ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY
February 2020, Vol 13(07), 767 – 786
DOI: 10.17485/ijst/2020/v13i07/149691,

Bitcoin's Blockchain Peer-to-Peer Network Security Attacks and Countermeasures

Mahmoud Mostafa[1,2,*]

[1]Information Systems Department, Faculty of Computers and Information, Helwan University, Helwan, Egypt
[2]Department of Information Technology, College of Computers and Information Technology, Taif University, Al-Hawiya, Saudi Arabia

Article Type: Article

Article Citation: Mahmoud Mostafa. Bit coin's block chain peer-to-peer network security attacks and countermeasures. *Indian Journal of Science and Technology*. 2020; 13(07), 767-786. DOI: 10.17485/ijst/2020/v013i07/149691

Received date: December 12, 2019

Accepted date: February 1, 2020

***Author for correspondence:**
Mahmoud Mostafa ✉ mahmoud.mostafa.m@gmail.com, mahmoud.m@tu.edu.sa 📍 Information Systems Department, Faculty of Computers and Information, Helwan University, Helwan, Egypt

Abstract

Objectives: The main objective of this work is familiarizing users and researchers about Bitcoin's blockchain peer-to-peer network system and investigating security attacks that threat this critical financial digital cash network. **Method:** A comprehensive research analysis was conducted to identify Bitcoin's blockchain peer-to-peer network security attacks and possible countermeasures to protect the Bitcoin network against such attacks. This bibliographical survey covers the related research works from the launch of blockchain in 2008 until the end of 2019. **Results:** This study investigates eleven attacks that threaten Bitcoin's blockchain peer-to-peer network systems and presents the possible countermeasures to defend these attacks. **Conclusion:** The conclusion obtained is encouraging the researchers to explore this hot research area. Besides, the study provides perspectives for future research directions in this domain.

Keywords: Bitcoin, Blockchain, Cryptocurrency, Security, Attacks, Countermeasures.

1. Introduction

In this technological era, we have seen a great deal of increasing interest in the digital world. The sector of financial services has also joined this growing trend by introducing crypto currencies as a digital payment method. By enabling the digital crypto currencies to be distributed but not duplicated, the blockchain innovation made the foundation of a new type of internet.

Bitcoin online virtual crypto currency is the first and most used application of blockchain technology. This technology benefits from the decentralized nature of the peer-to-peer network combined with modern cryptographic techniques to allow asset transfer between buyers and sellers without involving trusted third-party banking systems. Bitcoin crypto currency shapes the future of the world digital economy.

Blockchain technology was initially formulated for Bitcoin digital currency, however, now we discovered other potential uses of this innovation in many fields such as healthcare [1], Internet of Things (IoT) [2], e-voting [3], and supply chain management [4] systems.

In [5] 2008, Satoshi Nakamoto introduced Bitcoin as an electronic peer-to-peer network system. The currency became completely functional in 2009. Being the most widely used virtual currency [6], Bitcoin can be utilized to buy various products/services from a developing roster of traders including companies like Overstock.com, Expedia and various other platforms that accept Bitcoin as payment method [7]. The currency can also be traded with other private clients as consideration for different types of services. The user can also swap for other currency types that include both virtual and traditional currencies, on the electronic exchanges that operate like forex exchanges. As the most popular virtual currency money by a great margin, the currency has far more prominent liquidity than other virtual currencies. This enables clients to hold the vast majority of its inherent worth when exchanging over to traditional currencies, for example, the Euro and U.S. dollar [8]. However, the tremendous success of Bitcoin lured attackers to target its networks for criminal profits.

Regardless of high-visibility prosecutions of the most appalling offenders, the Bitcoin remains attractive to the gray market members and criminals. Moreover, with the blockchain innovation has been greatly utilized, different sorts of attacks and security issues have developed. Such as, we have seen many cases of a large number of virtual currencies being stolen, exchanges have been attacked and various other security issues [9]. The prominence of blockchain technology makes new demands on security solutions [10]. Due to the recent trend in digital currency theft, hackings, and security issues with user accounts, it is vital to establish appropriate security solutions to enhance the security measures of the Bitcoin's blockchain technology.

Since Bitcoin has been introduced in January 2009, 1560 blockchain platforms have been included in this market [11]. Such blockchain systems are used for various purposes, such as for digital payments or utilization of cryptocurrency to perform particular business transactions e.g., to accept payment for their services or products. With the utilization of this digital payment opportunity, pretty much all the open blockchain platforms have developed the digital currencies economy at a huge rate. Various types of network attacks including Distributed Denial-of-Service (DDoS) attack, Sybil attack, double-spending, transaction malleability, and attacks on mining pools, etc. encourage great privacy and security concerns in the crypto currency market. According to a recent study on Mt. Gox, which is well known Tokyo Bitcoin exchange platform, announced losses of 4.6 million US dollars' because of transaction vulnerability hack in Bitcoin in April 2013 and another loss of 470 million USD because of cyber-attack in 2014 [12]. This lead the company to face bankruptcy. Another case is the Hong-Kong-based Bitcoin trade, which announced losses of 65 million US dollars because of hacking in August 2015 [12]. Moreover, in January 2018, Japan-based Coin check, a large digital crypto currency exchange, was hacked and got losses of 534 million US dollars' value XEM. As indicated by the report of Imperva Incapsula, over 73 percent of particularly Bitcoin platforms utilizing their services were hacked in 2017 [13].

These cases and many others mandate the investigation of security threats and attacks vectors that threaten blockchain systems to provide adequate countermeasures to save guard such critical systems.

Bitcoin blockchain was initially provided as an open-source code that has been modified and extended to add new features and propose new crypto currency. This opens the door for many alternative coins (altcoin) to appear. Namecoin [14], Ethereum [15], NEO [16], Litecoin [17], and Zcash [18] are examples of alternative crypto currencies. Even though several crypto currencies are being used today, however, the leading crypto currency Bitcoin is by far the most well-known as well as broadly utilized currency. This why this article focuses on Bitcoin, hence it is the mother of other successors alternative digital coins.

The rest of this article is organized as follows: Section 2 provides background about Bitcoin's blockchain technology. Section 3 presents Bitcoin's blockchain peer-to-peer network security attacks and possible countermeasures. Section 4 concludes the article and provides perspectives for future research directions.

2. Overview of Bitcoin

Bitcoin is the most popular crypto currency that is controlled by a decentralized system of peer-to-peer network. Unlike traditional banking systems, the currency is not directly dependent upon the control of the national governments or central banking authorities. Bitcoin blockchain system uses a multitude of techniques including peer-to-peer network, Cryptography, algorithms, mathematics, distributed consensus protocol, and economic model [19].

This section covers wallet, transaction processing, mining, blockchain, proof-of-work consensus protocol and peer-to-peer networking infrastructure involved in the Bitcoin.

2.1. Bitcoin Wallet

Each Bitcoin holder must have a pair of keys. The Elliptic Curve Digital Signature Algorithm (ECDSA) [20] is used to generate those two keys. The public key is used as an individual unique address. While the other key is kept private and is used by the Bitcoin holder to sign transactions and proof his ownership of certain Bitcoin. Normally, these credentials are stored on off-line or on-line wallet [21]. This pair of keys is not linked to a person's real identity. While this provides anonymity, the loss of this pair of keys means a permanent loss of owned Bitcoin because there is no another way to prove the ownership relation. Wallet theft or loss is an important challenge that needs to be addressed [22].

2.2. Transaction Processing and Mining

As illustrated in Figure 1, when a Bitcoin holder (buyer) wants to transfer some money to another bitcoin holder (seller) to pay for products or services. He has to create a transaction that contains the amount of Bitcoin to be transferred and the public key of the seller as it

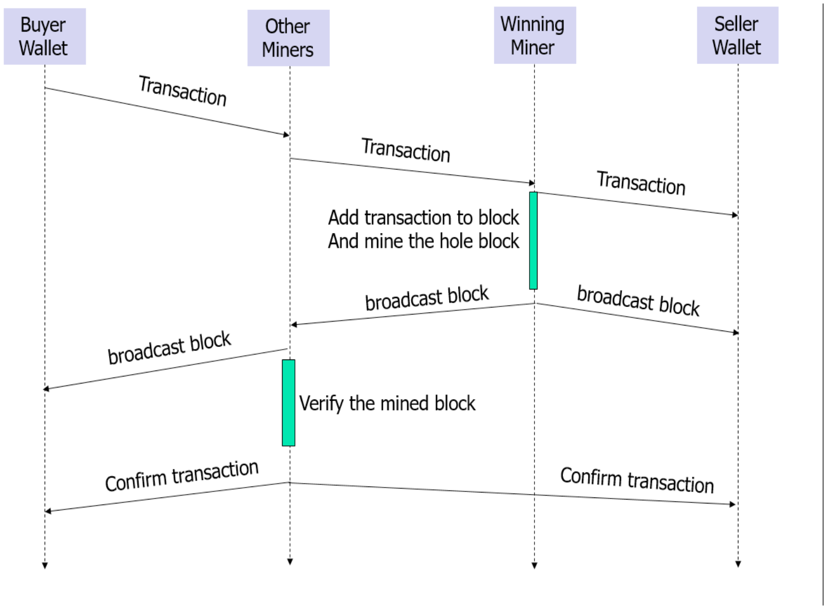

FIGURE 1. Bitcoin transaction processing.

uniquely identifies its Bitcoin wallet that will receive the transferred amount. In addition, the sender must sign the transaction with his own private key to prove his ownership of this Bitcoin. Then, he sends the transaction to the seller and broadcast it to all nodes on the network [5].

Some nodes in the network act as miners, their job is to verify the transaction, check its ownership and be sure it was not spent before to prevent double-spending [23]. Miner groups valid transactions into a block and start mining that block. To mine a block, miners try to solve a complex cryptographic puzzle that is hard to compute but easy to verify. The first miner that manages to solve the puzzle is the winning miner. Instantaneously, he broadcast the mined block to other nodes.

Other miners verify the received block and confirm it; this is implicitly verifying all its contained transactions. So, multiple messages sent from different miners to other nodes confirming the block and their contented transactions. When the seller receives a confirmation, he could release the service or ship the products. However, it is better to wait until receiving multiple confirmations to mitigate double-spending Finney [24] and Vector 76 [25] attacks.

When there is a consensus from the majority of miners on the validity of the block, it is appended to the chain of blocks previously mined and the ownership of bitcoin is transferred to the seller wallet.

If a whole block or a transaction within a block is considered invalid by the majority of miners, the whole block is rejected and not appended to the main chain.

In some cases, two miners may independently append different validated block to the end of their copy of the blockchain. This causes a fork to happen and we get two different branches with equal length. Although, blockchain forking is not desired as it is used as a vehicle for double-spending [23] and mining attacks [26], miners are free to continue mining and append to any of these two forks. However, after some time all miners rejoin the longest chain and forking is terminated as the shortest branch of blockchain is discarded.

Transactions through Bitcoin always require the transaction fee for confirmation. This transaction fee is collected by the first Bitcoin miner that mines the particular block containing transaction; this activity is additionally what gives the transactions its initial confirmation. The transaction fee varies according to how big (in bytes) the transaction is, how fast the user needs a transaction to be affirmed, and furthermore on the existing network conditions. At this point, paying the fixed fee, or even the fixed fee for per kB, is a pretty bad idea; here, all Bitcoin wallets utilize a few bits of information to evaluate a proper fee for the user, however, some are greater at the fee estimation than others [27]. Moreover, the transaction fee also relies upon the data size of the transaction. The transaction fee, however, does not rely upon the Bitcoin measure of the transaction, as bitcoin system does not mandate the existence of transaction fee. One major problem caused by transaction fee is that transactions with lower fees suffer from starvation, as miners prefer to serve higher fees transactions to gain more coins.

Currently, it is not regular to find individual miners. As the mining process requires high computing power and consumes a lot of electrical power, miners work together forming mining pool. This increases their chance in mining competition and hence, winning block mining award and their transactions associated fees that will be shared between pool members based on certain criteria [28].

2.3. Blockchain

The blockchain can be considered as an open distributed database of all the prior Bitcoin exchanges that are stored in particular groups called blocks. Blockchain is an immutable (tamper-proof) public shared digital ledger that is used to record and validate digital transactions. Bitcoin transactions are recorded into blocks. Those blocks are linked to each other to form blockchain. The blockchain of Bitcoin is essential to its function.

Each block consists of a header and a body part. The set of validated transactions are stored in the block body. While block header contains the version number, time stamp, nonce, block hash value calculated using SHA-256 and merkle tree root hash. Merkle tree is a binary tree data structure that stores the hash of all transactions stored on block body [29].

The hash value of the previous block is used as an input to generate the hash of the current block. In this way, blocks are linked in a chain from the beginning to the last block. This makes the blockchain hard to temper-with. No entity can modify or erase a block from the chain. In this sense, blockchain is immutable. Moreover, it is traceable; any one can trace back and verify the history of any stored assets or transactions.

2.4. Proof-of-Work Consensus Protocol

Consensus protocols are considered to be the most significant and revolutionary parts of blockchain innovation. These consensus protocols make an evident arrangement of understanding between different nodes involved across the distributed system while averting the exploitation of the framework. Consensus protocols perform an imperative part in the processing of Bitcoin transactions. Consensus protocols used in blockchain are what keep each node on the system synchronized with each other [30].

In order to solve the synchronization problem that exists in traditional decentralize database systems, blockchain uses proof-of-work (PoW) consensus algorithm [31]. PoW allows blockchain peer-to-peer network nodes to work collectively in order to reach a general agreement on either to accept or reject certain transaction or block of transactions.

To mine a block of transactions, miners compete to solve mathematical cryptographic puzzle. They must find the nonce value that is when used as input to SAH-25 hashing algorithm along with other block-hashed contents will produce a hash value less than a declared desired value. To reach this nonce value, miners use a brute force technique that takes a lot of time and consumes high electrical power. The obtained nonce value that solves the puzzle is stored on block header. It is considered as proof of performed mining work and hence it is called proof-of-work (PoW) [31].

The benefit of using this mechanism comprises of the fact, that it is pretty easy to check the outcome: Given the payload and a particular nonce, just a single call of the hashing function is needed to confirm that the hash includes the required properties. As there is no other method to discover such hashes other than the brute force method, this can be utilized as a "proof-of-work" that someone contributed a great deal of computing capacity to figure out the right nonce for this payload [31]. This method involved in the proof-of-work feature is then utilized in the Bitcoin system to enable the system to come to a consensus on the transaction's history. So, in this case, if the attacker aims to rewrite the history will need to first cover the required proof-of-work before the function will be accepted.

2.5. Bitcoin's P2P Networking Infrastructure

In [32–34] the beginning stages of Bitcoin, the currency was defined as the peer-to-peer electronic cash system. Bitcoin can be transferred from one entity to another using the peer-to-peer network that deals with blockchain-distributed ledger. In this sense, the peer-to-peer engineering that is intrinsic to blockchain innovation is the thing that permits Bitcoin and different digital forms of money or valued assets to be moved around the world, without the requirement for particular mediators or any central server. Peer-to-peer network grants blockchain the decentralized self-regulating natures.

In [33–35] this peer-to-peer network, anybody can set up a Bitcoin node in case they wish to join the procedure of validating and verifying blocks. Along these lines, no banks are handling or recording exchanges in the Bitcoin processing involved. Rather, the blockchain goes about as an advanced record that openly records all the transactions activity. Moreover, every hub involved in the processing can hold a duplicate copy of the blockchain and compares it to different hubs to make sure that the information is correct. The peer-to-peer infrastructure rapidly dismisses any inaccuracy or malicious activity. The high redundancy natures that exist on the blockchain peer-to-peer network make it fault tolerance. It can easily recover from any disasters as duplicate copies of blockchain stored in a multitude of nodes distributed all over the network and all generated transactions are broadcasted to all network nodes.

When a new node wants to join the Bitcoin blockchain network, the two peers establish an application-level handshake using underlying persistent TCP transport layer protocol. Each node has a list of the Domain Name System (DNS) servers. It can contact any of these DNS servers to request a list of current peers IP addresses to be connected to. The first contacted DNS server is called Seeder. This later provides the newly joining node with an initial list of other peers' IP addresses in a process called bootstrapping. The initial list of peers that have-not been contacted before by this node is stored in the "new table" of the address manager (addrman) database. This database has another table called "tried table". The later table stores the addresses of all previously contacted peers [36].

If the newly joining node fails to contact any DNS seeder, it can use the list of hard code IP addresses called seeds. Each node is allowed to simultaneously establish up to eight outgoing connections and accept up to 117 incoming connections with other nodes.

For a node (A) to establish a connection with another node (O). It first, randomly selects an IP address from the new table. This random selection process allows the network structure to remain unknown and provides dynamism. Moreover, randomly selecting peers to minimize the possibility of Sybil and eclipse attacks.

As illustrated in Figure 2(a), to establish an outgoing connection, node (A) sends version message to node (O). This message contains node (A) bitcoin's protocol version, its IP address and a timestamp necessary to perform inter nodes time synchronization. Bitcoin nodes are configured to listen to port 8333 for incoming messages.

Upon the receiving of version message, if node (O) accepts the connection, it replies with version acknowledgment (verAck) and version message consecutively. Finally, node

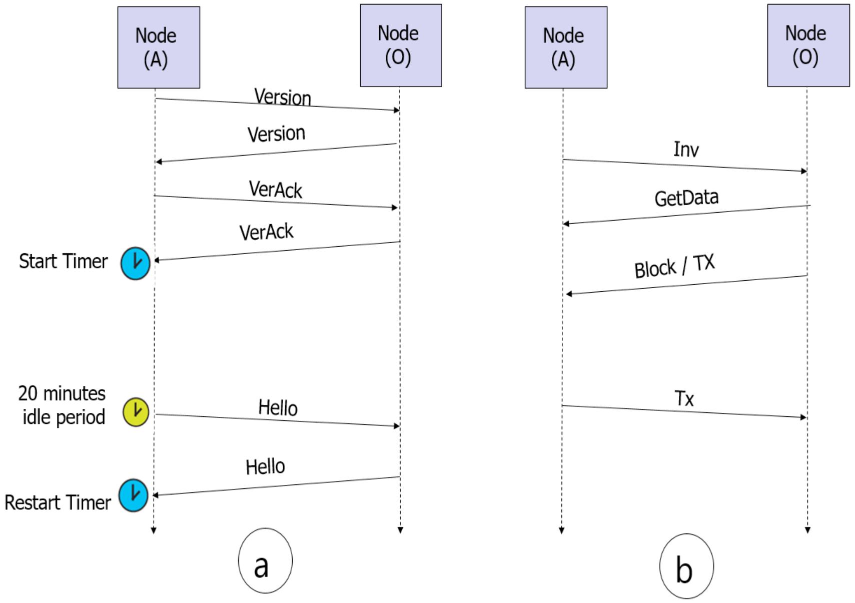

FIGURE 2. Bitcoin blockchain nodes (a) connection establishment and (b) data transfer.

(A) responds with a verack message and the connection is established. After successfully establishing the connection the IP address of each node is moved to the tried table on the other node and they start exchanging data transfer. To refresh the connection, after an idle period of 20 min, a hello message is sent.

As shown in Figure 2(b), to announce a new verified transaction or a mined block, the node sends a broadcast inventory (inv) message to the other connected nodes. Upon receiving inv message from the node (A) each node checks if it already received the transaction or the block from any other connected node, otherwise, it (node (O)) sends GetData message to request the transaction or the block from node (A). In response to this GetData request, node (A) sends the required transaction or block. If a node (A) is the initiator of a transaction, it directly floods the connected nodes with the Tx message congaing its newly generated transaction. In this way, transactions and blocks are propagated to all nodes in the network. These exchanged messages are transferred using an unencrypted TCP connection. A message may be intercepted, delayed and/or dropped maliciously or due to networking problems. Therefore, the quality of service requirements of the network should be considered for the proper functioning of the Bitcoin system. Malicious attacks and their countermeasures are described in the next section.

3. Attacks and Countermeasures

While there is a multitude of threats targeting Bitcoin systems such as double-spending [23], mining [36], smart contracts [37], and wallet theft [22] attacks. These attacks are out of scope of this article. This article focuses on various types of network attacks exist in Bitcoin's blockchain peer-to-peer network and presents appropriate countermeasures to deal with these attacks. While there are various other surveys on security issues in Bitcoin and blockchain security [38–43]; however, they lack extensive information about various attacks involved in Bitcoin's blockchain peer-to-peer network. This article provides a comprehensive coverage of such attacks. Table 1 summarizes these attacks and their countermeasures.

TABLE 1. Bitcoin's blockchain peer-to-peer network security attacks and countermeasures

Attack	Description	Affected entities	Countermeasures
DDoS [13,44]	Multiple machines are directed to exhaust the resources of a single machine.	Users, miners and exchange websites	Using proof-of-work [5]
Time jacking [48]	Attacker modifies the system time counter of some nodes causing miners to loss their resources by letting them mine outdate blocks	Miners	Confining acceptance time ranges, utilizing NTP or the nodes' internal machine time [49]

Tampering with message body [50]	Hacker alters some specific parts of the exchange. This facilitates DoS and double spending attacks.	Users and miners	The use of end-to-end integrity and improving block request management [51]
Transaction malleability [52]	Hacker changes the Bitcoin's transaction ID before making a confirmation causing double withdrawal or double deposit	Bitcoin exchange companies	Segregated Witness protocol [53]
Routing [54–56]	Partitioning routing attack splits Bitcoin networks into separate segments with the goal that no information can be transferred among them. While delayed routing delays blocks propagation causing DoS and wasting mining powers	Users, miners and Bitcoin network	End-to-end encryption [58]
Fake bootstrapping [59]	A malicious bootstrap node impacts the network view for the newly joining node	Users and miners	Using cached peers, utilizing 8 outgoing connections on each bootstrap, querying commonly used DNS nodes or hardcoded nodes [60].
Sybil [61]	The victim node of Sybil attack is bounded by fake nodes. These fake nodes isolate the victim and close up all its exchanges to the network. this facilitates double Spending, DDoS, time jacking, attacks,	Users, miners and Bitcoin network.	Two-party mixing protocol (Xim) [62]
Eclipse [63]	All incoming and outgoing connections of the victim's node are redirected to IP addresses managed by attacker	Users, miners and Bitcoin network	periodically make "feeler" connections to test the IP addresses in the "New Nodes" and only promote valid nodes to "Tried Nodes" [36]
Refund [64]	The attacker claims the refunds on the customer's behalf without any permission from the customer	Users and merchants	Multisignature mechanism and mixing servers [65]
Punitive and feather forking [66]	When the hacker has most of the hash power of the system, he blacklists or censors victim's Bitcoin address so that the victim cannot be able to spend any Bitcoins.	Users	Open challenge
De-anonymization [67]	Record targeted node activities that enable the hacker to easily make the required profiles of a certain user.	Users	Anonymous signature [72], CoinShuffle [73], CoinJoin [74] and MixCoin [75]

3.1. Distributed Denial-of-Service Attack

DDoS attack is different from the DoS attack, such as in the DDoS attack, various malicious machines are directed to focus on the single resource. The DDoS attack is more likely to be fruitful in disrupting the objective than the DoS attack originating from a single source. Many bad actors generally favor this technique as it turns out to be increasingly hard to trace the attack back to the source as the attack originate from different points. In most cases, the DDoS attacks have been utilized to target internet servers of large corporations, for example, banks, online business retailers, and even significant public and government services. But, it is imperative to consider that any network, server, or device associated with the web could be a possible target for such types of attacks [13,44].

As digital currencies have become popular among the public, the crypto currency traders have become progressively prominent targets for the DDoS attacks. For instance, when the digital currency Bitcoin Gold formally launched, it promptly turned into the target of a large DDoS attack lead to affecting their web site for many hours. However, the decentralized nature of the block chains peer-to-peer network makes a solid defense against various DDoS attacks. Regardless of whether a few nodes disconnect or fail to communicate, the blockchain can keep working and approving exchanges. At the point when the disturbed nodes figure out how to recoup and return to function, they re-synchronize as well as catch up with the latest data, given by the nodes that were not affected. The level of protection each blockchain contains against such attacks is identified with the number of nodes and hash rate of the system. As the most popular and largely used virtual currency, the Bitcoin is considered the most secure blockchain platform among other digital currencies. This implies that network attacks like DDoS are considerably less likely to make interruptions in Bitcoin [45].

A great countermeasure to deal with DDoS attacks is using the proof-of-work [5] consensus algorithm as it ensures that all system information is secured by cryptographic proofs. This implies that it is almost impossible to change recently approved blocks. Modifying the Bitcoin blockchain blocks requires the whole structure to be unwound record-by-record that is practical impossibility even for most powerful computer systems. Moreover, to send a bogus block, a hacker needs to spend a lot of computing power to solve the PoW puzzle which makes such attack impractical.

In the worst case, a successful DDoS attack will only be able to change the exchanges of only a few of the most recent blocks and for a brief timeframe. Moreover, regardless of whether the DDoS attack manages to control over half of the Bitcoin hashing capacity to play out so-called 51 percent or more attack [46], the underlying protocol will quickly get updated as a reaction to that attack [47].

3.2. Time Jacking Attack

This attack exploits the hypothetical weakness in Bitcoin timestamp management. During the time jacking network attack, the attacker modifies the system time counter of node and enables the node to acknowledge an alternate blockchain. It can be accomplished when an attack adds various phony peers to the system with off base timestamps. Time jacking could be used to facilitate the double-spending attack. It also could consume computing power of competing miners by letting them mine outdate blocks [48].

The user can overcome this network attack by confining acceptance time ranges, utilizing the Network Time Protocol (NTP) or the nodes “internal machine time [49]”.

3.3. Tampering with Message Body

It is another imperative security issue involved in Bitcoin’s peer-to-peer networks. While utilizing multi-hop, the intermediate network nodes are able to change content of the relaying packet.

Tampering with the message body changes the hash as well as invalidates the proof-of-work. In this manner, tampering the message body is certainly not a possible Bitcoin blockchain attack because there are various modifications need to be implemented that are not simple to achieve in the Bitcoin blockchain [50].

However, it may involve a particular case in which such a sort of attack would be possible. Since the Bitcoin exchanges are still malleable, therefore, it is achievable for the hacker to alter some specific parts of that exchange having used the valid signature of the transaction [51]. The occurs for the most part because not every part of the exchange is signed (such as the signatures themselves are not signed).

As the malleability issue in Bitcoin occurs when a client is managing 0-confirmation exchanges, that is, exchanges that have been sent to the system, however, has not yet been incorporated into the block. Since exchanges are not yet in that block, the attacker can change its part, making another valid exchange that uses similar data inputs, however, a fake identifier has. At that point, if the transaction is within the protocol, in which the exchanges are recognized by their particular hash, then hacker assailant might have the option to utilize it at their advantage.

The user can make use of end-to-end integrity to detect such types of security attacks. In addition, the management of block request should be improved [51].

3.4. Transaction Malleability Attack

It is a network attack that allows an individual to change the Bitcoin’s transaction ID before making a confirmation on the Bitcoin. This tamper with makes it workable for the individual to pretend that their transaction is not completed and hence he trays to repeat it. In the case of Bitcoin exchanges, the transaction malleability attack can be utilized to make a double withdrawal or double deposit [52].

Authors in Ref. [52] proposed two imperative countermeasures to prevent any loss, such as required transaction confirmation and manual confirmation of the Bitcoin withdrawals from transactions. Recently, Segregated Witness protocol [53] was proposed to prevent transaction malleability attack. This protocol stores transaction signature in a separate witness field in Merkle tree data structure.

3.5. Routing Attacks

The routing attack is able to influence both individual nodes as well as the complete network. The routing attack aims to tamper with the exchanges before pushing forward to peers. It is not feasible for other nodes to detect the tampering as the attacker alters the network into separate sections that make them not able to contact with each other [54]. There are two types of routing attacks. These include partition attack that divides various nodes of the network into separate groups and delay attack that tampers with the propagating messages.

3.5.1. Partition Routing Network Attack

Through partitioning network attacks, the attacker objects at splitting Bitcoin networks into separate segments with the goal that no information can be transferred among them. In order to alter the network into separate segments, the attacker interrupts the traffic intended to Bitcoin nodes contained inside one of its components as well as drops the connection to other components.

At this point, the attacker depends on the vulnerabilities in Border-Gateway-Protocol, which is the only internet routing protocol being utilized today that does not authorize origin of the routing announcement [54–55].

Such attacks, normally referred to as Border-Gateway-Protocol BGP attacks, include getting a router to wrongly propose that it has an enhanced route to particular IP prefix. In the hijacking process when the IP prefixed goes after nodes in a single component, the attacker can successfully interrupt the traffic transferred among two components. In this way, the hacker can sever the connections efficiently to disconnect both components. With a partition routing network attack, the attacker can creates two parallel blockchains and hence waste mining-efforts of competing miners.

3.5.2. Delay Routing Network Attack

The Bitcoin nodes are intended to request a block from just a single peer to abstain overtaxing network with extreme block transmissions. However, from another peer, the block is again requested if that request is not responded after some time like about twenty minutes. Design decision then enables powerful network attack where everyone interrupting traffic of Bitcoin can delay the block propagation on its corresponding connections. In this process, the attacker tries to perform some basic changes to the content of (inv, get data, and tx) messages of Bitcoin [56].

As these messages are not cryptographically protected against the tampering, and the sender or receivers do not have any sign that the Bitcoin message has been altered. Delay routing attack facilitates double-spending attack and may delay the podcasting of mined block leading competing miners to loss their chance in gaining mining reward.

There are long-term and short-term countermeasures available against these routing attacks. Firstly, peer selections can make routing-aware. The Bitcoin nodes aim at increasing diversity of the internet path seen by its connections to reduce the risks of the attacker to interrupt these nodes. In addition to this, nodes are also able to monitor performance of the connections to look for an event like abrupt disconnections from various peers or uncommon delays in the block delivery. Such events can be used as an early sign of the routing attack and could, for example, lead to the establishment of extra randomly chosen connections [57].

In addition, countermeasures like end-to-end encryption can help as well especially for delay attacks. However, encryption method alone would not be appropriate to protect against the partition attacks as the attacker can still interrupt the encrypted Bitcoin connections to achieve their goal [58].

3.6. Fake Bootstrapping Attack

It is another critical security threat involved in Bitcoin's peer-to-peer networks. This security threat begins when a new node starts connecting the network. Here, the first node that contacts with the newly joining node is called a bootstrap node. If this bootstrap node is a malicious one, it can impact the network view for the newly joining node [59].

Various countermeasures are available for this issue, for example, not to rely in the solitary bootstrap node, utilizing external mechanisms, utilizing network layer solutions, utilizing particular bootstrapping services, or implementing random address probing.

The Bitcoin overcomes various bootstrapping problems by using the local-peer-database for all the solitary nodes involved in the network. In that manner, Bitcoin applies the majority of the countermeasures such as using cached peers for the successive connections, utilizing the stored peers, utilizing 8 outgoing connections on each bootstrap, not relaying on the bootstrap node, and utilizing external mechanism by querying commonly used DNS nodes. In [60] this case, if the DNS cannot be reached by the user, they can go for hardcoded nodes.

3.7. Sybil Network Attack

In Sybil attack, the adversary set up multiple different identifiers to a particular node. During the Sybil attack process, a hacker tries to take control of different nodes within the network. In this way, the victim node of Sybil attack is bounded by fake nodes. These fake nodes isolate the victim and close up all its exchanges to the network [61].

Detecting Sybil attack is not easy at all, however, the following actions can be implemented to detect the Sybil network attacks: rising cost of creating the new identities, setting up the requirement of trust to join the network. In Ref. [62], researchers proposed two-party mixing protocol Xim to protect against Sybil attack.

3.8. Eclipse Network Attack

The eclipse attack has a requirement of distributed botnet or control authority of plenty of IP addresses. If the attacker has these perquisites, the attacker can overwrite the addresses on the tried table and hold until the victim node is restarted. So, after restarting the procedure, all outgoing connections of the victim's node will be redirected to IP addresses managed by attacker [63].

An eclipse attack targets a specific node and sends them blocks of a private fork, while attempting to eclipse them from the rest of the network so that they do not see the main blockchain. Once a victim has been disconnected from the honest network, they are vulnerable to double-spending attacks. The attacker can spend the same coins on their private fork and the main fork, and nodes which have been eclipsed from the main fork may accept the former as valid.

An effective countermeasure to deal with the eclipse network attack is to periodically make "feeler" connections to test the IP addresses in the "New Nodes" and only promote valid nodes to "Tried Nodes" if they connect to an appropriate Bitcoin node [36]. It will help prevent an attacker from filling up "New Nodes" with the random addresses; the attacker will also need to run a node at each IP address they target to add to "New Nodes".

This mechanism of filtering IP addresses makes sure that the attacker can only slowly and probabilistically bring new IP addresses into the "Tried Nodes". Since both the 'Tried Nodes' and 'New Nodes' are randomly chosen, the attacker will, therefore, require to occupy both of these sections with running nodes to alter the data. In this manner, such measures increase the costs to the attacker by requiring them to acquire a batch of new IP addresses to change the data from the required sections.

3.9. Refund Attack

This attacks target the BIP70 payment protocol overseeing how sellers and clients perform installments in the Bitcoin network. In this case, a trader that learns a client's address can claim the refunds on the customer's behalf without any permission from the customer [64].

To prevent this attack, a proposal was provided to modify the BIP70 payment standard protocol by using multi signature mechanism and mixing servers [65]. The proposal emphasis the importance of providing the merchant with all the required evidence that can assist to verify that received refund during the process when protocol was embraced by the equivalent pseudonymous client who approved the payment.

3.10. Punitive and Feather Forking Attacks

In the punitive forking, the hacker's goal is to blacklist or censor user's Bitcoin address that is owned by specifically targeted individuals so that they cannot be able to spend any Bitcoins. This process works only when the hacker has most of the hash power of the system [66].

In Feather Forking Attack, the hackers show that they will not extend any chain containing instantly forks and blacklisted exchanges, and generate a long chain of blocks containing such exchanges to show up. It has been noticed that other miners are still forced to block the blacklisted exchanges since they boost the possibility that the miner will lose out their reward [66].

Punitive and feather forking attacks are still open challenge that needs to be addressed.

3.11. De-anonymization

De-anonymization or user profiling is an attack against user privacy. In different peer-to-peer networks, the hacker can attempt to record targeted node activities that enable the hacker to easily make the required profiles of a certain user. This process is particularly appropriate in any anonymous systems [67]. The Bitcoin gives pseudonymity by enabling its clients to get direct payments to their individual unique address that is not originally associated in any way to the user's identity. In Bitcoin, there are two specific properties that can be viewed as identifiers such as Bitcoin address and IP address. Bitcoin addresses are linked to users whereas IP addresses are used to identify the peers. Utilization of unique Bitcoin address for each new transaction at the Bitcoin platform is projected to give the unlink ability among various activities that a particular individual performs using this blockchain.

To perform de-anonymization and user profiling, hackers use three methods for execution of address clustering: analyzing Bloom filters [68], inspecting transaction graph [27,69] and utilizing data of the network layer [70–71]. In this manner, user profiling in Bitcoin normally gives room to various security issues such as the leakage of all user's transactions.

To provide countermeasures against de-anonymization attacks, an anonymous signature has been proposed [72], also a number of mixing services have been proposed such as Coin Shuffle [73], Coin Join [74], and Mix Coin [75]; however, each of these protocols has its own limitations.

4. Conclusion and Future Directions

In the last few years, Blockchain technology has seen great development. In addition to Bitcoin, many other blockchain technologies are making their place in the market. However, there are plenty of security issues in Bitcoin's peer-to-peer networks. This article provided a detailed description of various security issues involved in Bitcoin peer-to-peer networks while also providing appropriate countermeasures for these issues. However, there are some issues still open challenges that researchers should explorer to provide more innovative solutions. In this section, future research directions are identified.

While the PoW consensus protocol makes blockchain more resistant to many attacks such as double-spending and Sybil attack, the time-wasting nature of PoW consensus protocol severely affects Bitcoin transaction processing time. It is very slow compared to other digital cash systems such as VISA card. Moreover, PoW's high power consumption rate cause threatens the future sustainability of Bitcoin. These force researchers to propose other consensus protocols such as Proof of Authority (PoA), Proof-of-Stake (PoS), Proof of Storage, Federated Byzantine Fault Tolerance (FBFT), Practical byzantine fault tolerance (PBFT), and Proof of Elapsed Time (PoET). However, each of these protocols has its own limitations. Additional proposals that combine good features and avoid previous weaknesses are required.

The cryptography is the foundation of blockchain innovation. When the encryption algorithms or hash functions are no longer safe, then, the blockchain security will no longer exist. Researchers raise concerns regarding the security of the Elliptic Curve Digital Signature Algorithm (ECDSA). More research work should be conducted to provide alternative secure cryptographic algorithms.

It is important to note that Punitive and feather forking attacks are still an open challenge that needs to be addressed. Wallet theft or loss is another open challenge.

The degree of anonymity provided by the Bitcoin blockchain system encourages criminals to use it for illegal activities such as money laundering and ransom ransomware. This requires the development of technical and legal solutions to prevent such illegitimate activities.

On the other side, though, blockchain provides user anonymization, however, it is not completely anonymous as the attacker can do various mapping by figuring out the system traffic and transaction data. Therefore, in the future, there is a great need to address these types of issues to effectively prevent these network attacks. Various blockchain technologies need to be studied efficiently to achieve a better security guarantee.

References

1. Mohammadi F, Panou A, Ntantogian C, Karapistoli E, Panaousis E, Xenakis C. CUREX: seCUre and pRivate hEalth data eXchange. Proceedings of IEEE/WIC/ACM international conference on web intelligence, Thessaloniki, Greece. 2019, 263–268. https://doi.org/10.1145/3358695.3361753
2. Fotiou N, Pittaras I, Siris VA, Polyzos GC. Enabling Opportunistic users in multi-tenant IoT Systems using decentralized identifiers and permissioned blockchains. Proceedings of 2nd international ACM workshop on security and privacy for the internet-of-things, London, United Kingdom. 2019, 22–23. https://dl.acm.org/doi/10.1145/3338507.3358622
3. Kshetri N, Voas J. Blockchain-enabled E-voting. *IEEE Software*. 2018, 35(4), 95–99. DOI: 10.1109/MS.2018.2801546.
4. Tian F. An agri-food supply chain traceability system for China based on RFID & blockchain technology. Proceedings of 13th international conference on service systems and service management, Kunming, China. 2016, 1–6. DOI: 10.1109/ICSSSM.2016.7538424
5. Nakamoto S. Whitepaper. Bitcoin: a peer-to-peer electronic cash system. 2008. https://bitcoin.org/bitcoin.pdf
6. Baumann A, Fabian B, Lischke M. Exploring the Bitcoin network. Proceedings of WEBIST, Barcelona, Spain. 2014, 369–374. https://www.scitepress.org/Papers/2014/49373/pdf/index.html
7. Glaser F, Zimmermann K, Haferkorn M, Weber C, Siering M. Bitcoin-asset or currency? Revealing users' hidden intentions. Revealing users' hidden intentions. Proceedings of 20th ECIS, Tel Aviv, Israel. 2014, 1–14. https://pdfs.semanticscholar.org/3c7d/998b88bf48c88cf693625d2852706e7cb8e4.pdf
8. Simser J. Bitcoin and modern alchemy: in code we trust. *Journal of Financial Crime*. 2015, 22(2), 156–169. DOI: 10.1108/JFC-11-2013-0067.
9. Antonopoulos AM. Mastering Bitcoin: unlocking digital crypto currencies. 2nd edn. O'Reilly Media, Inc: Boston. 2017. https://www.oreilly.com/library/view/mastering-bitcoin-2nd/9781491954379/
10. Conti M, Kumar S, Lal C, Ruj S. A survey on security and privacy issues of Bitcoin. *IEEE Communications Surveys & Tutorials*. 2018, 20(4), 3416–3452. DOI: 10.1109/COMST.2018.2842460.
11. The history of the Mt Gox hack: Bitcoin 's biggest heist. https://blockonomi.com/mt-gox-hack/. Date accessed: 01/12/2019.
12. Q3 2017 global DDoS threat landscape report: Imperva. 2017. https://www.imperva.com/blog/q3-2017-global-ddos-threat-landscape-report/. Date accessed: 23/10/2019.

13. Lee K, Kim J, Kwon KH, Han Y, Kim S. DDoS attack detection method using cluster analysis. *Expert Systems with Applications.* 2008, 34(3), 1659–1665. DOI: 10.1016/j.eswa.2007.01.040.
14. Loibl A, Namecoin. Proceedings of seminars future internet (FI) innov. internet technol. mobile commun. (IITM), Munich, Germany. 2014, 107–113. https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2018-11-1.pdf
15. Bogner A, Chanson M, Meeuw A. A decentralised sharing app running a smart contract on the Ethereum blockchain. Proceedings of 6th international conference on the internet of things, Stuttgart, Germany. 2016, 177–178. https://doi.org/10.1145/2991561.2998465
16. Elrom E. NEO blockchain and smart contracts. The blockchain developer. Apress: Berkeley, USA. 2019; 257–298. https://www.apress.com/gp/book/9781484248461
17. Haferkorn M, Diaz J. Seasonality and interconnectivity within cryptocurrencies - An analysis on the basis of Bitcoin, litecoin and namecoin. In: enterprise applications and services in the finance industry. A. Lugmayr (ed.), Springer: Cham. 2015; 106–120. https://www.springerprofessional.de/en/seasonality-and-interconnectivity-within-cryptocurrencies-an-ana/7354044
18. Kappos G, Yousaf H, Maller M, Meiklejohn S. An Empirical analysis of anonymity in Zcash. Proceedings of 27th USENIX security symposium, Baltimore, MD, USA.*2018, 463–477. https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-kappos.pdf*
19. Garay J, Kiayias A, Leonardos N. The Bitcoin backbone protocol: analysis and applications, Proceedings of EUROCRYPT 2015. Sofia, Bulgaria. 2015, 281–310. https://doi.org/10.1007/978-3-662-46803-6_10
20. Johnson D, Menezes A, Vanstone S. The elliptic curve digital signature algorithm (ECDSA). *International Journal of Information Security.* 2001, 1(1), 36–63. DOI: https://doi.org/10.1007/s102070100002.
21. Jarecki S, Kiayias A, Krawczyk H, Xu J. Highly-efficient and composable password-protected secret sharing (or: how to protect your Bitcoin wallet online), Proceedings of IEEE european symposium on security and privacy (EuroS&P2016), Germany. 2016, 276–291. https://doi.org/10.1109/EuroSP.2016.30
22. Gennaro R, Goldfeder S, Narayanan A. Threshold-optimal DSA/ECDSA signatures and an application to Bitcoin wallet security. In: Applied cryptography and network security. ACNS 2016. Lecture notes in computer science, vol 9696. M. Manulis, A.R. Sadeghi, S. Schneider (eds.), Springer: Cham. 2016; 156–174. https://link.springer.com/book/10.1007/978-3-319-39555-5
23. Karame GO, Androulaki E, Capkun S. Double-spending fast payments in Bitcoin, Proceedings of 2012 ACM conference on computer and communications security, CCS'12. New York, USA. 2012, 906–917. https://doi.org/10.1145/2382196.2382292
24. Best practice for fast transaction acceptance how high is the risk? https://bitcointalk.org/index.php?topic=3441.msg48384#msg48384. Date accessed: 27/11/2019.
25. Vector67, fake Bitcoins? https://bitcointalk.org/index.php?topic=36788.msg463391#msg463391. Date accessed: 27/11/2019.
26. Eyal I, Sirer E. Majority is not enough: Bitcoin mining is vulnerable. *Communications of the ACM.* 2018, 61(7), 95–102. DOI: 10.1145/3212998.
27. Ron D, Shamir A. Quantitative analysis of the full Bitcoin transaction graph. Proceedings of international conference on financial cryptography and data security. Springer, Berlin. 2013, 6–24. https://link.springer.com/chapter/10.1007/978-3-642-39884-1_2
28. Schrijvers O, Bonneau J, Boneh D, Roughgarden T. Incentive compatibility of Bitcoin mining pool reward functions. *Lecture Notes in Computer* Science. 2017, 9603, 477–498. https://doi.org/10.1007/978-3-662-54970-4_28.
29. Beck R. Beyond Bitcoin: the rise of blockchain world. *Computer*, 2018, 51(2); 54–58. DOI: 10.1109/MC.2018.1451660.

30. Cachin C, Vukolić M. Blockchain consensus protocols in the wild, Zurich, IBM research. arXiv. 2017. https://arxiv.org/abs/1707.01873
31. Becker J, Breuker D, Heide T, Holler J, Rauer HP, Böhme R. Can we afford integrity by proof-of-work? Scenarios inspired by the Bitcoin currency. In: The economics of information security and privacy. R. Böhme (ed.), Springer: Berlin. 2013; 135–156. https://www.springerprofessional.de/en/can-we-afford-integrity-by-proof-of-work-scenarios-inspired-by-t/4140152
32. Donet JAD, Pérez-Sola C. Herrera-Joancomartí J. The Bitcoin P2P network. In: Financial cryptography and data security. FC 2014. Lecture notes in computer science, vol 8438. R. Böhme (ed.), Springer: Berlin, Heidelberg, 2014; 87–102. https://link.springer.com/chapter/10.1007/978-3-662-44774-1_7
33. Feld S, Schönfeld M, Werner M. Analyzing the deployment of Bitcoin's P2P network under an AS-level perspective. *Procedia Computer Science*, 2014, 32, 1121–1126. https://doi.org/10.1016/j.procs.2014.05.542.
34. Fanti, G, Viswanath P. Anonymity properties of the Bitcoin P2P network. *arXiv*. 2017. preprint arXiv:1703.08761.
35. Feld S, Schönfeld M, Werner M. Traversing Bitcoin's P2P network: insights into the structure of a decentralised currency. *International Journal of Computational Science and Engineering*. 2014, 13(2), 122–131. DOI: 10.1504/IJCSE.2016.10000107.
36. Heilman E, Kendler A, Zohar A, Goldberg S. Eclipse attacks on Bitcoin's peer-to-peer network. Proceedings of 24th USENIX security symposium, Washington, USA. 2015, 129–144. https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-heilman.pdf
37. Velner Y, Teutsch J, Luu L. Smart contracts make Bitcoin mining pools vulnerable. In: Financial cryptography and data security. FC 2017. Lecture notes in computer science, vol 10323. M. Brenner, et al. (eds.), Springer: Cham. 2017; 298-316. https://www.springer.com/gp/book/9783319702773
38. Vyas CA, Lunagaria M. Security concerns and issues for Bitcoin. Proceedings of national conference cum workshop on bioinformatics and computational biology, India. 2014, 10–12. https://www.ijcaonline.org/proceedings/ncwbcb/number2/16513-1414
39. Yli-Huumo J, Ko D, Choi S, Park S, Smolander K. Where is current research on blockchain technology?—a systematic review. *PLoS One*, 2016, 11(10), 1–27. https://doi.org/10.1371/journal.pone.0163477.
40. Lin I, Liao T. A Survey of blockchain security issue and challenges. *International Journal of Network Security.* 2017, 19(5), 653–659. DOI: 10.6633/IJNS.201709.19(5).01.
41. Joshi AP, Han M, Wang Y. A survey on security and privacy issues of blockchain technology. *Mathematical Foundations of Computing*. 2018, 1(2): 121–147. DOI: http://dx.doi.org/10.3934/mfc.2018007.
42. Viji Priya G, Krishna Priya G, Vivek M, Ashwini R. A survey on security attacks and challenges in Bitcoin. *International Journal of Computer Engineering & Technology.* 2018, 9(6), 65–74. https://www.iaeme.com/MasterAdmin/uploadfolder/IJCET_09_06_007/IJCET_09_06_007.pdf
43. Tasca P, Tessone CJ. Taxonomy of blockchain technologies: principles of identification and classification. *LEDGER*. 2019, 4, 1–39. DOI: 10.5195/LEDGER.2019.140.
44. Feinstein L, Schnackenberg D, Balupari R, Kindred D. Statistical approaches to DDoS attack detection and response. Proceedings of 3rd DARPA information survivability conference and exposition, Washington, USA. 2003, 303–314. https://www.tib.eu/en/search/id/ieee%3Adoi~10.1109%252FDISCEX.2003.1194894/Statistical-approaches-to-DDoS-attack-detection/
45. Li L, Lee G. DDoS attack detection and wavelets. *Telecommunication Systems.* 2005, 28(3–4), 435–451. https://doi.org/10.1007/s11235-004-5581-0.

46. Bastiaan M. Preventing the 51%-attack: a stochastic analysis of two phase proof of work in Bitcoin. https://pdfs.semanticscholar.org/0336/6d1fda3b24651c71ec6ce21bb88f34872e40.pdf?_ga=2.109266181.1207932880.1577133217-871105636.1575420591. Date accessed: 3/9/2019.
47. Xiang Y, Lin Y, Lei WL, Huang SJ. Detecting DDOS attack based on network self-similarity. *IEE Proceedings-Communications*. 2004, 151(3), 292–295. DOI: 10.1049/ip-com:20040526.
48. Time jacking and Bitcoin. http://culubas.blogspot.com/2011/05/timejacking-bitcoin_802.html. Date accessed: 07/08/2019.
49. Network time protocol version 4: protocol and algorithms specification, rfc 5905, internet engineering task force. http://www.ietf.org/rfc/rfc5905.txt. Date accessed: 09/10/2019.
50. Ren Y, Leng Y, Zhu F, Wang J, Kim, HJ. Data storage mechanism based on blockchain with privacy protection in wireless body area network. *Sensors*. 2019, 19(10), 2395–2410. https://dx.doi.org/10.3390%2Fs19102395.
51. Gervais A, Ritzdorf H, Karame GO, Capkun, S. Tampering with the delivery of blocks and transactions in Bitcoin. Proceedings of 22nd ACM SIGSAC conference on computer and communications security. Colorado, USA. 2015, 692–705. https://doi.org/10.1145/2810103.2813655
52. Rajput U, Abbas F, Hussain R, Eun H, Oh H. A simple yet efficient approach to combat transaction malleability in Bitcoin. Proceedings of 15th international workshop on information security applications, Korea. 2014, 27–37. https://link.springer.com/chapter/10.1007%2F978-3-319-15087-1_3
53. Wuille P. Segregated witness and its impact on scalability. Proceedings of SF Bitcoin devs seminar, San Francisco, USA. 2015, 1–7. https://diyhpl.us/wiki/transcripts/scalingbitcoin/hong-kong/segregated-witness-and-its-impact-on-scalability/
54. Wallgren L, Raza S, Voigt T. Routing attacks and countermeasures in the RPL-based internet of things. *International Journal of Distributed Sensor Networks.* 2013, 9(8), 794326. https://doi.org/10.1155%2F2013%2F794326.
55. Sun Y, Edmundson A, Vanbever L, Li O, Rexford J, Chiang M, Mittal P. RAPTOR: routing attacks on privacy in Tor. Proceedings of 24th USENIX security symposium, Washington, USA. 2015, 271–286. https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-sun.pdf
56. Apostolaki M, Zohar A, Vanbever L. Hijacking Bitcoin: routing attacks on cryptocurrencies. Proceedings of 24th of IEEE symposium on security and privacy, USA. 2017, 375–392. https://arxiv.org/abs/1605.07524v2
57. Conti M, Kumar ES, Lal C, Ruj S. A survey on security and privacy issues of Bitcoin. *IEEE Communications Surveys & Tutorials*. 2018; 20(4), 3416-3452. DOI: https://doi.org/10.1109/COMST.2018.2842460.
58. Kiran M, Stanett M. Bitcoin risk analysis. NEMODE policy. 2015. http://www.nemode.ac.uk/wp-content/uploads/2015/02/2015-Bit-Coin-risk-analysis.pdf
59. Narayanan A. Bonneau J, Felten E, Miller A, Goldfeder S. Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press: New Jersey. 2016. https://press.princeton.edu/books/hardcover/9780691171692/bitcoin-and-cryptocurrency-technologies
60. Touceda, DS, Sierra JM, Izquierdo A, Schulzrinne H. Survey of attacks and defenses on P2PSIP communications. *IEEE Communications Surveys & Tutorials*, 2011, 14(3), 750–783. DOI: https://doi.org/10.1109/SURV.2011.060711.00152.
61. Newsome J, Shi E, Song D, Perrig A. The sybil attack in sensor networks: analysis & defenses. Proceedings of 3rd international symposium on information processing in sensor networks, California, USA. 2004, 259–268. https://doi.org/10.1145/984622.984660

62. Bissias G, Ozisik AP, Levine BN, Liberatore M. Sybil-resistant mixing for bitcoin. Proceedings of 13th workshop on privacy in the electronic society, Rizona, USA, 2014, 149–158. https://dl.acm.org/doi/abs/10.1145/2665943.2665955

63. Singh A. Eclipse attacks on overlay networks: threats and defenses. Proceedings of 25th IEEE international conference on computer communications, Barcelona, Spain. 2006, 1–12. https://ieeexplore.ieee.org/document/4146884

64. McCorry P, Shahandashti SF, Hao F. Refund attacks on Bitcoin's payment protocol. In: Financial cryptography and data security. FC 2016. Lecture notes in computer science, vol 9603. J. Grossklags, B. Preneel (ed.), Springer: Berlin, Heidelberg. 2016; 581–599. https://www.springerprofessional.de/en/refund-attacks-on-bitcoin-s-payment-protocol/12291404

65. Avizheh S, Safavi-Naini R, Shahandashti SF. A new look at the refund mechanism in the Bitcoin payment protocol. arXiv, 2018. https://arxiv.org/abs/1807.01793.

66. Magnani A, Calderoni L, Palmieri P. Feather forking as a positive force: incentivising green energy production in a blockchain-based smart grid. Proceedings of 1st workshop on cryptocurrencies and blockchains for distributed systems, Munich, Germany. 2018, 99–104. https://dl.acm.org/doi/10.1145/3211933.3211951

67. Alshamsi A, Andras P. User perception of Bitcoin usability and security across novice users. *International Journal of Human-Computer Studies*. 2019, 126, 94–110. https://doi.org/10.1016/j.ijhcs.2019.02.004

68. Gervais A, Karame GO, Gruber D, Capkun S. On the privacy provisions of bloom filters in lightweight Bitcoin clients. Proceedings of ACSAC'2014, USA. 2014, 326–335. https://dl.acm.org/doi/10.1145/2664243.2664267

69. Ober M, Katzenbeisser S, Hamacher K. Structure and anonymity of the Bitcoin transaction graph. *Future Internet*. 2013, 5(2), 237–250. https://doi.org/10.3390/fi5020237.

70. Androulaki E, Karame GO, Roeschlin M, Scherer T, Capkun S. Evaluating user privacy in Bitcoin. In: Financial cryptography and data security. FC 2013. Lecture notes in computer science, vol 7859. A.R. Sadeghi (ed.), Springer: Berlin, Heidelberg. 2013, 34–51. https://link.springer.com/chapter/10.1007/978-3-642-39884-1_4

71. Koshy P, Koshy D, McDaniel P. An Analysis of Anonymity in Bitcoin Using P2P Network Traffic. In: Financial Cryptography and Data Security. FC 2014. Lecture notes in computer science, vol 8437. N. Christin, R. Safavi-Naini (eds.), Springer: Berlin Heidelberg. 2014; 469–485. https://www.springerprofessional.de/en/an-analysis-of-anonymity-in-bitcoin-using-p2p-network-traffic/4391582

72. Liu Y, Li R, Liu X, Wang J, Tang C, Kang H. Enhancing anonymity of Bitcoin based on ring signature algorithm. Proceedings of 13th international conference on computational intelligence and security. Hong Kong. 2017, 317–321.https://doi.org/10.1109/CIS.2017.00075

73. Ruffing T, Moreno-Sanchez P, Kate A. Coinshuffle: practical decentralized coin mixing for Bitcoin. Proceedings of ESORICS2014, Poland. 2014, 345–364. https://doi.org/10.1007/978-3-319-11212-1_20

74. Maxwell G. Coinjoin: Bitcoin privacy for the real world. https://bitcointalk.org/index.php?topic=279249.0. Date accessed: 11/8/2019.

75. Bonneau J, Narayanan A, Miller A, Clark J, Kroll JA, Felten EW. Mixcoin: anonymity for Bitcoin with accountable mixes. In: Financial cryptography and data security. FC 2014. Lecture notes in computer science, vol 8437. N. Christin, R. Safavi-Naini (ed.), Springer: Berlin, Heidelberg. 2014; 486–504. https://link.springer.com/chapter/10.1007/978-3-662-45472-5_31