JOURNAL OF APPLIED SECURITY RESEARCH
https://doi.org/10.1080/19361610.2021.1933322

Routledge
Taylor & Francis Group



# A Review on Cryptocurrencies Security

T. M. Navamani

School of Computer Science and Engineering, VIT University, Vellore, Tamil Nadu, India

**ABSTRACT**

Security and privacy are the two terms that are well connected with the current trends in cryptocurrency, and this study gives an extensive review of the same. Cryptocurrency adds security to the transaction flow and regulates the formation of additional units of currency. The massive growth in the market assessment of cryptocurrency leads to misuse of deficiencies for profit by adversaries. In this study, a review was made to focus on the security and protection measurements of cryptocurrencies specifically on Bitcoin. This study describes cryptocurrency conventions, their usefulness, and communications within the framework.

**KEYWORDS**

Attacks; Bitcoin; blockchain; cryptocurrency; decentralization; security

## Introduction

In recent years, the global economy is certainly moving toward a digital era. Everything is carrying out by the people in digital form. The hottest trend in the digital payment division is cryptocurrency. Like normal currencies, cryptocurrencies are used as the medium of exchange but designed purposefully to exchange digital information. It is a decentralized digital currency that uses cryptography for security and thus makes it difficult to forge. Meanwhile, it is not provided by the central government authority and hence it is not taken away from the users. Cryptocurrency is a kind of trusted and safe form of digital currency which people prefer to use nowadays. Since there is no third-party involvement, cryptocurrencies provide a kind of reassurance to the users and a feeling of safety while carrying out the transactions (Ghosh et al., 2020; Narayanan et al., 2016).

When users create cryptocurrencies, all legitimate and confirmed transactions are stored in a public ledger. The identities of users who own currencies are completely encrypted to confirm the validity of record keeping. Another reason is that people need not spend their money to carry out the transactions. It is because the people who mine the cryptocurrencies (referred to as Miners) receive their compensation from the network itself.

**CONTACT** T. M. Navamani navamani.tm@vit.ac.in School of Computer Science and Engineering, VIT University, Vellore, Tamil Nadu, India.

Also, people can save their currencies in safe wallets which are free of charge only. People can carry out their transactions in an anonymous manner and it is highly confidential. As senders or receivers of cryptocurrencies, they cannot transfer money directly to their credit card accounts or any other accounts and also users need not share their credentials with anyone. Thus, Identity theft can be avoided (Narayanan et al., 2016).

In 2009, a person going by the name of Satoshi Nakamoto published a research article related to a concept that later went on to bring a disruption in the realm of the Internet. Ever since Bitcoin digital currency was discharged, around 600 distinctive cryptographic money propositions have emerged. Among the several cryptocurrencies launched, Bitcoin is the most successful and popular digital currency. It contains a distinct type of data structure that can be utilized for storage and transactions occurring on its network without the association of a third party. The foremost method utilized in the development of Bitcoin is blockchain innovation, which was introduced in the year 2008 and its real-time implementation was accomplished in the year 2009. Blockchain technology was developed with the incorporation of decentralized techniques and does not involve any trusted authority. This incredible mechanism was realized for the continuous development of cryptocurrencies. In these technologies, the exchange of digital resources taken place in a decentralized manner. Further, several cryptocurrencies have emerged into the real world like Bitcoin, Ripple, Litecoin, Ethreum, etc. In all these cryptocurrencies, legitimate entities can undertake economic transactions without any central authority (Ghosh et al., 2020). It was observed that Bitcoin was the highest operating product in the year 2016 and the same year, blockchain technology achieved 10 billion dollars in its capital market (Nakamoto, 2008).

These cryptocurrencies do not need a centralized regulating authority and operate independently. Bitcoin, just like any other cryptocurrency, uses the concept of peer-to-peer (recently termed "blockchain") technology, in which any person who owns any unit of this currency could utilize or spend it anywhere and anytime without the contribution of any trusted third party. Bitcoin is planned as an open-source, and nobody possesses or controls it. Bitcoin integrated with blockchain technology was arranged in a distributed environment and thus single user authority was avoided. Subsequently, there was no single point of failure and fund transfer between clients was done without the involvement of any third party. Thus, a self-policing methodology was created by incorporating a decentralized blockchain technology along with the consensus approach-based maintenance system which assured that only valid transactions are added to the blockchain system.

Using Bitcoin, users can complete electronic payments by initiating transactions that transfer Bitcoins between users. The target address

(Bitcoin address) is computed by applying a sequence of cryptographic hash functions on the user's public key. In Bitcoin, users can keep multiple addresses by creating multiple public keys and all these addresses could be linked with their wallets. To spend the owned Bitcoins in the form of digitally signed transactions, users have to submit their private key which is kept secret. Users' anonymity can be governed by applying a hash function on the public key as a receiving address and it is suggested to have a different Bitcoin address for every receiving transaction (Conti et al., 2018).

Since their deployment, cryptocurrencies have attracted much attention from both academic and industrial institutions. Once the amount of money at stake is specified, they have become a target for adversaries. Different aspects of the cryptocurrency system have been targeted, using various kinds of attacks, such as double spending, transaction malleability, netsplit, networking attacks, or attacks targeting miners and mining pools. These security concerns and vulnerabilities are the main reason why, in malice of all the popularity that Bitcoin and other cryptocurrencies have gained, they are nevertheless not practiced with as much religion as other kinds of currency. Security solutions for cryptocurrencies are of most importance and need to be spread over all the significant protocols implementing the functions, such as blockchain, consensus, key management, and networking protocols.

Apart from the use of cryptocurrencies, the underlying concepts and recent technologies like blockchain and consensus protocols are being used in numerous different fields, for example, Internet of Things (IoT), smart cities, healthcare data management (Azaria et al., 2016; Ekblaw et al., 2016), Finance (Huckle et al., 2016; Hurich, 2016; Jindal et al., 2019), Software Engineering (Lee Kuo Chuen, 2015), IoT (Chaudhary et al., 2019; Dorri et al., 2017), etc. Since cryptocurrencies and related concepts are essential for next-generation applications, our purpose is to examine the related security issues and concerns.

Cryptocurrencies, especially Bitcoin, are prevalent on a global scale. Since a cryptocurrency is a distributed model with an overwhelming environment, hackers and malicious users find this system an easy way to fraud the transactions. Also, there exists a substantial amount of security vulnerabilities in the cryptocurrency protocols, and also within the network. Hence, there exists more debate around the world as the security and privacy issues of cryptocurrencies are still being investigated. Moreover, the attacks, particularly in blockchain networks such as netsplit, double spending, transaction malleability, Finney attack, etc., are discussed in the literature focusing on miners or mining pools.

This study presents a comprehensive survey with a focus on the security and protection parts of Bitcoin and other cryptocurrencies and their

underlying concepts. This work includes a discussion on the state-of-the-art attack vector, which involves threats to the security of the user and the anonymity of transactions, which thus looms the usage of cryptocurrencies in real-world applications and services. In recent years, researchers have proposed a large number of security solutions to address the current security and privacy challenges in Bitcoin, which are discussed in this work and also focus made on the security issues and their countermeasures related to the significant components of cryptocurrencies.

Tschorsch and Scheuermann (2016) provided a detailed survey on digital currencies with an emphasis on Bitcoin. Exploration of details related to Bitcoin is done well by the authors and also discussed the consequences of the design decisions for various cryptocurrency technologies. In the work of Bonneau et al. (2015), the authors presented all the different cryptocurrencies in use and discussed the advantages and disadvantages of Bitcoin. However, there lacks of a proper survey about the security and privacy concerns of cryptocurrencies, even though security is a significant issue in the realm of cryptocurrencies.

Particularly, the main contributions of this article are as follows –

- This work presents basic concepts for Bitcoin, its functionalities, and related ideas, its functionalities. The readers need to have a clear and robust foundation regarding cryptocurrencies and underlying concepts to understand further the security issues and challenges faced by the world of cryptocurrencies.
- Also, systematic presentation and discussion are done on various threats based on security and privacy, which occur either directly or indirectly with Bitcoins. Moreover, exploring the possibilities of various threats that an adversary could exploit.
- Discussed the effectiveness and shortcomings of the existing solutions which deal with the security threats and enable secure privacy in Bitcoin, thus providing a technical view on these challenges in the use of cryptocurrencies.
- Discussed the security challenges in the Bitcoin network, which outlines the open research challenges in the blockchain technology.

This study seems to assist interested readers:

- To give insight into the security and privacy concerns and their scope and impact.
- To be aware of the damage that these threats can do.
- To give a positive direction to this topic and find ways to detect and contain these threats.

The main objective of this work is to present detailed background knowledge in the cryptocurrency research community with a focus on mitigating the alarming threats from disturbing the community. Although there is no hard proof that these threats have already been applied to specific cryptocurrencies, however, there is a chance that some of the essential features of cryptocurrencies make these threats in reality.

## Attacks on cryptocurrencies

Bitcoin network is vulnerable to various categories of attacks due to the double-spending concept which is the primary cause for most of the attacks in the network. Table 1 shows the summary of attacks on blockchain networks. Double Spending is a kind of attack which occurs when someone tries to transmit two conflicting transactions from the same address.

Bonneau et al. (2015) discussed various vulnerabilities and security loopholes in Bitcoin, which questions the stability of the currency, performance of the protocol, and also the usage of different solutions are proposed concerning the above issues, which include changing parameters such as limits on the block and transaction size, inter-block time, monetary policy, etc., and coming up with a substitute for cryptographic puzzles used practically and help humankind by solving real-world scenarios.

Karame et al. (2012) mentioned the costs incurred by computational transactions and also about increasing security which causes a delay in the whole process of about 10 min. Cryptocurrencies involve higher layers of security and will have a delay in transactions. Therefore, they are not supposed to be used for faster transactions where time is a critical factor. Following the same notion, if these are made to use for faster payments by reducing the security, which will increase the performance, there will be an issue of double-spending that can make cryptocurrencies very insecure. Vyas and Lunagaria (2014) described the concept of proof-of-work (PoW), and its usage in the blockchain ensured that the block initiated by the miner matches with the pattern of the next block. Moreover, they discussed the security threats concerned with blockchains such as time-jacking issues, attacks occurring in wallet software, the "$>$50%" attack, double-spending, and selfish mining.

Conti et al. (2018) mentioned the parts of the protocol of Bitcoin and also discussed their functionality. This work questions the exploitable loopholes in the cryptocurrency and also finds vulnerabilities in its base technology of PoW-based consensus and blockchain protocol. People who are working on the Bitcoin are threatened by these vulnerabilities, which, if executed, can bring many damages.

**Table 1.** Summary of attacks on blockchain system.

| Attacks | Attack description | Key targets | Effects on the system | Potential countermeasures |
|---|---|---|---|---|
| Bribery attacks (Bonneau, 2016) | Attackers provide payments to existing miners to divert from the normal execution policies. Miners are diverted to mine on the attackers' division | Miners and Mer Chants | Increase in the possibility of double spends or block withholding | Rewards for honest Miners can be increased Giving awareness to the miners about the long-standing losses of bribery (Bonneau et al., 2015) |
| Refund attacks (McCorry et al., 2017) | Attackers exploit the existing fund strategies of the Payment processors | Merchants, sellers, users | Money loss for the merchants Honest users lose their reputation. | A publicly verifiable algorithm can be used (Karame et al., 2012) |
| Punitive and feather forking (Miller, 2013; Narayanan et al., 2016) | Blacklisting transactions initiated by specific addresses | Users | The Bitcoins of users are restricted forever | This issue remains an open challenge |
| Transaction malleability (Andrychowicz et al., 2015) | The transaction ID can be changed by an adversary without invalidating the transaction | Bitcoin exchange centers | Loss funds are exchanged as a result of an increase in double deposit or double withdrawal instances | Various metrics can be adopted for transactions verification (Wuille, 2014) |
| Wallet theft (Saad et al., 2019) | Intentionally, adversaries snip or destroy the private key of the users | Individual users or business companies | Suddenly Bitcoins in the Wallet are lost | A mechanism named Threshold signature Based two-factor security can be incorporated (Gennaro et al., 2016; Goldfeder et al., 2014), Hardware wallets (Bamert et al., 2014) TrustZone-backed Bitcoin wallet (Jarecki et al., 2016), Password-protected secret sharing (PPSS) (Saad et al., 2019) |
| Time jacking (Miller, 2013, Corbixgwelt, 2011) | Attackers speedup most of the miners' clock | Miners | Miners are isolated and their resources are wasted to enable difficulty in the calculation process | Implementing constraint tolerance ranges (Gennaro et al., 2016), Network time protocol (NTP) or time sampling on the values received from trusted peers (Mills et al., 2011) |
| Distributed denial of service (DDoS) Attack (Johnson et al., | A cooperative attack to drain the network resources | | | Proof-of-activity (PoA) protocol (Bentov et al., |

| | | | | |
|---|---|---|---|---|
| 2014; Saad et al., 2019; Vasek et al., 2014; ) | | Bitcoin network, Business companies, miners, and users | Denying the services to honest users/miners, isolate or push away from the miners | 2014), fast verification signature-based authentication |
| Sybil attack (Johnson et al., 2014; Vasek et al., 2014) | Attacker generate many virtual identities | Bitcoin network, miners and users | Enables time jacking, DDoS, and double spending attacks, threatens user privacy | Xim (a two-party mixing protocol) (Bissias et al., 2014) |
| Eclipse or netsplit (Ghosh et al., 2020; Koshy et al., 2014; Saad et al., 2019) | An intruder exploits all transactions of a victim | Miners, users | The erratic perspective of the network and blockchain, enable double-spends with multiple confirmation messages | Use whitelists, disabling incoming connections |
| Tampering (Ghosh et al., 2020; Johnson et al., 2014; Saad et al., 2019; Vasek et al., 2014) | Delaying the propagation of transactions and blocks to specific nodes | Miners, users | Influence DoS attacks, double-spend attacks | Enhance block request management system |
| Routing attacks (Ghosh et al., 2020; Johnson et al., 2014; Vasek et al., 2014) | Separating the set of nodes from the Bitcoin network, postponing block transmission | Miners, users | Influence DoS attack, which raises the possibility of zero-confirmation, increases in fork rate, wastes the mining power of the pools | Extend the diversity of node connections, observing the round-trip time, using gateways |
| Deanonymization (Biryukov et al., 2014; Koshy et al., 2014) | Connecting IP addresses with a Bitcoin wallet | Users | User's privacy violation | Mixing services (Danezis et al., 2003), CoinJoin (Maxwell, 2013), CoinShuffle (Ruffing et al., 2014) |
| Double spending (Biryukov et al., 2014; Ghosh et al., 2020; Koshy et al., 2014; Saad et al., 2019) | Used the same currency in several transactions, sending two inconsistent transactions in rapid succession. | Sellers or merchants | Sellers miss their products, losing honest users, Creates blockchain forks | Adding observers in the network, sharing double-spending warning messages among peers, Neighbor peer notifies the merchant about ongoing double sending; Merchants can deactivate the incoming transactions |
| Finney attack (Ghosh et al., 2020; Koshy et al., 2014) | Untruthful miner transmits a pre-determined block for double-spending once it receives product from the merchant | Sellers or merchants | Invokes double spending | The merchant must wait for a substantial number of authentications (Ghosh et al., 2020). |

(*continued*)

**Table 1.** Continued.

| Attacks | Attack description | Key targets | Effects on the system | Potential countermeasures |
|---|---|---|---|---|
| Brute force attack (Biryukov et al., 2014; Ghosh et al., 2020; Koshy et al., 2014) | In private, mining on the blockchain to carry out double-spending | Sellers or merchants | Influences double-spending, Constructs huge size blockchain forks | Adding observers in the network, Inform the merchant about an ongoing double-spend (Ghosh et al., 2020) |
| Vector 76 or one-confirmation attack (Biryukov et al., 2014; Ghosh et al., 2020; Saad et al., 2019) | Mixture of the double-spending and the finney attack | Bitcoin exchange services | Invokes double-spending of the substantial number of Bitcoins | Wait for multiple confirmation messages for transactions |
| Selfish mining (Biryukov et al., 2014; Ghosh et al., 2020) | Exploiting Bitcoin forking feature to receive an unfair reward | Honest miners, mining pools | Announcing new race conditions by forking, Intentionally using the computational power of honest miners | ZeroBlock mechanisms, Timestamp-based techniques such as freshness, DÉCOR + protocol |

From Table 1, it is clear that malicious users can attack a cryptocurrency in many ways. There are a significant number of attacks that can be used to exploit the vulnerabilities in the system. With the exponential rise in the popularity of cryptocurrencies, the rate of attacks on them is also extremely alarming. It can be prevented only by adequately designing the architecture of the blockchain and proper implementation of the algorithms used in cryptocurrencies.

## Architecture of blockchain

Cryptocurrencies can be defined as an asset that is purely digital and is made to work as a trade medium by utilizing the field of cryptography to not only form some units which are extra but also to provide a secure path for the exchanges and verify the authenticity of the transactions (All you need to know about Bitcoin - Bitcoin Forum, 2018). These are decentralized and mostly work through a decentralized system known as blockchain, which is a database that is open and is available to be everyone. The blockchain functions like a distributed ledger (Chohan, 2017).

Blockchain is the backbone behind legitimizing cryptocurrency transactions and also making them secure. It is continuously making new records which are called squares; these squares are connected and secured with the help of cryptography. Blockchain behaves like a linked list where each piece contains a pointer which is a hash and points to a previous block, and it can also include a timestamp and the data that is exchanged. By definition, blockchain is immutable and impervious if someone wants to change the data existing on the blockchain. Similarly, an example has been displayed in Figure 1. A blockchain is overseen by a system that is shared and relies on the convention of everyone approving the addition of new blocks. Once these blocks are added, and the data are made part of the system, they cannot be modified because the corresponding hash of the block will change and all the subsequent hashed needs to be changed accordingly.

In general, blockchains are very secure. They are usually the case of a framework that is appropriate in the concerned discussion with great Byzantine adaptation to failures concerned with internal functioning. The accord of decentralization has been achieved with the invention and implementation of blockchain, and it tackles many issues, such as a 2-fold spending issue without involving an expert or a dedicated focal server. Square time is defined by the time taken for a system to produce and adding a block in the blockchain. Few blockchains formulate a block every 7 s. By the time the block is created and added, the included information ends up evident, and at that time, an exchange of cash took place. Thus a short square time will result in faster exchanges.

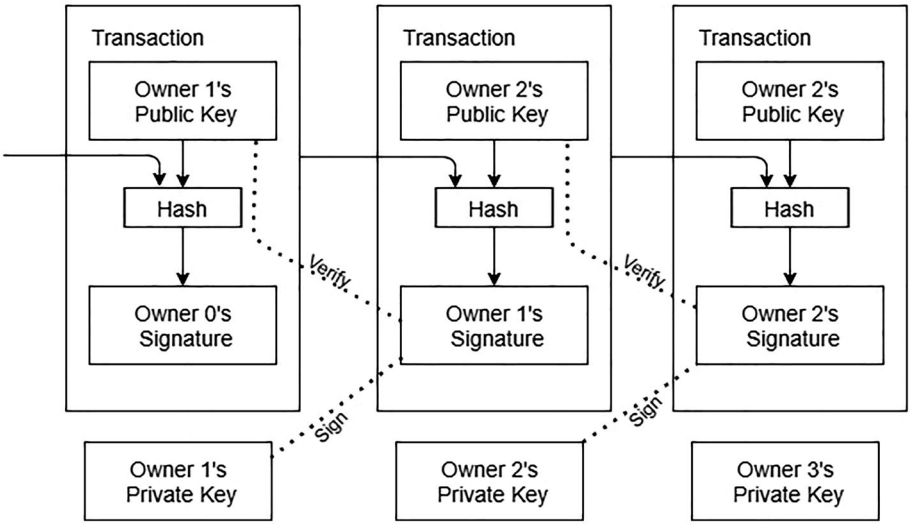


**Figure 1.** Flow of Bitcoin transaction (Wheatley, 2018).

### *Proof-of-work (PoW)*

The concept of the PoW system is used for preventing abuse of the cryptocurrency system, such as the denial of service attacks, spam, double-spending, and many other attacks. This concept is used to create a distributed trustless consensus, in which the system requires some work, i.e. computational work, from the computer requesting the service. This "work" is usually in the form of processing time by the computer of the requester. Cynthia and Moni (1993) invented this concept of doing "work" for your request to be granted.

The main characteristic and probably the reason why PoW is a concept that most cryptocurrency systems have been able to rely on ever since their establishment is the asymmetry between when it comes to the actual computational work, and when it comes to validating it (Markus & Ari, 1999). This idea goes by many other names—computational puzzle, CPU cost function, cryptographic puzzle. Even with its base concept being very similar to that of a CAPTCHA, it is different from it and is intended for humans to solve rapidly than computers. Along the lines of PoW, various other concepts are proposed, such as proof-of-space, proof-of-bandwidth, and proof-of-ownership.

### *Proof-of-stake (PoS) and combined schemes*

Unlike PoW which forms a distributed consensus purely based on the amount of computational work done by the service requester, in the proof-of-stake (PoS) system, the owner of the succeeding block is selected based on the combination of random selection and wealth or age (i.e. stake).

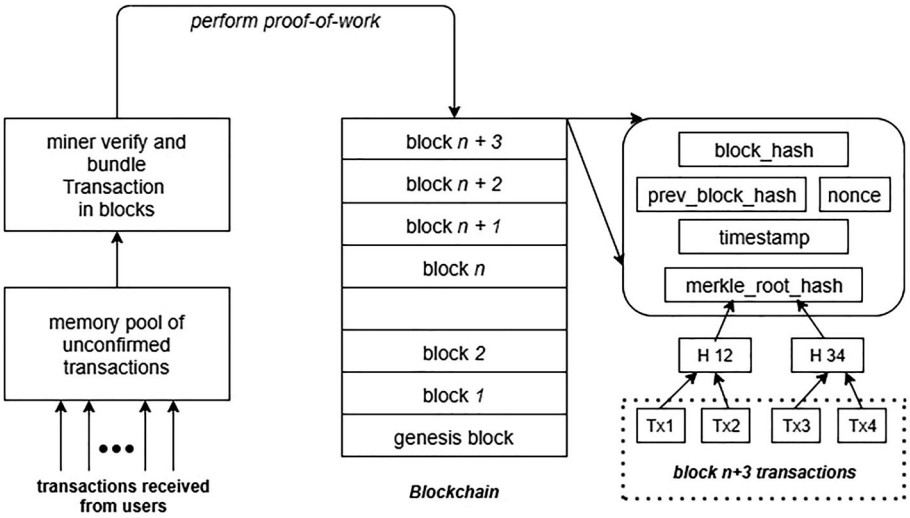


**Figure 2.** Creation and addition of blocks in blockchain (Conti et al., 2018).

Although the PoS is more energy-efficient than PoW, PoW is still a highly favored scheme because it provides a better consensus about which computer shall be made the creator of the next block. Most popular crypto-currencies either use a PoW system or a combined PoW/PoS scheme.

### *Mining of blocks*

After the process is done and the transactions take place, they are combined with the timestamp and hash of the previous block and are stored using a Merkle tree (Merkle, 1987) which is different for each block. The methodology has been visualized in Figure 2, which is used for maintaining and creating blocks in the cryptocurrencies' corresponding blockchain. The miners solve a problematic cryptographic puzzle using their resources and in the process, verify the block that needs to be added to the blockchain. The blocks are stored in a linked list manner where one can traverse the list or chain to find out the owner of each transaction. The data in the blocks are immutable because if one tries to change the block by modifying the data, the corresponding hash will change and thus change the subsequent blocks. Each block consists of the hash of the previous block, make changing the whole subsequent block.

The length of the blockchain keeps on increasing because of the addition of blocks through mining which is a continuous process. This process includes two steps (i) A miner needs to validate the hash value, i.e. it should be less than or equal to the target value for a particular block. Once the validation is done, the block is added to the local blockchain of the miner, and this is broadcast to the whole network. (ii) Once the miners receive the broadcasted solution, they validate the block, and if it is valid,

then they append the block to their local blockchain, or else they discard the block for an invalid solution (Conti et al., 2018). Figure 2 shows the architecture of mining blocks in the network.

### Digital signature

The user who signs the transactions digitally should own two keys: a public key and a private key. The procedure is that the private key is used to sign the transactions and is kept a secret. After signing the transactions, the transactions are announced on the full network; the verification takes place with the public key that the user sent. The general digital signature scheme involves two phases as specified: the signing phase and the verification phase. For instance, a user Bob willing to send another user Alice a message, and also wants that no one else should read the message on the network.

1. In the signing phase, Bob encrypts his data with his private key which is maintained secretly, and sends Alice the encrypted result and original data.
2. In the verification phase, Alice validates the value with Bob's public key, and thus Alice can verify if the data has been tampered with or not with ease. Elliptic curve digital signature algorithm (ECDSA; Johnson et al., 2001; Zheng et al., 2017) is the digital signature scheme that is widely used in blockchains.

### Smart contract

A smart contract is a computer program, or a digital document, with the purpose of digital facilitation, verification, and enforcement of the negotiation and execution of a contract. The term and the concept of smart contracts were coined and proposed by Nick Szabo (2017).

Smart contracts act as a ledger and allow the performance of credible transactions. The workflow is such that each block in the blockchain consists of a ledger of its own, thus avoiding the need for any third party. This way, the smart contracts achieve their aim of providing security and trust in a manner superior to conventional contract law and minimizing other overheads which arise with contracting. Byzantine fault-tolerant algorithms have enabled security in decentralization, which eased the construction of smart contracts. Besides that, the programming languages used to create blockchains have several degrees of Turing-completeness as their built-in feature, which in turn allows the creation of sophisticated custom logic. Different hash algorithms are used to secure these cryptocurrencies, a

**Table 2.** Different cryptocurrencies and hash algorithms.

| Currency | Hash algorithm | Cryptocurrency blockchain (PoS, PoW, or other) |
|---|---|---|
| Bitcoin | SHA-256d | PoW |
| Litecoin | SCRYPT | PoW |
| Bytecoin | CryptoNote | PoW |
| Peercoin | SHA-256d | PoW & PoS |
| Dogecoin | SCRYPT | PoW |
| Primecoin | 1CC/2CC/TWN | PoW |
| Ripple | ECDSA | "Consensus" |
| MazaCoin | SHA-256d | PoW |
| Monero | CryptoNight | PoW |
| Ether or Ethereum | ETHASH | PoW |
| Ethereum Classic | ETHASH | PoW |
| Zcash | Equihash | PoW |
| Bitcoin Cash | SHA-256d | PoW |

summary of which is presented in Table 2. New cryptocurrencies are made with even better secure algorithms.

A hash algorithm transforms an arbitrarily large amount of data into a fixed-length hash code. Hash code would be changed according to the data, i.e. the same hash code will be a result of the same data, but altering the data by just a bit will completely change the hash code. A hash function is a computing process that takes input data of any size, applies an operation on it, and then gives output data of a fixed size.

## Security algorithms

Different security algorithms (Dai et al., 2017) are analyzed to visualize the security issues, and the solutions have been presented.

### *SHA-256*

Secure hash algorithm (SHA) is much more complicated when compared with algorithms, such as SCRYPT. This algorithm is used extensively by different cryptocurrencies and Bitcoin itself. To increase the security of this algorithm, the processing of data blocks is done almost free of any errors. However, it leads to slowing down the transactions, and thus minutes are used instead of seconds to measure the time. For the mining of coins to be successful when SHA-256 is in use, hash rates at the GH/s level or higher level are needed. That is why it is not easy for all the miners to mine and use the network at this high hash rate (Dai et al., 2017; Ghosh et al., 2020).

### *SCRYPT*

As mentioned in the description of SHA-256, SCRYPT is a relatively more comfortable and faster algorithm. In this review, it is observed that crypto-currencies that are new in the market are using SCRYPT over SHA-256

due to more comfortable and faster operations. SCRYPT requires fewer resources than SHA-256 and does not need a dedicated machine for its operations and thus many miners are opting to mine SCRYPT based cryptocurrencies rather than SHA-256 based (Dai et al., 2017). The hash rates of this algorithm lie in the range of KH/s or MH/s, which can be achieved by a single compute operation. Some people doubt its authenticity and security levels due to its fast transaction turnaround time, but no one has proven this practice until now (Ghosh et al., 2020).

### *CryptoNote*

It is a protocol concerned with the application layer of the OSI model. It is the crucial protocol behind many cryptocurrencies and is one of the reasons behind the evolution of ideas such as Bitcoin although both of these differ from each other. The critical difference between these two technologies is the opacity which is more of CryptoNote because its blockchain is almost anonymous. On the other hand, non-CryptoNote blockchains are less opaque. Although CryptoNote currencies use a ledger that is public and shared keeps the record of all the transactions, the balances of its corresponding currency, it does not follow through the blockchain and does not disclose the identity of the receiver or the sender. An approximation of the amount can be made available, but the actual amount, origin, or destination cannot be found out. The approximation is always more than the actual amount, and only the sender and receiver of the transaction know the full dataset. This dataset can also be retrieved by the person who has one or both of the secret keys (Cynthia & Moni, 1993).

There is one more significant difference which is a hash-based PoW algorithm. SHA-256, which is a CPU-bound function, is used in Bitcoin, whereas CryptoNote uses CryptoNight, which is a memory-bound function and cannot be pipelined easily. The miners have their limit based on the speed of calculation taking place. CryptoNote code has not been derived from Bitcoin and thus has many different algorithms which are used in inner functioning, such as recalculation of the size of the new block.

### *ECDSA*

ECDSA (Dikshit & Singh, 2017) is a cryptographic algorithm used by different blockchain networks and is majorly used by Bitcoin. This algorithm makes sure that the money is spent only by their trusted owners.

Some key concepts related to this algorithm:

*Private Key:* A randomly generated number that is supposed to be kept as a secret and is only known to the person that generated it. In the case of Bitcoin, the person having the private key which is connected to the money on the ledger that is available to everyone can spend that money.

*Public key:* This is deeply connected to its corresponding private key with the difference being that this does not have to be kept as a secret. This key can be derived or computed from the corresponding private key, but a private key cannot be retrieved from a public key. This is majorly used to find out whether the digital signature is authentic or not without making use of the private key. In the case of Bitcoin, these keys can be found in either of the two states: compressed or uncompressed.

*Signature:* It is a number that acts as proof of operation once the signing takes place. This is generated mathematically by two numbers, one being the hash of the transaction that will be signed and the second being the private key itself. The signature consists of two parts s and r. If one has the public key, then using a predefined algorithm, anyone verifies whether the signature was formed by the hash and the private key and this process does not include private key at all. Signatures are 71, 72, or 73 bytes in length with probabilities are of 25%, 50%, and 25%, respectively.

### *ETHASH*

Blockchain currencies that are based on Ethereum use ETHASH (Ghosh et al., 2020) as their PoW function. ETHASH uses a hash function called Keccak which is later on made to be similar to SHA-3 although the two are not similar. This function resists ASIC through memory-hardness and can be verified with fewer efforts. To remove computational overhead, it makes use of Dargger-Hashimoto hashes which are changed according to the needs of ETHASH (Jakobsson & Juels, 1999).

## Security challenges

Even though the blockchain is a ground-breaking and succeeding technology, it is associated with a substantial number of issues and challenges (Ghosh et al., 2020). In the research works (Bose et al., 2019; Di Battista et al., 2015), the authors came up with the following challenges for the usage and acceptance of this blockchain technology.

### *Usability*

Thorough analysis of Bitcoin flow and the Bitcoin user group in the network will give the correct outline of the percentage of usability. Moreover, the analysis of Transaction validity checking will show the usability

performance. Thus, addressing the usability issue is an evolving challenge for the researchers.

### *Size and bandwidth*

The Bitcoin size is continuously increasing since the year it was created, i.e. from the year 2009 and it has reached approximately 269.82 GB at the end of September 2019. When throughput performance is increased, the blockchain size can rise 214 PB every year. Hence, this issue leads to the existence of a constraint for the number of transactions that can be managed. If the number of transactions is more, then size and bandwidth issues have to be resolved (Barkatullah & Hanke, 2015; Ghosh et al., 2020; Jindal et al., 2019; Kaur et al., 2018).

### *Privacy and security*

In recent days, it is observed that blockchain has more possibility of the 51% attack in which one participant will have full control over more portions of the mining hash-rate of the network. Besides, that entity will have the ability to update or alter the blockchain. This issue is remaining as a vital security challenge for researchers (Ghosh et al., 2020).

### *Versioning, multiple chains, and hard forks*

If the chain on the Bitcoin network consists of fewer entities, then there will be more possibility of occurrence of the 51% attack. Moreover, if the chains are divided for versioning or managerial reasoning, then it will lead to an additional problem (Ghosh et al., 2020).

### *Wasted resources*

To mine Bitcoin, more resources are needed due to the usage of the PoW scheme. Alternatively, the PoS scheme can be used. In the PoW scheme, mining depends on the miners and the amount of work done by them (Ghosh et al., 2020; Shojafar et al., 2019). In the case of the PoS scheme, the amount of Bitcoin held by a miner counted as resources used. Thus, the issue with the wasted resources has to be solved for more production in the blockchain network.

### *Latency*

To achieve security efficiency, more time is spent in one block itself to avoid the double-spending attack. Thus, to avoid security attacks, more

time is spent in successfully executing the transactions. However, this issue remaining as a research challenge for the satisfaction of participants (Ghosh et al., 2020).

### *Throughput*

In recent years, the throughput of the Bitcoin network is raised to seven transactions per second (tps). If the throughput of competing applications is more, and the growth of blockchain transactions is high, then increasing the throughput of blockchain networks must be a challenge (Ghosh et al., 2020).

## Conclusion

One of the most famous cryptocurrencies is Bitcoin which not only attracted the best people, fascinated by the idea of decentralized blockchain but also attracted people to misuse the blockchain interconnections. There are 5,563 different cryptocurrencies in the world, and the number is growing every day. However, Bitcoin has always outshone every other when it comes to usage, and that makes it a prime objective for black-hat hackers to conduct various malpractices against the same. The review resulted in findings, such as how protocols related to Bitcoin works, including PoW and making the whole concept decentralized therefore every user needs to agree on a transaction, and this keeps the people who are using it safely. However, these set-of-rules become a loophole and a breaking point that is exploited by people with wrong intentions. The attacks which can affect Bitcoin are discussed and the countermeasures are also presented. The existing research works on Bitcoin discussed different ways in which some of the cyber attacks can be mitigated and dealt with. However, when it comes to the total security of Bitcoin and the secured functioning of blockchain, no procedure can ensure that. The decentralized concept of blockchain has resulted in problems concerned with privacy and the characteristics of anonymous users.

In summary, this review article is a work to bring up the privacy and security problems in various areas of cryptocurrency. After defining the architecture of Bitcoin and a breakdown of the working of it, this review highlights the privacy and security that can be witnessed at different stages of the working, from creating the transaction to adding the transaction to the blockchain. This work explored the problem of privacy concerned to an individual user and anonymous users in the world where cryptocurrencies and their usage are increasing exponentially. Besides, security challenges in the Bitcoin network are discussed

to outline the open research challenges as well as hoping that this study will motivate the researchers to initiate the research in this interesting domain.

## References

All you need to know about Bitcoin - Bitcoin Forum. (2018). Retrieved March 30. https://bitcointalk.to/index.php?topic=1177304.0;prev_next=next

Andrychowicz, M., Dziembowski, S., Malinowski, D., & Mazurek, Ł. (2015). *On the malleability of bitcoin transactions. Financial cryptography and data security: FC 2015 international workshops, BITCOIN, WAHC, and wearable* (pp. 1–18). Springer.

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016, August). Medrec: Using blockchain for medical data access and permission management. *In 2016 2nd International Conference on Open and Big Data (OBD)* (pp. 25–30). IEEE.

Bamert, T., Decker, C., Wattenhofer, R., & Welten, S. (2014, September). Bluewallet: The secure bitcoin wallet. In *International workshop on security and trust management* (pp. 65–80). Springer.

Barkatullah, J., & Hanke, T. (2015). Goldstrike 1: CoinTerra's first-generation cryptocurrency mining processor for bitcoin. *IEEE Micro*, *35* (2), 68–76. https://doi.org/10.1109/MM.2015.13.

Bentov, I., Lee, C., Mizrahi, A., & Rosenfeld, M. (2014). Proof of activity: Extending bitcoin's proof of work via proof of stake. *ACM SIGMETRICS Performance Evaluation Review*, *42*(3), 34–37. https://doi.org/10.1145/2695533.2695545.

Biryukov, A., Khovratovich, D., & Pustogarov, I. (2014). Deanonymisation of clients in bitcoin p2p network. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Ser. CCS '14* (pp. 15–29). ACM.

Bissias, G., Ozisik, A. P., Levine, B. N., & Liberatore, M. (2014). Sybil resistant mixing for bitcoin. *Proceedings of the 13th Workshop on Privacy in the Electronic Society, Ser. WPES '14* (pp. 149–158). ACM.

Bonneau, J. (2016). *Why buy when you can rent? International conference on financial cryptography and data security* (pp. 19–26). Springer.

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. *Security and Privacy (SP), 2015 IEEE Symposium* (pp. 104–121). IEEE.

Bose, A., Singh Aujla, G. S. M., Kumar, N., & Cao, H. (2019). Blockchain as a service for software-defined networks: A denial of service attack perspective. *2019 IEEE International Conference on Dependable, Autonomic and Secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Cloud and Big Data Computing, International Conference on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)* (pp. 901–906). IEEE.

Chaudhary, R., Jindal, A., Singh Aujla, G., Aggarwal, S., Kumar, N., & Raymond Choo, K. K. (2019). BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system. Computers & *Security*, *85*, 288–299. https://doi.org/10.1016/j.cose.2019.05.006

Chohan, U. (2017). Cryptocurrencies: A brief thematic review. https://doi.org/10.2139/ssrn.3024330

Conti, M., Kumar, E. S., Lal, C., & Ruj, S. (2018). A survey on security and privacy issues of bitcoin. *IEEE Communications Surveys & Tutorials*, *20*(4), 3416–3452. https://doi.org/10.1109/COMST.2018.2842460.

Corbixgwelt. (2011). *Timejacking and bitcoin*. http://culubas.blogspot.de/2011/05/timejacking-bitcoin802.html.

Cynthia, D., & Moni, N. (1993). Pricing via processing, or, combatting junk mail, advances in cryptology. *CRYPTO'92: Lecture Notes in Computer Science No. 740* (pp. 139–147). Springer.

Dai, F., Shi, Y., Meng, N., Wei, L., & Ye, Z. (2017). From bitcoin to cybersecurity: A comparative study of blockchain application and security issues. *2017 4th International Conference on Systems and Informatics (ICSAI)* (pp. 975–979). IEEE.

Danezis, G., Dingledine, R., & Mathewson, N. (2003, May). Mixminion: Design of a type iii anonymous remailer protocol. In *2003 Symposium on Security and Privacy* (pp. 2–15). IEEE.

Di Battista, G., Di Donato, V., Patrignani, M., Pizzonia, M., Roselli, V., & Tamassia, R. (2015). Bitcoin review: Visualization of flows in the bitcoin transaction graph. *Visualization for Cyber Security (VizSec), 2015 IEEE Symposium* (pp. 1–8). IEEE.

Dikshit, P., & Singh, K. (2017). Efficient weighted threshold ECDSA for securing bitcoin wallet. *2017 ISEA Asia Security and Privacy (ISEASP)* (pp. 1–9). IEEE.

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. *IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom workshops)* (pp. 618–623). IEEE.

Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016). *"A case study for Blockchain" Healthcare: Medrec prototype for electronic health records and medical research data.* https://www.media.mit.edu/publications/medrecwhitepaper/.

Gennaro, R., Goldfeder, S., & Narayanan, A. (2016). Threshold-optimal DSA/ECDSA signatures and an application to bitcoin wallet security. *Applied Cryptography and Network Security: 14th International Conference* (pp. 156–174). ACNS 2016. Springer International Publishing.

Ghosh, A., Gupta, S., Dua, A., & Kumar, N. (2020). Security of Cryptocurrencies in blockchain technology: State-of- art, challenges and future prospects. *Journal of Network and Computer Applications*, *163*, 102635. https://doi.org/10.1016/j.jnca.2020.102635.

Goldfeder, S., Bonneau, J., Felten, E. W., Kroll, J. A., Narayanan, A. (2014). *Securing bitcoin wallets via threshold signatures.* http://www.cs.princeton.edu/stevenag/bitcointhresholdsignatures.pdf.

Huckle, S., Bhattacharya, R., White, M., & Beloff, N. (2016). Internet of things, blockchain, and shared economy applications. Procedia *Computer Science*, *98*, 461–466. https://doi.org/10.1016/j.procs.2016.09.074.

Hurich, P. (2016). The virtual is real: An argument for characterizing bitcoins as private property. *Banking & Finance Law Review*, *31*, 573.

Jakobsson, M., & Juels, A. (1999). *Proofs of work and bread pudding protocols. Communications and multimedia security* (pp. 258–272). Kluwer Academic Publishers.

Jarecki, S., Kiayias, A., Krawczyk, H., Xu, J. (2016). Highly-efficient and composable password-protected secret sharing (or: How to protect your bitcoin wallet online). *2016 IEEE European Symposium on Security and Privacy*. IEEE.

Jindal, A. S., Aujla, G., & Kumar, N. (2019). SURVIVOR: A blockchain-based edge-as-a-service framework for secure energy trading in SDN-enabled vehicle to-grid environment. Computer *Networks*, *153*, 36–48. https://doi.org/10.1016/j.comnet.2019.02.002.

Johnson, B., Laszka, A., Grossklags, J., Vasek, M., & Moore, T. (2014). Game-theoretic analysis of DDoS attacks against bitcoin mining pools. Financial cryptography and

data security: FC 2014 workshops, BITCOIN and WAHC (Vol. 2014, pp. 72–86). Springer.

Johnson, D., Menezes, A., & Vanstone, S. (2001). The elliptic curve digital signature algorithm (ECDSA). *International Journal of Information Security*, *1*(1), 36–63. https://doi.org/10.1007/s102070100002.

Karame, G. O., Androulaki, E., & Capkun, S. (2012, October). Double-spending fast payments in bitcoin. In *Proceedings of the 2012 ACM conference on computer and communications security* (pp. 906–917).

Kaur, H., Kumar, N., & Batra, S. (2018). An efficient multi-party scheme for privacy-preserving collaborative filtering for healthcare recommender system. *Future Generation Computer Systems*, *86*, 297–307. https://doi.org/10.1016/j.future.2018.03.017.

Koshy, P., Koshy, D., & McDaniel, P. (2014). An analysis of anonymity in bitcoin using p2p network traffic. Financial *Cryptography* and *Data Security*: 18th *International Conference* (pp. 469–485). Springer.

Lee Kuo Chuen, D. (Ed.). *Handbook of digital currency* (1st ed.). Elsevier.

Markus, J., & Ari, J. (1999). *Proofs of work and bread pudding protocols. Communications and multimedia security* (pp. 258–272). Kluwer Academic Publishers.

Maxwell, G. (2013, March). *Coinjoin: Bitcoin privacy for the real world*. https://bitcointalk.org/index.php?topic=279249.0

McCorry, P., Shahandashti, S. F., & Hao, F. (2017). Refund attacks on bitcoin's payment protocol. Financial *Cryptography* and *Data Security*: 20th *International Conference* (pp. 581–599). Springer.

Merkle, R. C. (1987). A digital signature based on a conventional encryption function. Conference on the *Theory* and *Application* of *Cryptographic Techniques* (pp. 369–378). Springer.

Miller, A. (2013). *Feather-forks: Enforcing a blacklist with sub-50% hash power*. https://bitcointalk.org/index.php?topic=312668.0

Mills, D., Martin, J., Burbank, J., & Kasch, W. (2011). *Network time protocol version 4: "Protocol and algorithms Specification", rfc 5905, internet engineering task force*. http://www.ietf.org/rfc/rfc5905.txt

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). B*itcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.

Ruffing, T., Moreno-Sanchez, P., & Kate, A. (2014). Coinshuffle: Practical decentralized coin mixing for bitcoin. *ESORICS 2014: 19th European Symposium on Research in Computer Security* (pp. 345–364). Springer International Publishing.

Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Nyang, D., & Mohaisen, A. (2019). *Overview of attack surfaces in Blockchain. Blockchain for distributed system security* (pp. 51–66).John Wiley & Sons.

Shojafar, M., Cordeschi, N., & Baccarelli, E. (2019). Energy-efficient adaptive resource management for real-time vehicular cloud services. *IEEE Transactions on Cloud Computing*, *7*(1), 196–209. https://doi.org/10.1109/TCC.2016.2551747

Szabo, N. (2017). *Smart contracts: Building blocks for digital markets, 1996*. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials*, *18*(3), 2084–2123. https://doi.org/10.1109/COMST.2016.2535718.

Vasek, M., Thornton, M., & Moore, T. (2014). Empirical analysis of denial-of-service attacks in the bitcoin ecosystem. Financial *Cryptography* and *Data Security*: FC 2014 *Workshops*, BITCOIN and WAHC (pp. 57–71). Springer.

Vyas, C. A., & Lunagaria, M. (2014). Security concerns and issues for Bitcoin. The Proceedings of National Conference cum Workshop on Bioinformatics and Computational Biology. NCWBCB.

Wheatley, M. (2018). *Bitcoin: Architecture, malware, and platforms –what are the real threats? – AlleyWatch*. [online] AlleyWatch. http://www.alleywatch.com/2013/10/bitcoin-architecture-malware-and-platforms-what-are-the-real-threats/.

Wuille, P. (2014). *Bip 62: Dealing with malleability*. https://github.com/bitcoin/bips/blob/master/bip-0062.mediawiki.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. *Big Data Congress, 2017 IEEE International Congress* (pp. 557–564). IEEE.