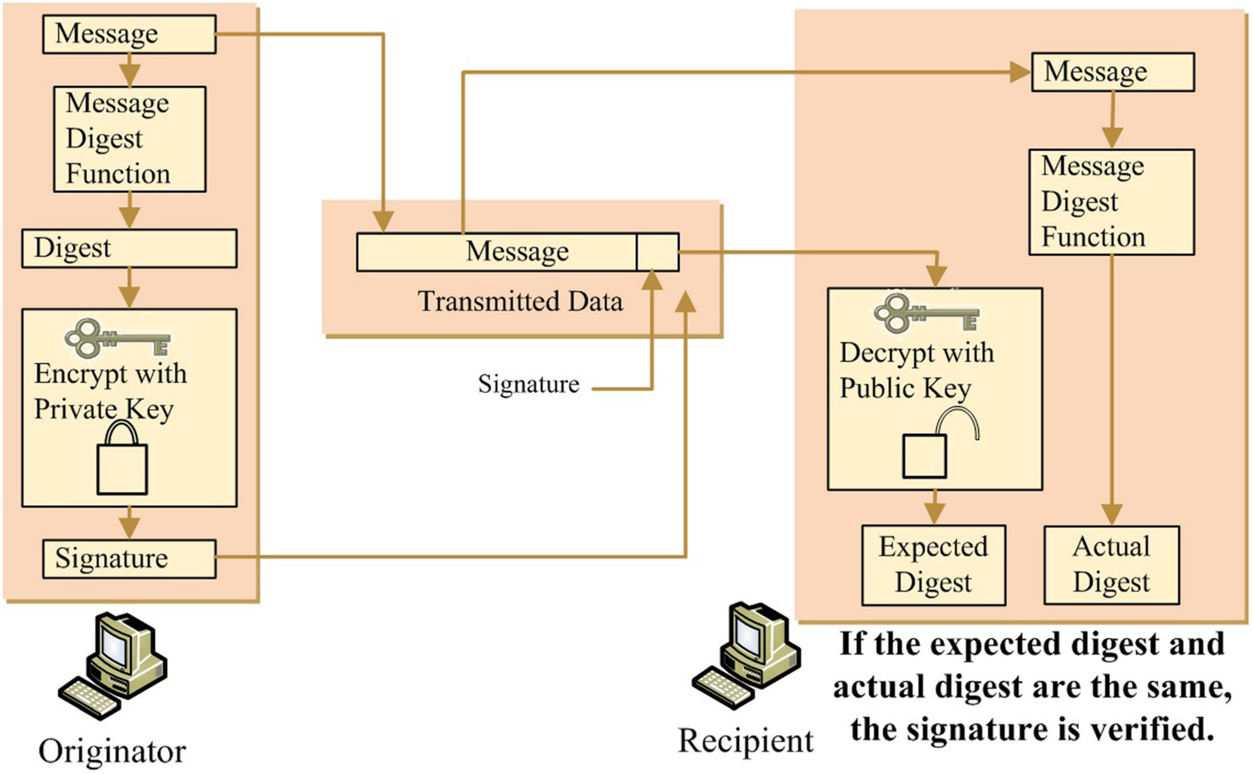
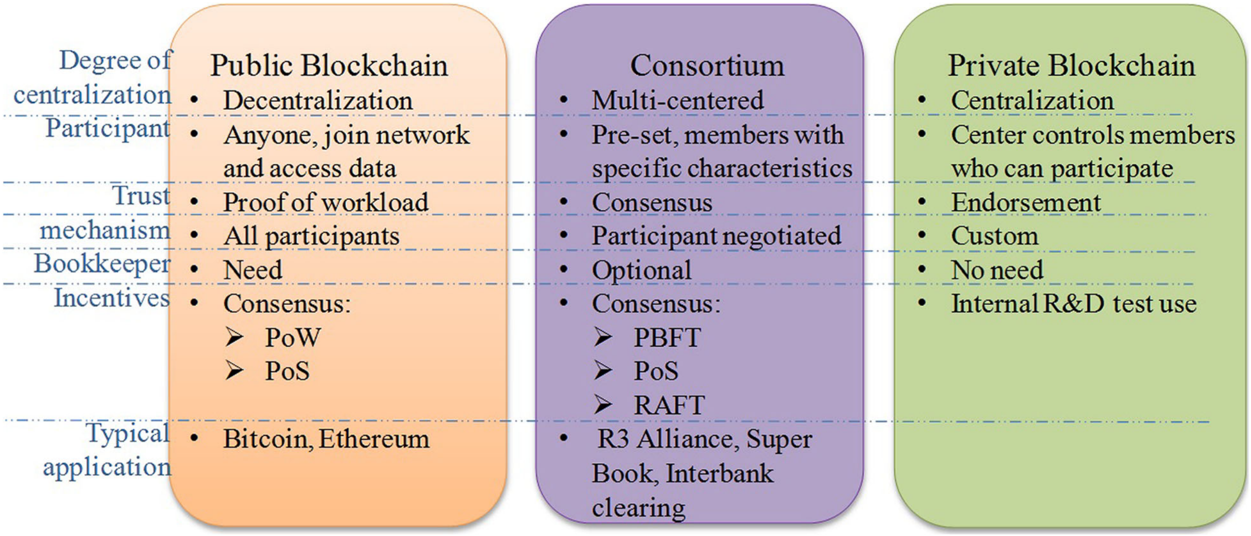


Fig. 1 Data security digital signature process basic on RSA

possibility of increasing value. For example, digital signature only carries information on the Internet, but has no value transfer.

In blockchain system, there is not only information transmission, but also the transfer of value. In such a context, our contributions of this paper include the following:

1) Digital signature schemes to guarantee the non-repudiation of information in blockchain, as well as



	Public Blockchain	Consortium	Private Blockchain
Degree of centralization	• Decentralization	• Multi-centered	• Centralization
Participant	• Anyone, join network and access data	• Pre-set, members with specific characteristics	• Center controls members who can participate
Trust mechanism	• Proof of workload	• Consensus	• Endorsement
	• All participants	• Participant negotiated	• Custom
Bookkeeper	• Need	• Optional	• No need
Incentives	• Consensus: ➢ PoW ➢ PoS	• Consensus: ➢ PBFT ➢ PoS ➢ RAFT	• Internal R&D test use
Typical application	• Bitcoin, Ethereum	• R3 Alliance, Super Book, Interbank clearing	

Fig. 2 Blockchain classification

the state-of-the-art works in digital signatures are reviewed, analyzed, and compared systematically, in order to facilitate the design and optimization of signature algorithms.

2) Future research directions on digital signature are suggested so as to provide possible opportunities for this research field.

The rest of this paper is organized as follows. Firstly, the blockchain and non-repudiation are discussed in Section 2. Then, the digital signature schemes are analyzed in Section 3. Furthermore, the related works are reviewed and compared in detail in Section 4. Finally, the conclusions and future works are given in Section 5.

2 Blockchain and non-repudiation

2.1 Blockchain

The concept of blockchain was originally proposed by Nakamoto in 2008 [18], and now has become the core technology of Bitcoin. In the original text, the terms “block” and “chain” were used separately at the earliest stage and were used as blockchain after being widely used. The block is a recorded Bitcoin transaction data unit, which consists of two parts: one is the block header, and the other is the block content. It is not until 2016 that the word “blockchain” has been synthesized. Generally, the blockchain can be categorized into as follows: Public Blockchain, Consortium, and Private Blockchain. In addition, different blockchains can also form a network, and the links and the chains in the same network are interconnected to generate an interchain [13]. The relationship of blockchain classification is shown in Fig. 2.

The blockchain has some features, including decentralization, openness, self-control, untamperability, and anonymity [19]. The core technologies in blockchains involve asymmetric encryption, P2P, distributed ledger, consensus mechanism, and smart contract [20]. Many traditional security schemes and algorithms [21–26] are deployed in blockchains. With the development of the blockchain, it has also merged with a series of new information technologies, such as IoT, cloud computing, and big data and is becoming the support of infrastructures. Meanwhile, it also plays an important role in promoting the development of a new-generation information technology. By using the blockchain, up to military-grade security can be achieved with typical devices in IoT [27]. Furthermore, many researchers have done a series of works to observe whether it is well suited to the IoT. They also describe how blockchain and IoT are integrated closely, such as facilitating the sharing of services and resources, establishing a service market between devices, and allowing users to automate the encryption and authentication process in the time-consuming workflow of several existing units. Finally, according to the research results, they show that combining blockchain and IoT is quite optimistic. The combination can promote the development of a number of industries, can drive major reforms and innovations across multiple fields of industry, and, furthermore, also can pave the way for new business models and new distributed applications [28].

2.2 Non-repudiation

Non-repudiation means that participants cannot deny the transaction and behavior in the transaction of E-commerce in the blockchain. The purpose of non-repudiation service is to collect, maintain, provide, and verify the undeniable evidence about messages from the transmitter to the receiver. The non-repudiation service may involve the services of the trusted third party, called the delivery authority (DA) [29]. In blockchain, the non-repudiation involves two aspects: one is that the sent information cannot be denied, for example, A sent a message to B, so A cannot deny the behavior. The other is the information receiver cannot be denied. Similarly, A sent to B a message, but B cannot claim that he did not receive this message. Digital signatures in blockchain systems use asymmetric encryption techniques that are typical of elliptic curve equations [30] to guarantee the non-repudiation of information.

For example, a digital signature for Bitcoin is achieved by using elliptic curves and modular arithmetic in finite fields [31]. It allows non-repudiation, as it means the person who sent the message had to be in possession of the private key. Therefore, owns the Bitcoins—anyone on the network can verify the transaction as a result. The Bitcoin digital signature is shown in Fig. 3.

3 Digital signature

In this section, we will survey and analyze several typical digital signature schemes in blockchain. These signature schemes include aggregate signature, group signature, ring signature, blind signature, and proxy signature.

3.1 Aggregate signature

An aggregate signature [32] is a typical digital signature scheme with aggregation function based on co-GDH and bilinear mapping. The meaning of aggregation is given n signatures on n different messages from n different users, and it is possible to summarize all these signatures into a short signature. This brief single signature (n original messages) will convince the verifier that the n users do indeed sign n messages (e.g., user i signs message M_i from i = 1 to n).

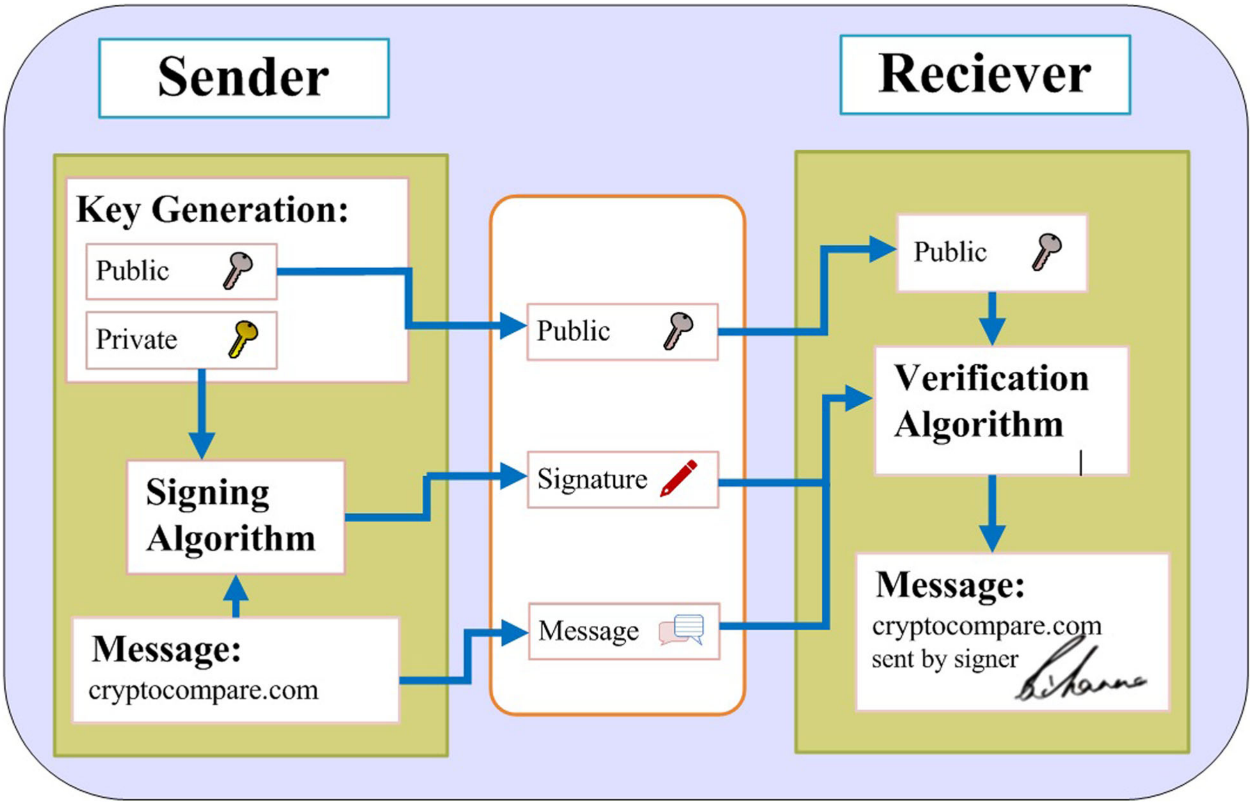


Fig. 3 A Bitcoin digital signature diagram

The aggregate signatures greatly reduce the workload of signature storage and signature verification. In practice, the computational and communication costs can be reduced. It is usually used in environments where bandwidth and storage space are limited.

3.2 Group signature

A group signature [33] scheme allows members in a group to anonymously represent group signed messages. The security elements formed by group signatures must comply with the following eight requirements: reliability and integrity, unforgeable, anonymity, traceability, unlinkability, no framing, unforgeable tracing verification, and coalition resistance.

Due to the differences in blockchain application scenarios, the execution efficiency of the group signature scheme becomes critical. Generally, the execution efficiency of the group signature mechanism can be evaluated by the length of the group signature, the size of the public key, the time of signature generation, and the verification time.

3.3 Ring signature

A ring signature scheme [34] uses the public key of all users on a set U and a single private key of a user on U. Considering the feature of the ring signature, it can be deployed to the anonymous payment applications or the transactions that need the untraceability. The signature scheme has no trusted center, the signer is in a completely anonymous state, and there are significant special cases in which the information needs long-term protection. This signature scheme has better security. For attacker A, even if he has private keys of all members, he cannot determine the specific signer. The probability that the real signer is determined is $1/n$ (n is the total number of ring members), and A cannot generate the ring signature of the message from all kinds of non-negligible probability. Generally, a good ring signature must meet the following security requirements:

- Unconditional anonymity. Even if an attacker illegally obtains the private key of all possible signers, he can determine that the probability of the true signer does not exceed $1/n$.
- Unforgeability. If an external attacker does not know any member's private key, even if he can get the signature of any message m from a random predictor that generates a ring signature, the probability that he successfully forged a legitimate signature is negligible.

- The signer can freely specify his own anonymous scope, can constitute a beautiful circular logical structure, and can realize the main function of group signature but does not need a trusted third party or group administrator.

3.4 Blind signature

A blind signature [35] is based on the problem of large number factor de-composition, discrete logarithm problem, and elliptic curve. It is characterized by the fact that the message is disguised before it is signed. Typically, it is used where the transmitter's privacy is very important, for example, it is used in the privacy-related protocol where the signer and the message author are different. In blockchain applications, the blind signature is often used for encrypted election systems and digital cash plans. In addition to satisfying the general digital signature conditions, blind signatures must also satisfy the following two properties:

- The signer is invisible to the message he signed, namely the signer does not know the specific content of the message he signed.
- The signed message is not traceable, that is, when the signed message is published, the signer cannot know which one he signed.

3.5 Proxy signature

The proxy signature [36] allows a designated signer, called as a proxy signer, to represent an original signer. Proxy signature is based on the discrete logarithm problem. Compared with the continuous execution of ordinary digital signature schemes, the proxy signature has a direct form. The verifier does not need the public key of the user other than the original signer in the verification process. In terms of performance, it requires less computational cost than the continuous execution of a general signature scheme.

Essentially speaking, the proxy signature in blockchain is that the original signer authorizes his signature to the proxy signer and then causes the proxy signer to generate a valid signature on behalf of the original signer. It contains the following sections:

- Initialization process (e.g., signature system parameters, user's key);
- Power delegation process;
- Process of generating a proxy signature;
- Verification process of the proxy signature.

The comparisons of five typical digital signatures in blockchain are shown in Table 1. Digital signatures are implemented to achieve the identification of digital information by using public-key cryptography. A set of digital signatures usually defines two complementary operations, one for signature and one for verification. To put it simply, only a string of digits that cannot be forged by someone else can be generated by the transmitter of the message. This string of digits is also a valid proof of the authenticity of the information sent by the sender of the message. In the distributed network of blockchains, communication and trust between nodes rely on digital signature technology. It mainly implements information non-repudiation, identity verification, as well as information authenticity, and integrity verification.

4 Related work and comparison

In this section, we will systematically review some state-of-the-art digital signature schemes, which are deployed in blockchain. Then, we give a comparative analysis of the mentioned signature schemes, in terms of application fields, methods, security, and performance.

Zhu et al. [37] proposed an IIS, which could protect the owner's information from being falsified and the trader's information could not be denied. This signature protocol was mainly used to build a blockchain system that was more accurate and had higher performance than existing blockchain systems. As the core of this system, IIS could ensure that the transaction was confirmed by the dealer and was undeniable. With this signature, the merchant could assure the owner that the transaction would be included in the blockchain system in an undeniable manner. The signature scheme proved to be a security guarantee for the owner's unforgeability and the merchant's non-repudiation. This scheme solved the problem of ensuring instant confirmation of non-repudiation during blockchain implementation.

Tian et al. [38] proposed a BVES based on traditional verifiable cryptographic signatures and blind signature ideas. Since each node of the blockchain could read transaction data during the transaction to verify that the transaction data was correct, but the transaction data involved the content of privacy. Therefore, either the contradiction arose or the privacy was protected. It was difficult to design a fair contract-signing agreement that protected privacy on the blockchain. They built a fair and confidential contract signing agreement based on this signature system, which not only allowed contract signers to complete fair contract signing through the blockchain, but also protected the privacy content related to the contract. This new blind verifiable cryptographic signature system effectively protected contract-related privacy content in the event of a transaction being disclosed.

Sato et al. [39] pointed out how the security of blockchain information would be affected when the underlying encryption algorithm (hash function and digital signature) compromised. If compromise occurred in

Table 1 Comprehensive comparisons of five digital signatures in blockchain

Digital signatures	Principle	Security	Performances
Aggregate signature (AS)	Based on co-GDH and bilinear mapping	The security in AS is mainly guaranteed by the bilinear mapping and the trapdoor permutation. AS has the ability to detect the attackers' forged signature.	Verification time of AS is linear with the number of signatures. In special cases, when all *n* signatures are generated by the same public key *k*, verification speed in AS is faster. Meanwhile, the workload of signature storage and verification are reduced.
Group signature (GS)	Based on non-repudiation signature	Reliability and integrity, unforgeability, anonymity, traceability, no correlation, no framework, and defense against joint attack.	The length of the public key, the length of signature, and the number of group members have a linear relationship and impact on GS performance. GS is not suitable for a large group. A new member needs to restart the entire system, when it enters. Fortunately, zero-knowledge proof is an effective approach to improve GS.
Ring signature (RS)	Variant of group signature. Two ring signatures based on RSA and Labin versions	Untraceability and anonymity. The attacker cannot find who the specific signer is. Even if he has the private keys of all ring members. This is due to that the probability of determining the real signer is 1/*n* (*n* is the number of ring members).	In essence, RS is a series of cryptographic transformations by using a public key, a private key, and the information to be signed. It signature process and the verification process is similar to a regular signature for each non-signer, RS runs efficiently even if there are hundreds of members in a ring.
Blind signature (BS)	Based on RSA or DSA	Blindness, non-repudiation, anonymity, and untraceability, if the signer is not the sender of the message, the BS can hide the message *m* by blinding, the signer cannot obtain the *m* content, thereby protecting the *m* privacy.	Performance of BS depends on the key length, the signature length, and the signature and verification algorithms. Although there are different performances with different signature algorithms, generally speaking, the overhead of BS is similar to the RSA signature or DSA signature scheme. The BS using RSA is applicable for the signatures of small data.
Proxy signature (PS)	Based on discrete logarithm	Identifiability and traceability. Due to the inherent characteristics of the discrete logarithm problem, agents can forge the original signature to launch the security attacks, or replace the public key.	The overheads of communication and computing in PS are larger. PS is inferior to the signature schemes based on the elliptic curve in terms of computational complexity and communication overhead.

SHA256, it would result in stolen electronic money, double payment, and failure to complete the agreement; when RIPEMD160 compromises, it would result in a denial of payment; when ECDSA compromised, it would result in currency theft and send a false alarm claims No payment was received; the hash function and the digital signature scheme produced compromises that, when combined, resulted in denied transactions, currency theft, double payments, and changes to existing transaction data. In order to solve the security problems in the blockchain, they proposed how to use a long signature scheme like the ETSI [40] standard and did not require the TTP mechanism. Through the research and analysis, it was found that the change of the key pair and the bifurcation could not be avoided when the signature scheme was compromised, but the additional blockchain could be used in a certain period of time (within a few years) through the protocol proposed by the researchers.

Aitzhan et al. [41] solved the problem of providing transaction security in decentralized smart grid energy trading without relying on trusted third parties. The concept validation of the decentralized energy trading system was implemented through blockchain technology, multiple signatures, and anonymously encrypted information flows. It enabled peers to anonymously negotiate energy prices and conducted transactions securely. Because they replicated between all active nodes, the system used P2P community data replication methods to protect transactions from failure. In addition, the use of workload proofs, such as Bitcoin, allowed the system to overcome the Byzantine general problem and to defend against any double payment attack that occurred in electronic payment systems.

Yuan et al. [42] proposed that privacy protection and blockchain performance were two research hotspots in academia and business fields, but there were still some unsolved problems in these two aspects. They designed a new signature scheme based on the aggregation signature algorithm in the blockchain big data transaction to try to solve the above problems. This scheme was applied to the transaction with multiple inputs and outputs whose amount would be hidden. In addition, the size of the signature in the transaction was constant, and it improved the performance of the signature regardless of the number of inputs and outputs contained in the transaction.

Shen et al. [43] introduced a method of concealing the transaction amount in the strongly dispersed anonymous password currency Monero. Similar to Bitcoin, Monero is a cryptocurrency that was assigned through a workload proof “dig” process, with no center or trusted party established. The original Monero protocol was based on Crypto Note, which used ring signatures and one-time keys to hide the purpose and source of the transaction. Bitcoin core developer Gregory Maxwell had discussed and implemented techniques for using a commitment scheme to hide transaction amounts.

Benjamin [44] described how ECDSA was applied to Bitcoin technology and introduced the elliptic curve digital signature and its application in blockchain technology. The emphasis on the elliptic curve theory and its application in cryptography was a more extensive topic, and it was proved that the security of elliptic curve-based cryptosystem was infeasible by the computation of elliptic curve discrete logarithm problem, thus deriving its security. The difficulty of solving this problem also ensured the security and authenticity of the Bitcoin network’s transaction on the blockchain.

ShenTu et al. [45] proposed an order to strengthen the anonymity of Bitcoin in the blockchain and prevented the centralized coin mixing provider (mixer) to mix bits with multiple inputs and multiple outputs to reveal the relationship between them, in order to provide real anonymity for user. Then, a centralized coin mixing algorithm based on the elliptic curve blind signature scheme (expressed as Blind-Mixing) was proposed, which prevented the mixer from linking the input address with the output address. In addition, Blind-Mixing blind signature scheme was 10.5 times faster than RSA Coin-Mixing, and Blind-Mixing can resist super attackers.

Mercer [46] focused on implementing the privacy on the blockchain and introduced a unique ring signature scheme that worked with the existing blockchain systems, implemented a URS scheme by using secp256k1, and created the first instance that was compatible with the blockchain library to easily implement Ethereum smart contracts. Researchers had demonstrated the privacy and security attributes of the solution and compared its efficiency with other commonly recommended blockchain privacy methods. Although the URS scheme was expensive to implement in the Ethereum, it had realistic feasibility. The compromise between the anonymous guarantee and the availability of the program was decided by the users.

Wu et al. [47] studied how to jointly manage Bitcoin transactions in a blockchain where multiple participants had Bitcoin accounts while maintaining the anonymity of multiple owners. A scenario in which a distributor owned a Bitcoin account and authorized multiple participants to manage together, and a Bitcoin account was shared by peers. Based on the above two application scenarios, partial blind threshold signatures and their extensions were proposed to meet these requirements. The proposed solution was compatible with the current Bitcoin system. The proposed scheme bound the public information c with a key that only the distributor knew, so that an attacker who wanted to tamper with c' must solve the CDH problem, which was computationally infeasible. As for Bitcoin, the platform could not know the amount of Bitcoin and the output address of the transaction. This was the main purpose of ensuring the security of this scheme.

Andreev [48] mentioned that existing ECC blind signatures lack compatibility with the standard ECDSA and therefore could not be directly used for Bitcoin transactions in the blockchain. A solution that allowed the generation of a blind signature that was compatible with existing Bitcoin protocols was then proposed. In this situation, signatories could provide services to store private keys and authenticate transactions without knowing the funds being transferred. Combined with multi-signature transactions, the program could privately lock some money and multiple parties. As in normal ECDSA, secret parameters must never be reused in different signatures.

Bonneau et al. [49] mentioned that Bitcoin's ecosystem in the blockchain was often subject to theft and loss, affecting businesses and individuals. Because of the irreversibility, automation, and pseudonym of transactions, Bitcoin lacked support for the complex internal control systems deployed by modern companies to stop fraud. The first threshold signature scheme compatible with Bitcoin's ECDSA signature was proposed to solve how to use this original resource to establish a distributed Bitcoin wallet and how to use it to implement a threshold wallet and various internal control protocols. The proposed solution had the potential to significantly increase the security of Bitcoin and make it closer to the widely adopted currency.

Dikshit and Singh [50] stated that all Bitcoin transactions were recorded and stored in a publicly available database called blockchain. Because these transactions were available to everyone, Bitcoin must be stored in a secure wallet. These Bitcoin wallets could only be opened with a key, and if the wallet's key was lost, it could not be recovered because of the irreversibility of Bitcoin transactions. In order to solve this problem, previous researchers proposed some solutions, but these solutions had the disadvantage of managing and processing each player's key. In order to remedy this deficiency, they proposed a scheme in which all participants could obtain a single share and could meet the requirements of the weight concept.

Cruz and Kaji [51] studied various cryptographic schemes to implement a secure and efficient electronic voting system, but these systems were difficult to use for actual voting. One of the technical reasons for this unfortunate situation was that many E-voting systems require an anonymous communication channel that was difficult to implement on the Internet. An E-voting system based on Bitcoin protocol and blind signature was proposed. In the proposed system, Bitcoin protocol was supplemented by known protocols (such as blind signature protocol and digital signature protocol) to implement a secure, anonymous, and transparent electronic voting system, and several important features of the electronic voting system were discussed, including fairness, anonymity, soundness, and verifiability. It had shown that the use of the Bitcoin protocol brought other advantageous features in addition to the anonymity of the communication.

Fu et al. [52] mentioned that because of the transaction in the blockchain, even if the user used the public key as the account address to make the transaction anonymous, it would bring potential privacy leakage to the user. In addition, in order to prevent recurring costs, the system agreed only when there were k subsequent blocks generated after the target block, in order to confirm that the transaction on the target block was valid. This time, waiting for the subsequent block generation was longer, and the transaction efficiency was greatly reduced. In view of the above problems, a proxy-based payment system model of password money was proposed, and an implementation scheme based on a blind signature algorithm was given. By introducing agents at the payment stage, the transaction validation time was shortened, the transaction efficiency was improved, and the anonymity of the user was realized better.

Chalkias et al. [53] proposed BPQS, an extensible PQ-resistant digital signature scheme from the blockchain architecture and existing Merkle tree-based signature schemes. BPQS could apply specific chain/graph structures in order to decrease key generation, signing, and verification costs as well as signature size. Compared to recent improvements in the field, BPQS outperformed existing hash-based algorithms, when a key was reused for reasonable numbers of signatures. It also supported a fallback mechanism to allow for a practically unlimited number of signatures if required. BPQS had shorter signatures and faster key generation, signing, and verification times. It was computationally comparable to non-quantum schemes. One could take advantage of the easy-to-apply multiple hash-chain WOTS parallelization and cache to provide almost instant signing and faster verification. Meanwhile, it could be used as a building block to implement novel PQ schemes. In addition, when used in blockchain and DLT applications, it could deploy the underlying chain/graph structure by referencing a previous transaction, in which the same key was reused. This could effectively mean that each new BPQS signature simply required the effort of an OTS scheme, because the rest of the signature path to the root was in the ledger already and can be omitted

Lin et al. [54] introduced the concept and security model of ID-based linearly homomorphic signature and then designed a new ID-based linear homomorphic signature scheme to avoid the shortcomings of the use of public-key certificates. It meant that the signer could construct a linearly homomorphic signature in identity-based cryptosystems. The proposed scheme was proved secure against existential forgery on adaptively chosen message and ID attack under the random oracle model. The ID-based linearly homomorphic signature schemes could be deployed in e-business, cloud computing, and blockchain.

In e-Health, Guo et al. [55] proposed an attribute-based signature scheme to guarantee the validity of EHRs encapsulated in blockchain. The proposed scheme had multiple authorities, in which a patient endorsed a message according to the attribute while disclosing no information other than the evidence that he had attested to it. Furthermore, there were multiple authorities without a trusted single or central one to generate and distribute public/private keys in this scheme. It was to avoid the escrow problem and conforms to the mode of distributed data storage in the blockchain. By sharing the secret pseudorandom function seeds among authorities, this protocol resists collusion attacks. Under the assumption of the computational bilinear Diffie-Hellman, the unforgeability and perfect privacy of the attribute signer were also formally demonstrated.

Qian et al. [56] proposed an efficient short signature length aggregate signature scheme, which solved the privacy protection and performance issues of the blockchain. In this scheme, the length of the aggregate signature was independent of the number of users, which was fixed and reduced the storage overhead. In addition, the signature scheme constructed a signature based on the discrete logarithm problem, instead of constructing a bilinear map-based. It reduced the computational overhead. Meanwhile, in the blockchain transaction, the identity privacy of the receiver was effectively protected. When a transaction contained n input addresses and m output addresses, the number of signatures could be reduced from n to 1. Compared with related schemes, the privacy protection scheme reduced the computational overhead of the signature and verification process, reduced the storage overhead of the blockchain, and improved the communication efficiency.

Li et al. [57] proposed a new lattice-based signature scheme that could be used to secure the blockchain network over existing classical channels. In the key generation phase, they combined the algorithm RandBasis with the algorithm ExtBasis to generate the sub-private keys for verifying the transaction message. This could randomize the output of algorithm ExtBasis and improve the security of the users' private information. Furthermore, the security proof showed that the scheme was secure against the adaptively chosen message attack in random oracle, and the comparison results indicated that it was more efficient than similar works. Therefore, this scheme was more suitable for the transaction implementation in P-QBN.

In addition, Cao et al. [58] proposed a group signature based on blockchain. This signature could be proofed to guarantee security in an untrusted environment and extend the real applications. Long and Wei [59] presented a new Byzantine Fault Tolerance (BFT) consensus mechanism based on an aggregated signature gossip protocol. This mechanism could take thousands of nodes to participate in the consensus process. It had high transaction throughput and low messaging complexity. To meet the requirement of lower bandwidth cost in blockchain, Ren et al. [60] proposed a compact Non-Interactive Zero-Knowledge (NIZK) argument of knowledge and then used it to improve a ring signature. The proposed signature scheme was anonymous and unforgeable and need lower storage space of signature and pairing computations in the verification process. Wang et al. [61] used both mixing and confidential transaction technique to construct a full anonymous blockchain system by a one-way aggregate signature scheme and a homomorphic encryption scheme. In this blockchain, the full anonymity of user identities and transaction amounts were achieved. All individual signatures were compresses by the one-way aggregate signature scheme to reduce storage space. Comparisons of various improved digital signature schemes in blockchain are shown in Table 2. Continuing the classification strategy of Table 1, we conclude these various improved digital signature schemes into six types as follows: aggregate signature (AS), group signature (GS), ring signature (RS), blind signature (BS), proxy signature (PS), and other signatures. The security and performance of different signature schemes in the table vary according to the specific scenarios of their application. It shows that the digital signature technology has relatively good security performance under various applications in the future of the blockchain.

From the above analysis, most of the digital signature schemes in blockchain are deployed by the asymmetric encryption algorithms, which involve RSA, DSA, and ECDSA. For example, Zhu [37], Benjamin [44], Bonneau [49], and Dikshit [50] use ECDSA to implement the digital signatures. In general, DSA can only be used for digital signatures, not encryption (some extensions can support encryption); RSA can be used as a digital signature algorithm or as an encryption algorithm. However, when RSA is used as encryption, its performance decreases sharply with the increase of key length. With the same key length,

Table 2 Digital signatures scheme comparison

Types	Schemes	Application Fields	Methods	Security	Performance
AS	Aitzhan [41]	Problems of providing transaction security in decentralized smart grid energy trading	Blockchain, multi-signed, and anonymous encrypted traffic	To overcome the problem of General Byzantine and to defend against double payment attacks in any electronic payment system	Although the performance of centralized solutions will eventually outperform decentralized solutions, this does not negate the need for decentralized solutions.
	Yuan [42]	Amount will be hidden in blockchain big data transactions with multiple inputs and outputs	Elliptic curve discrete logarithm and bilinear mapping.	According to the security analysis, the potential forgery of the attacker cannot be realized, and the security performance and the aggregate signature are basically the same.	The evaluation by the aggregated signature time, aggregate verification time, and signature space size proves to be superior to other signature schemes.
	Bonneau et al. [49]	In the blockchain Bitcoin transaction, the modern enterprise deploys a complex internal control system	ECDSA compatible threshold signature	Integrate two-factor security measures to increase Bitcoin's security potential and bring it closer to the widely used currency	The total execution time is small compared to the time required for Bitcoin transactions to be confirmed on the blockchain, with an average of 10 min. Therefore, this system is efficient enough to work well in practice.
	Dikshit and Singh [50]	All Bitcoin transactions are recorded and stored in the publicly available database of the blockchain	ECDSA and threshold signature	Potential to significantly increase Bitcoin's security	The program is more practical than previously proposed, users can get different weights according to their needs
	Qian et al. [56]	Solving the privacy protection and performance issues of the blockchain	Based on the discrete logarithm problem, instead of constructing a bilinear map-based.	Length of the aggregate signature was independent of the number of users	Reducing the computational overhead of the signature and verification process, reducing the storage overhead of the blockchain, and improving the communication efficiency
	Li et al. [57]	Used to secure the blockchain network over existing classical channels.	Public and private keys are generated by the Bonsai trees with RandBasis algorithm from the root keys.	Secure against the adaptively chosen message attack in the random oracle	Not only ensure the randomness, but also construct the lightweight nondeterministic wallets
	Zhu et al. [37]	In the process of building blockchain system	Elliptic curve pairs based on bilinear mapping group system	It can protect the owner's unforgery and trader's non-repudiation.	Using exponent times and element length calculation complexity of linear group and communication/storage costs indicate that the program performance is better than previous
GS	Benjamin [44]	Bitcoin transactions in the blockchain	ECDSA	Security of cryptosystem based on the elliptic curve is derived from the computation infeasibility of the discrete logarithm problem of elliptic curve.	Same as ECDSA
	Guo et al. [55]	Guaranteeing validity of EHRs encapsulated in blockchain	Multiple authorities to generate and distribute public/private keys.	By sharing the secret pseudorandom function seeds among authorities, the collusion attack can be defended against.	Avoiding the escrow problem and conforms to the mode of distributed data storage in the blockchain

Table 2 Digital signatures scheme comparison *(Continued)*

Types	Schemes	Application Fields	Methods	Security	Performance
	Shen and Ring [43]	In the transaction of the strongly dispersed anonymous password currency Monero	Ring signature	Hides the volume of transaction transactions between the sender and the receiver to protect privacy	The actual size of the signature is smaller than estimated
RS	Mercer et al. [46]	Compatible with blockchain library and implements Ethereum smart contract	Ring signature	Integrity, unforgeability, and anonymity	Since the compromise between anonymity guarantees and program availability is at the discretion of the user, it is more expensive to implement in Ethereum.
	Ren et al. [60]	Suitable for the blockchain with lower bandwidth cost	Non-interactive zero-knowledge with Compact Linear Knowledge of Exponent Assumption	This scheme is anonymous and unforgeable in the standard model.	This scheme could reduce the signature size and pairing computations in the verification process. When the ring size is large, the effect of our improvements is obvious.
	Tian et al. [38]	Fair contract signing protocol for privacy protection on blockchain	Based on blind signatures and verifiable signatures	By setting the three aspects of the security definition, verifying that the hypothesis is fulfilled, and having the ability to resist fraud, the security of the solution can be proved.	Evaluate the performance of signatures and protocols better than previous ones, from block generation time and the cost of communications through fair-contract-signing agreements
BS	Shentu [45]	In block chain transactions, a centralized coin mixer is prevented from mixing Bitcoins with multiple inputs and multiple outputs.	Blind signature based on elliptic curve	Resists super attackers	10.5 times faster based on Rabin than RSA-based version
	Wu et al. [47]	Bitcoin transactions where multiple participants in the blockchain have Bitcoin accounts while maintaining the anonymity of multiple owners	Blind signature and threshold signature	Prevents attackers from altering transaction information	Calculate the computational complexity of the generated key, the modular multiplication time, the signature and verification of the use of the operation time to illustrate its efficiency
	Andreev [48]	Bitcoin transactions in the blockchain	Blind signature	The signing party can provide services for storing private keys and authentication transactions without knowing the funds being transferred and has confidentiality.	Similar to the overhead of blind signatures
	Cruz and Kaji [51]	E-voting system under blockchain	Bitcoin protocol and blind signature	Protects the privacy and anonymity of voters	The computational cost is very low and does not require much computing power
	Fu et al. [52]	A transaction with a public key as an account address on a blockchain	Blind signature.	With anonymity and privacy protection	Introducing agents at the payment stage, shortening transaction confirmation time and improving transaction efficiency
PS	Lin et al. [54]	Deploying in e-business, cloud computing, and blockchain.	Bilinear groups as the underlying tool.	Secure against existential forgery on adaptively chosen message and ID attack	Avoiding the shortcomings of the use of public-key certificates

Table 2 Digital signatures scheme comparison *(Continued)*

Types	Schemes	Application Fields	Methods	Security	Performance
	Sato and Matsuo [39]	When the underlying encryption algorithm (Hash function and digital signature) compromise.	Long-term signature scheme based on ETSI	When the compromise of the signature scheme occurs, this scheme can avoid the change of the key pair and hard fork.	When changing the hash algorithm, the consumption of the block size depends on the output length of the new hash function and the number of transactions in the block (the number of mutual references between the transaction's hash values) and is therefore superior to other schemes.
Other Signatures	Chalkias et al. [53]	Applying specific chain/graph structures to decrease key generation, signing, and verification costs and signature size	Blockchain architecture and Merkle tree-based signature schemes.	BPQS outperforms existing hash-based algorithms when a key is reused for reasonable numbers of signatures.	BPQS supports a fallback mechanism to allow for a practically unlimited number of signatures if required.

DSA is faster when doing signatures, but slower when doing signature verification. Generally, the number of signature verifications is greater than the number of signatures. Similarly, with the same key length, DSA (with extended support) decrypts the ciphertext faster and the encryption is slower; RSA is just the opposite, and generally, the decryption times are more than the encryption times. However, due to the inherent performance issues of asymmetric encryption algorithms, neither is a good choice for encryption. Compared with RSA and DSA, ECDSA has the following advantages:

- Higher security performance: for example, 160-bit ECDSA has the same security strength as 1024-bit RSA and DSA.
- Lower computation is and fast processing speed: in the processing speed of the private key (decryption and signature), ECDSA is much faster than RSA and DSA.
- Small storage space: the key size and system parameters of ECDSA are much smaller than those of RSA and DSA, so the storage space occupied is much smaller.
- Low bandwidth requirements make ECDSA widely used.

5 Conclusions and future works

In this paper, we focus on the non-repudiation of information security in blockchain. By comparing and analyzing the features of different digital signature schemes used in blockchain system in recent years, it is demonstrated that digital signature technology can well satisfy various specific application properties of blockchains and meet the security requirements in different situations. Our contributions in this paper can facilitate to guide the design of the digital signature schemes in blockchain and optimize the digital signature algorithm to enhance the blockchain security.

Based on the above overview on the digital signature schemes of blockchain systems, we propose the following future suggestions to improve security and performance in this field:

1)For the Bitcoin transaction scenario in the blockchain environment, the characteristics of schemes such as ring signature and blind signature can be used to further study the anonymity of transaction membership and the level of encryption of transaction information and reduce the transaction overhead.

2) Combining digital signatures with identity authentication or time stamps can improve multidimensional security and protect the non-repudiation of information in the blockchain from a broader perspective and direction.

The convergence of blockchain and IoT is the future development trend. Considering the resource-constrained terminals in IoT, we are working on the certificateless aggregation signature scheme for a mobile terminal.

Abbreviations

BVES: Blind verifiable encrypted signature; CDH: Computational Diffie–Hellman; DA: Delivery authority; DLT: Distributed ledger technology; DSA: Digital Signature Algorithm; ECC: Elliptic curve cryptography; ECDSA: Elliptic Curve Digital Signature Algorithm; EHRs: Electronic health records; ETSI: European Telecommunications Standards Institute; IIS: Interactive Incontestable Signature; IoT: Internet of Things; OTS: One-time schemes; P2P: Peer to peer; PQ: Post-quantum; P-QBN: Post-Quantum Blockchain Network; RSA: Named after its inventors Rivest, Shamir and Adleman; SHA: Secure Hash Algorithm; TTP: Trusted Third Party; URS: Unique Ring Signature; WOTS: Winternitz type one-time signature

Acknowledgements

We are grateful to the anonymous reviewers who have contributed to the enhancement of the paper’s completeness with their valuable suggestions.

Authors’ contributions

The six authors of the paper have extensively participated in all of the paper writing. WF mainly worked on the researched. WZ, WC, and JP revised this paper. WG and GW mainly added to and revised the related works. All of the authors equally contributed to reviewing the manuscript. All authors read and approved the final manuscript.

Funding

This research was funded by the National Natural Science Foundation of China (Grant No. 51874300, No. 61571303); the National Science and Technology Major Project of China (Grant No. 2018ZX03001031); the National Natural Science Foundation of China and Shanxi Provincial People’s Government Jointly Funded Project of China for Coal Base and Low Carbon (Grant No. U1510115); the Qing Lan Project, the China Postdoctoral Science Foundation (Grant No. 2013T60574); the Shanghai Natural Science Foundation (Grant No. 17ZR1429100); the Shanghai Sailing Program (Grant No. 19YF1455800); the National key Research and Development Program of China (Grant No. 2019YFB2101602); and the Fundamental Research Funds for State Key Laboratory of Synthetical Automation for Process Industries (Grant No. PAL-N201703).

Availability of data and materials

Not applicable.

Consent for publication

Not applicable.

Competing interests

The authors declare that they have no competing interests.

Author details

[1]Key Laboratory of Wireless Sensor Network & Communication, Shanghai Institute of Micro-system and Information Technology, Chinese Academy of Sciences, Shanghai 201800, China. [2]Shanghai Research Center for Wireless Communication, Shanghai 201210, China. [3]School of Computer Science and Technology, China University of Mining and Technology, Xuzhou 221116, China. [4]State Key Laboratory of Synthetical Automation for Process Industries, Northeastern University, Shenyang 110819, China.

Received: 8 September 2019 Accepted: 13 February 2020
Published online: 04 March 2020

References

1. T.T.A. Dinh, Liu R., Zhang M., Chen G., Ooi B.C., Wang J. Untangling blockchain: a data processing view of blockchain systems. Ieee T Knowl Data En 2018, **30**, 1366-1385.
2. C.-H. Chen, F. Song, F.-J. Hwang and L. Wu. A probability density function generator based on neural networks. *Physica A: Statistical Mechanics and its Applications*. Accepted Manuscript. (acceptance on 01 November 2019) DOI: 10.1016/j.physa.2019.123344

3. C.-H. Chen. A cell probe-based method for vehicle speed estimation. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*. vol. E103-A, no. 1, pp. 265-267, January 2020. DOI: https://doi.org/10.1587/transfun.2019TSL0001
4. C.-H. Chen, F.-J. Hwang, H.-Y. Kung, Travel time prediction system based on data clustering for waste collection vehicles. IEICE Transactions on Information and Systems **E102-D**(7), 1374–1383 (July 2019). https://doi.org/10.1587/transinf.2018EDP7299
5. C.-H. Chen, An arrival time prediction method for bus system. IEEE Internet Things J **5**(5), 4231–4232 (2018). https://doi.org/10.1109/JIOT.2018.2863555
6. Y. Yang, H. Lin, X. Liu, W. Guo, X. Zheng, Z. Liu, Blockchain-based verifiable multi-keyword ranked search on encrypted cloud with fair payment. IEEE Access **7**, 140818–140832 (2019)
7. X. Feng, J. Ma, Y. Miao, Q. Meng, X. Liu, Q. Jiang, H. Li, Pruneable sharding-based blockchain protocol. Peer-to-Peer Netw. Appl. **12**, 934–950 (2019)
8. Y. Zhang, R. Deng, X. Liu, D. Zheng, Outsourcing service fair payment based on blockchain and its applications in cloud computing. IEEE Trans Services Comp. https://doi.org/10.1109/TSC.2018.2864191
9. X. Feng, J. Ma, T. Feng, Y. Miao, X. Liu, Consortium blockchain-based sift: outsourcing encrypted feature extraction in the D2D network. *IEEE Access* **6**, 52248–52260 (2018)
10. W. Zheng, Z. Zheng, X. Chen, K. Dai, P. Li, R. Chen, NutBaaS: a blockchain-as-a-service platform. Ieee Access **7**, 134422–134433 (2019)
11. D. Mao, F. Wang, Y. Wang, Z. Hao, Visual and user-defined smart contract designing system based on automatic coding. Ieee Access **7**, 73131–73143 (2019)
12. Karame G. O., Androulaki E., Capkun S. Double-spending fast payments in Bitcoin. In Proceedings of ACM Conference on Computer and Communications Security. Sheraton Raleigh Hotel, Raleigh, NC, USA, October 16-18, 2012, pp. 906-917.
13. J. Bae, H. Lim. Random mining group selection to prevent 51% attacks on Bitcoin. In Proceedings of the 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W). Luxembourg City, Luxembourg, June 25-28, 2018, pp. 81-82.
14. W. Fang, W. Zhang, T. Pan, W. Chen, Y. Yang, Cyber security in blockchain: threats and countermeasures. J Cyber Security **3**, 87–104 (2018)
15. S.G. Aki, Digital signatures: a tutorial survey. Computer **16**, 15–24 (1983)
16. A. Israeli, M. Li, Bounded time-stamps. Distrib Comput **6**, 205–209 (1993)
17. Digital Signatures. 07/18/2012, https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc962021%28v=technet.10%29
18. A. Nordrum, Wall street occupies the blockchain - financial firms plan to move trillions in assets to blockchains in 2018. Ieee Spectrum **54**, 40–45 (2017)
19. Y. Yuan, F.-Y. Wang, Blockchain: the state of the art and future trends. Acta Automat. Sinica **42**, 481–494 (2016)
20. M.D. Pierro, What is the blockchain? Comput Sci Eng **19**(5), 92–95 (2017)
21. Y. Yang, X. Zheng, W. Guo, X. Liu, V. Chang, Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system. *Inform Sci* **479**, 567–592 (2019)
22. Y. Yang, Y.-C. Zhang, J. Liu, X.-M. Liu, F. YUAN, S.-P. Zhong, Chinese multi-keyword fuzzy rank search over encrypted cloud data based on locality-sensitive hashing. J Inform Sci Eng **35**(1), 137–158 (2019)
23. Y. Yang, X. Zheng, W. Guo, X. Liu, V. Chang, Privacy-preserving fusion of IoT and big data for e-health. Future Gen Comp Syst **86**, 1437–1455 (2018)
24. Y. Yang, X. Zheng, X. Liu, S. Zhong, V. Chang, Cross-domain dynamic anonymous authenticated group key management with symptom-matching for e-health social system. Future Gen Comp Syst **84**, 160–176 (2018)
25. Y. Yang, X. Liu, R. Deng, Expressive query over outsourced encrypted data. Inform Sci **442–443**, 33–53 (2018)
26. C.-L. Chen, Y.-X. Chen, C.-F. Lee, Y.-Y. Deng, C.-H. Chen, An efficient and secure key agreement protocol for sharing emergency events in VANET systems. Ieee Access **7**, 148472–148484 (2019)
27. N. Kshetri, Can blockchain strengthen the Internet of Things? It Prof **19**, 68–72 (2017)
28. K. Christidis, M. Devetsikiotis, Blockchains and smart contracts for the Internet of Things. Ieee Access **4**, 2292–2303 (2016)
29. ISO 10181-4: Information technology – Open Systems Interconnection – security frameworks for open systems: non-repudiation framework, International Organization for Standardization, 1997.
30. D. Johnson, A. Menezes, S. Vanstone, The Elliptic Curve Digital Signature Algorithm (ECDSA). Int J Inf Secur **1**, 36–63 (2001)
31. How do digital signatures in Bitcoin work? https://www.cryptocompare.com/wallets/guides/how-do-digital-signatures-in-bitcoin-work/
32. B. Dan, C. Gentry, B. Lynn, H. Shacham, in *Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques*. Aggregate and verifiably encrypted signatures from bilinear maps (Springer, Berlin, Heidelberg, 2003), pp. 416–432
33. D. Chaum, E.V. Heyst, in *Proceedings of Advances in Cryptology — EUROCRYPT '91*. Group Signatures (Springer, Berlin, Heidelberg, 1991), pp. 257–265
34. R.L. Rivest, A. Shamir, Y. Tauman. How to leak a secret. In Proceedings of Advances in Cryptology — ASIACRYPT. Gold Coast, Australia, December 9-13, 2001, pp. 552-565.
35. D. Chaum. Blind Signature System. In Proceedings of Advances in Cryptology — CRYPTO '83, Santa Barbara, California, USA, August 21-24. 1984, pp. 153.
36. M. Mambo, K. Usuda, E. Okamoto. Proxy signatures for delegating signing operation. In Proceedings of the 3rd ACM Conference on Computer and Communications Security. New Delhi, India, March 14-16, 1996, pp. 48-57.
37. Y Zhu, R Guo, G. Gan, W.-T. Tsai. Interactive incontestable signature for transactions confirmation in Bitcoin blockchain. In Proceedings of IEEE 40th Annual Computer Software and Applications Conference (COMPSAC). Atlanta, Georgia, USA, June 10-14, 2016, pp. 443-448.
38. H.B. Tian, J.J. He, L.Q. Fu, A privacy preserving fair contract signing protocol based on public blockchains. J Cryptol Res **4**, 187–198 (2017)
39. M. Sato, S. Matsuo. Long-term public blockchain: resilience against compromise of underlying cryptography. In Proceedings of the 26th International Conference on Computer Communication and Networks (ICCCN). Vancouver, Canada, July 31 – August 3, 2017, pp. 1-8.
40. J. Naoum. European Telecommunications Standards Institute. 2011.
41. N.Z. Aitzhan, D. Svetinovic, Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. Ieee T Depend Secure **15**(5), 840–852 (2018)
42. C. Yuan, M.X. Xu, X.M. Si, Research on a new signature scheme on blockchain. Secur Commun Netw **2**, 1–10 (2017)
43. N. Shen, Adam M. Ring confidential transactions. MONERO RESEARCH LABS, 2016. https://eprint.iacr.org/eprint-bin/getfile.pl?entry=2015/1098&version=20151217:200440&file=1098.pdf
44. B.K. Kikwai, Elliptic curve digital signatures and their application in the bitcoin crypto-currency transactions. Int J Sci Res Publications. **11**, 135–138 (2017)
45. Q.C. Shentu, J.P. Yu, A blind-mixing scheme for bitcoin based on an elliptic curve cryptography blind digital signature algorithm. Comp Sci (2015) https://arxiv.org/ftp/arxiv/papers/1510/1510.05833.pdf
46. R. Mercer. Privacy on the blockchain: unique ring signatures. 2016. https://arxiv.org/pdf/1612.01188.pdf
47. Q. Wu, X. Zhou, B. Qin, J. Hu, J. Liu, Y. Ding, Secure joint Bitcoin trading with partially blind fuzzy signatures. *SOFT COMPUT* **21**, 1–12 (2015)
48. O. Andreev. Blind signatures for Bitcoin transactions. 2017. http://pdfs.semanticscholar.org/af74/cc0dcdaece3d7586d8c33d3f3bd0cf377e1a.pdf
49. J. Bonneau, E. W. Felten, H. Kalodner, J. Bonneau, E.W. Felten, j.A. Kroll, A. Narayanan. Securing Bitcoin wallets via a new DSA/ECDSA threshold signature scheme. 2015. http://stevengoldfeder.com/papers/threshold_sigs.pdf
50. P. Dikshit, K. Singh. Efficient weighted threshold ECDSA for securing Bitcoin wallet. In Proceedings of ISEA Asia Security and Privacy (ISEASP), NIT SURAT, INDIA, January 29 - February 1 2017, pp. 1-9.
51. J.P. Cruz, Y. Kaji, E-voting system based on the bitcoin protocol and blind signatures. IPSJ Trans Mathematical Model Appl **1**, 14–22 (2017)
52. X.-T. Fu, S. Chen, N. Zhang, Proxy-cryptocurrency payment system. J Commun **38**, 199–206 (2017)
53. K. Chalkias, J. Brown, M. Hearn, T. Lillehagen, I. Nitto, T. Schroeter, in *Proceedings of IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. Blockchained post-quantum signatures (Halifax, Canada, 2018), pp. 1196–1203
54. Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen, Y. Tang, An ID-based linearly homomorphic signature scheme and its application in blockchain. IEEE Access **6**, 20632–20640 (2018)
55. R. Guo, H. Shi, Q. Zhao, D. Zheng, Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. IEEE Access **6**, 11676–11686 (2018)
56. K. Qiao, H. Tang, W. You, Y. Zhao. Blockchain privacy protection scheme based on aggregate signature. In Proceedings of IEEE 4th International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), Chengdu, China, April 12-15, 2019, pp. 492-497.

57. C.-Y. Li, X.-B. Chen, Y.-L. Chen, Y.-Y. Hou, J. Li, A new lattice-based signature scheme in post-quantum blockchain network. IEEE Access **7**, 2026–2033 (2019)
58. Y. Cao, Y. Li, Y. Sun, S. Wang. Decentralized group signature scheme based on blockchain. In Proceedings of International Conference on Communications, Information System and Computer Engineering (CISCE), Haikou, China, July 5-7, 2019, pp.566-569.
59. J. Long, R. Wei. Scalable BFT consensus mechanism through aggregated signature gossip. In Proceedings of IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, South Korea, May 14-17, 2019, pp. 360-367.
60. H. Ren, P. Zhang, Q. Shentu, J.K. Liu, T.H. Yuen, in *Proceedings of International Conference on Information Security Practice and Experience Information Security Practice and Experience (ISPEC). Lecture Notes in Computer Science.* Compact ring signature in the standard model for blockchain, vol 11125 (Springer, Cham, 2018), pp. 50–65
61. Z. Wang, J. Liu, Z. Zhang, H. Yu, Full anonymous blockchain based on aggregate signature and confidential transaction. J Comp Res Dev **5**(10), 2185–2198 (2018)

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.