A Taxonomy of Bitcoin Security Issues and Defense Mechanisms

Author Prachi Gulihar

Abstract

Cryptocurrency is a subset of digital currency. When the core building blocks of any digital currency are its cryptographic primitives then it is called a cryptocurrency. Bitcoin is recent and most popular cryptocurrency which has been in news for its several advantages over other cryptocurrencies. The core difference from other cryptocurrencies is that there exists no governing body to manage bitcoins, all the trust is mathematically ensured. Having strength of borderless payments with lowest transaction fees, bitcoin is now used to do financial transactions in more than 20,000 online stores. So understanding the security levels of bitcoin is of utmost importance.

Keywords: Bitcoin, bitcoin protocol, cryptographic primitives, bitcoin security, defense mechanisms.

1. Introduction

Cryptocurrency lies between fiat money and quantum money. There are many e-payment systems existing in today's world. A financial infrastructure which works on the internet technology is the need of the hour. Currently, the most dominant payment system is the credit card system which involves a bank as the trusting authority. Other systems in practice are e-wallets like Paypal, Paytm which follow an intermediatory architecture in which instead of bank, the company stands responsible for fair transactions [1, 2]. The successor to the intermediary architecture was SET(not an acronym) architecture in which the customer did not have to register himself with the company and credit card details also were not necessary to be shared. Cybercoin was based on this architecture but this architecture did not stay for long. The problem was there was no way to certify which CyberCoin belonged to which real-life user. This problem was solved by bitcoin which removed the real-life identities from the whole transaction process [3]. In the discussed e-payment systems, the characteristic of anonymity was missing. By making use of clever engineering, bitcoin was able to achieve this. Bitcoin is a famous cryptocurrency which was introduced by Satoshi Nakamoto in 2008 [4]. His name is said to have derived from subparts of names of four firms namely Samsung, Toshiba, Nakamichi and Motorola. The first bitcoin was realeased on January 3, 2009. It was a code of thirty-one thousand lines released online as-all bit, no coin. Bitcoin operates in a peer-to-peer(P2P) network. Smallest unit of a bitcoin is called satoshi which equals 10^{-8} bitcoins. It is a decentralized cryptocurrency which works by maintaining a public ledger like in ethereum [5] called blockchain.

Blockchain is a transaction ledger which is maintained in a distributed manner by the anonymous participating entities called miners. These miners are responsible for maintaining and extending the blockchain by solving a cryptographic puzzle as a Proof-of-Work(PoW) [6, 7]. PoW supplants the trust of bitcoin user in the mathematical equations. The senders broadcast

their transaction in the bitcoin network then it is the responsibility of the miners to include them in the blockchain. They are rewarded by the senders for doing so. This reward comes as a transaction fee. It is an instantaneous method of transferring payments with minimal transaction fees. The government has always been wary of bitcoins. The reason behind this is due to anonymity property, the taxation is not possible. Another reason is that although the maximum number of bitcoins is fixed to 21 million but there is no way to find out how many bitcoins are in circulation at any point of time which leads to lack of traceability. Bitcoin is a new type of money which works on an innovative platform of network.

2. Overview of Bitcoin Protocol and its Working

Bitcoin system is a distributed system [8] which comprises of five main components as shown in the above figure. First component are the users. The whole purpose of bitcoins is to transfer money from one user to another without any restrictions of geographical boundaries and without any authority to keep a check on the transactions. Any bitcoin user is strongly related another component of the bitcoin environment known as bitcoin wallet. Identity of any bitcoin wallet is its address. The user owning the bitcoin wallet has a single private key which remains secret from other users. The other key is dynamic public key which is changed every time the user initiates a new transaction. This enhances the security of the transaction. The fixed private key is used by the users to sign his transactions digitally by elliptic curve cryptographic [9] techniques. Bitcoin wallets [10] are mainly of two types- hot and cold. The hot wallets remain connected to the internet continuously whereas the cold wallets need to be connected to the

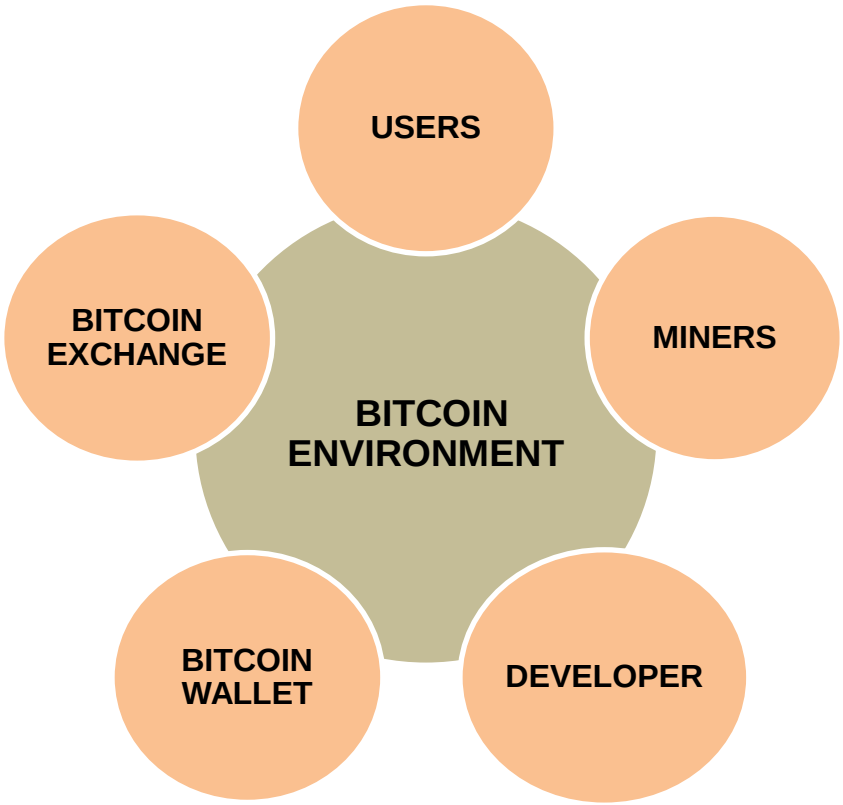

Figure 1. Components of Bitcoin System

internet only when the transaction is to be performed using the stored bitcoins. Hot wallets are more vulnerable to cyber attacks due to prolonged connectivity, therefore it is advised to keep only a small portion of the bitcoins in the hot wallet and keep the rest in the cold wallet. As an analogy cold wallets are comparable to safe in our homes. The daily use things and money is kept in open whereas valuables are stored in a separate hidden place. The hidden place in this case becomes the hard disks and other storage devices. Users operate the wallets by installing the bitcoin client on their personal computer or smartphones [11].

2.1. Miners

The next component is the miners. Their function is to club the transactions waiting for confirmations into a single block and then generate the hash of the block. This process is repeatedly done by every miner until the hash value of the block becomes less than the target value. They do so by varying the set of transactions being included in the block. It is the miners who are responsible for verification of authenticity, integrity and correctness of the bitcoin transactions. Miners may work in collaboration with co-miners to form a mining pool [12]. Whenever any miner or mining pools is successful in generating the proof-of-work, then that miner broadcasts the verified block in the bitcoin network. To gain rewards this block must be verified by majority of participating miners after which this block is added to the public blockchain. The bitcoins which are rewarded as transaction fees are them distributed among the co-miners in the mining pool in proportion to how much work effort was put in by each individual miner. Some mining pools distribute the rewards equally among the co-miners but this policy is unfair [13]. The miner who manages the mining pool is rewarded with a higher share for he has extra work of management of mining pool as well.

Bitcoin exchange is the virtual space in which bitcoins are sold and bought against other functional currencies. And developers are a set of programmers who work to improve the bitcoin cryptocurrency and add new features to it. Their work can be found on Github repository. They mainly focus on developing new services and softwares which make use of bitcoins.

2.2. Blockchain

The backbone of bitcoin is blockchain. Blockchain's basic component is block which is a public log of all the transactions which have taken place in the bitcoin network which supports distributed type of computation because it is P2P. These blocks are chained in a form of Merkle tree [14] comprising of full transaction nodes. Merkle tree is tree-like data structure which stores a summary of the transactions in the blocks. Transaction is a script which identifies the owner of the bitcoin. Script is a sequence of instruction which the miners execute. To ensure that the transactions once written in the public log are unchangeable, the bitcoin miners solve a cryptographic puzzle which is called proof-of-work. The transfer of coin ownership from one person to another is denoted by transactions.

2.3. Transaction script

A transaction comprise of two components- inputs and outputs. Inputs denote the unspent coins and output denote the address of the receiver. Inputs are defined by scriptSig which is a signature ensuring that the bitcoins being transferred are unspent and belong to the

sender. Outputs are defined by scriptPubKey which specifies the condition for redeeming the bitcoin being transferred. The bitcoin environment comprise of five standard scripts- Public-Key, Pay-to-public-Key Hash(P2PKH), Multi-Signature, Pay-To-Script Hash [15] and Data Output. Public-Key script defines the key using which the transaction will be signed. P2PKH script is used to find that public key which is hashed to a given value. In Multi-Signature script more than one signature is required for a public key to be able to redeem a transaction.

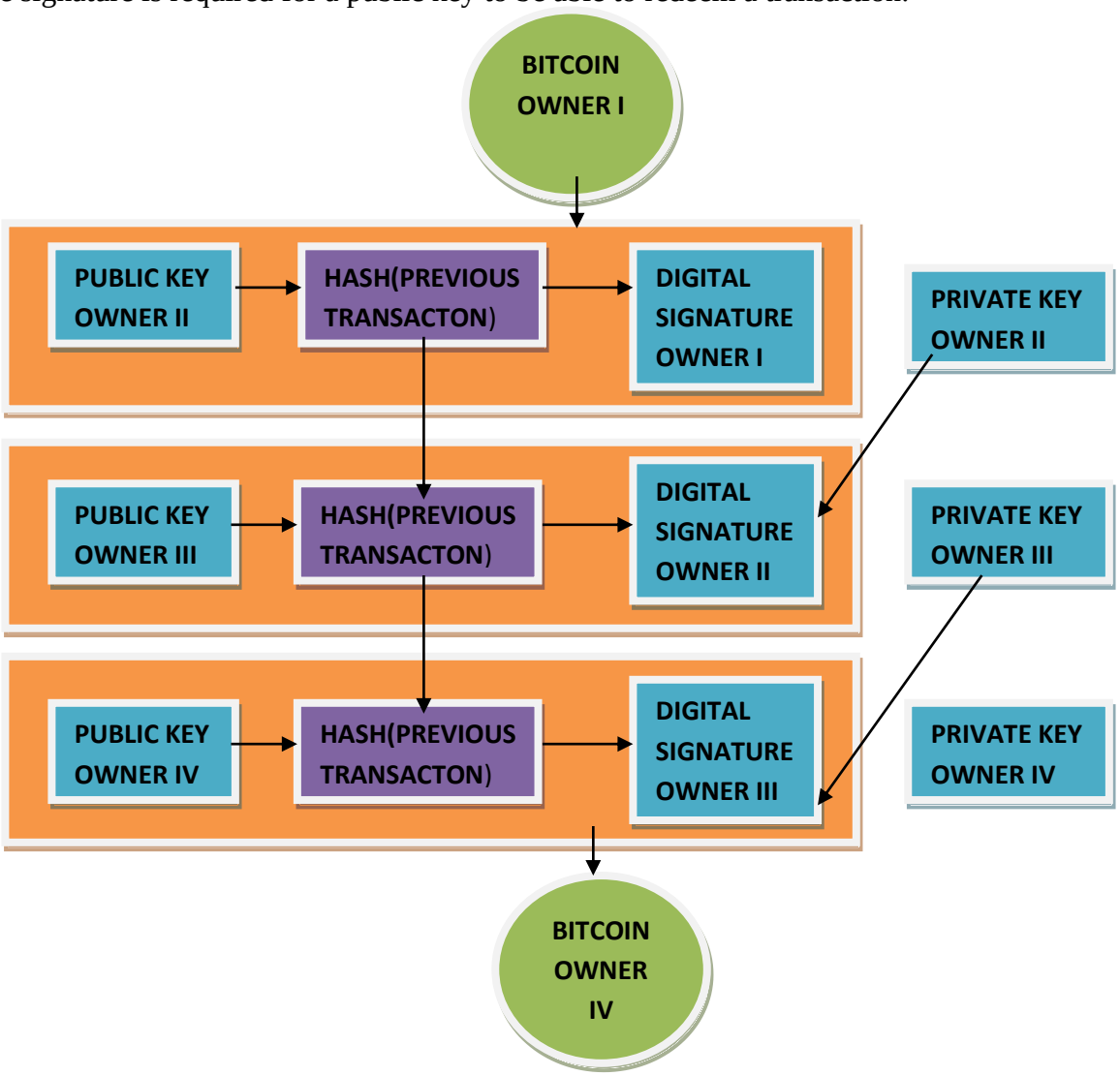

Figure 2. Bitcoin transaction flow

Pay-To-Script Hash [16] is used to decrease the length of the Multi-Signature script by hashing the non-standard to transaction scripts to standard ones. Data Output script is used to store the transaction messages in a human readable form. It is the task of miners to ensure that the transaction is valid by verifying the signatures and using standard transaction scripts. For new blocks become a part of the blockchain the miners need to find a random value called nonce satisfying the condition that it is less than the block header. This block header value is known as target value. This process is called Proof-of-Work(PoW) that depends on the miner's computational power [17]. For validating a transaction the miners get transaction fees which motivate them to work on extending the blockchain by adding new blocks. The public key of the

next owner is the address to which the bitcoins are to be sent. The collection of public addresses of all the e-wallets is saved as a file in distributed database. For a miner to solve one cryptographic hash puzzle, the machine calculates around 650 trillion hashes to get the acceptable one. So even if the PC is of i7 processing speed, still it would take around 21 years to mine one bitcoin. This brings in the need of formation of mining pools by sharing the computational resources among partner miners. BTC Guide is the largest mining group which has the capacity to mine 25 bitcoins in 20 minutes.

2.4. Byzantine agreement

Bitcoin relies on the concept of Byzantine agreement [18] to ensure distributed and mutual extension, exchange and acceptance of a final blockchain at any point of time. The Byzantine agreement has to ensure two properties- agreement and validity. Agreement means that all the participating miners return the same blockchain at the end of validating a transaction. Validity means the blockchain extended by an honest miner is valid and in further used by other participating miners to extend the current blockchain. In the blockchain, the blocks are connected in a chain like linear structure. The rightmost block in the blockchain is the block recently mined and is called head. The leftmost block in the blockchain is the first ever block mined called the genesis block. The length of a blockchain is the number of blocks it has after the genesis block. The bitcoin environment sets a parameter which determines the difficulty level of mining the next block. It is set by increasing the level of the cryptographic hash puzzle to a level where only one block is generated every 10 minutes, not more or less than that. This difficulty level is recalibrated after every 2016 blocks.

2.5. Bitcoin protocol

The bitcoin protocol [19] is the protocol which is implemented by the bitcoin miners. Its two main properties are- common prefix property and chain quality property. The common prefix property means that the blockchain of any two honest miners are different only in the most recent blocks. Chain quality property ensures that the honest miner mines on a blockchain whose sufficiently long part is absent of any adversarial block. Ideal chain quality is never attained by the bitcoin protocol. Further, it can be divided in three sub protocols- chain validation protocol, chain comparison protocol and PoW protocol.

The chain validation protocol validates the structural properties of the blockchain. For every block in the blockchain, this protocol checks three things. Firstly, whether the PoW is solved correctly. Secondly, the timestamp timer has not exceeded. Thirdly, the hash of the previous block is present or not. If all blocks are able to pass the verification test then the blockchain is valid, otherwise it is rejected. The chain comparison protocol is responsible to find out the most suitable blockchain from a set of blockchains. The competing chains may be picked up randomly or lexographically and in the output the blockchain having the longest length becomes a winner. The PoW protocol attempts to extend the winner blockchain by solving the cryptographic hash puzzle by doing brute-force for a predefined number of times. For every new proposed block this protocol generates the block hash which must be less than the set target value. If the puzzle is solved then the blockchain is extended by one block, otherwise it remains unaltered. This way the bitcoin protocol is iterated indefinitely.

3. Taxonomy of Attacks against Bitcoin Protocol

Bitcoin environment is an uncontrollable and decentralized which makes it more prone to cyber attacks as it becomes easier to generate fraud transactions. Various vulnerabilities are found in bitcoin protocol and bitcoin network. Figure 3 lists the different possible attacks based on various threats.

3.1. Distributed Denial-of-Service attack

The first category of cyber attack the bitcoin system is prone to is the networking infrastructure attacks. They are done by exploiting the vulnerabilities in the communication protocols of the bitcoin peer-to-peer network. First under this classification comes the Distributed Denial of Service(DDoS) attack [20]. In this attack the network resources are exhausted to block access of services to the genuine users. This attack is performed under the instruction of a master machine which instructs other compromised machines also known as slaves machine to overload the victim machine's network by flooding it with malicious request packets. 142 unique kinds of DDoS attacks have been identified to have taken place in the bitcoin network. In this attack a large number of compromised client nodes send fake transaction requests to an honest miner. After a while that honest miner is burdened and starts discarding all the requests including those coming from other honest miners, thus causing a denial-of-service. DDoS attacks take place on large mining pools [21] and big bitcoin exchanges due to bigger rewards [22]. Individual miners and small mining pools are safe from such kind of attacks. DDoS attacker's main motive is generation of bulk ransom. DDoS attack discourages the participating miners in the mining pool leading to their withdrawal from the pool. For example, the malicious miner shows its co-miner that he owns more computing power, enough to snatch his rewards, the honest miner finds it better to step back thus successfully imposing DDoS in the bitcoin network.

The attacker on gaining the majority of the computing power will be able to launch double-spending attack and Distributed Denial-of-Service(DDoS) attack [43]. Three methods are there to bribe the co-miners- out-band offer, in-band offer and negative fee offer. In out-band offer the attacker offers a direct payment to the co-miners who are ready to work on the attacker's private blockchain which comprises of attacker's pre-mined block. In in-band offer the attacker lures co-miners by offering bitcoins on. The attacker creates a blockchain fork and any miner choosing to mine on that fork gets the rewards in the form of bitcoins which are available for free. In negative free offer the attacker lures the co-miners by paying better reward shares than the current mining pool has to offer.

Although the gains by the co-operating miners are highly rewarding, but they are short-lived because in the long run the honest miners will lose trust in the mining pool ultimately leading to a crash in bitcoin rates. Another mining pool attack is feather forking. In this attack, the attacker blackmails the user client to pay him some bitcoins or else the attacker shall blacklist the transaction performed by that particular client node. The attacker does this by publically broadcasting the blacklisted transaction. Attacker creates a blockchain fork and works to extent this fork so that it may outrace the public blockchain. If the attacker fails to do so then it discards its private blockchain and resumes working on the public blockchain. When the attacker is

determinant to block and blacklist a particular transaction, then he or she will perform iterative forking to gain trust from the co-miners. The attacker will then be able to block the selected transaction without any inherent cost because then majority of miners will be entrusting his forking strategy.

3.2. Malleability attack

Next category of attacks is malleability attacks [23, 24]. Malleability attacks also lead to denial-of-service. In malleability attacks, the order of the transaction to be processed is disturbed by putting in fake transaction. These fake transaction poses higher transaction validation fee thus luring honest miners to include this fake transaction with higher priority than the in-queue transactions. The attacker's purpose is to waste miner's resources of time and computing power in validation of a fake transaction which is ultimately in vain. In cryptography, the term malleable is used if the attacker is able to generate an output Y similar to X without knowing the function used to generate X. In the bitcoin network, it is the transaction which is made malleable by varying syntax configuration of two semantically identical transactions. This can be done without knowing the user's private key because there is a bug in the bitcoin protocol which identifies every transaction by its transaction -id. But this transaction id may not be unique which means that transaction of transfer of x bitcoins from Alice to Bob may have two transaction ids- T and T'. This happens because the hash of these transactions are different because although the amount of bitcoins being transferred is similar but it is a different set of bitcoins which are transferred every time. This loop-hole of the bitcoin protocol is exploited in transaction malleability attack.

Mt. Gox bitcoin exchange was using the custom implementation of the bitcoin protocol which had this bug [25, 26], the exchange had to block accounts and the transactions were barred due to this attack. The attacker was able to withdraw his or her coins twice form the bitcoin exchange. This was possible because the custom implementation of the bitcoin protocol which was used by Mt. Gox bitcoin exchange searched in only for matching transaction-id unlike the recent reference implementations of bitcoin protocol which searches for any transaction which is semantically equivalent. In Mt. Gox [27] case, the attacker had a bitcoin trading account in Mt. Gox. For example, Alice first deposited X bitcoins in her exchange account. She then sent a transaction Tx to Mt. Gox asking to transfer her coins back to her. In response, Mt. Gox issued transaction Ty to transfer Alice's coins back to her. Next, Alice generates T' which is semantically same as Tx but has different transaction-id. This transaction T' gets included in the public blockchain and the transaction Tx is rolled back, so Alice now informs Mt. Gox of unsuccessful deposit transaction Tx. Then, Mt. Gox check its transaction and will not find the transaction Tx which makes him believe that Alice is saying correct about the unsuccessful transaction and thus returns X bitcoins back to her, X bitcoins which were never submitted.

3.3. Refund attacks

Whenever any bitcoin transaction fails then the refund has to be initiated by the bitcoin exchanges. This is where refund attacks [28] come into place. Border Internet Protocol-70(BIP-70) is widely accepted by the community of bitcoin developers for performing successful payments using bitcoins. Almost all major wallet and exchange services use this protocol. There

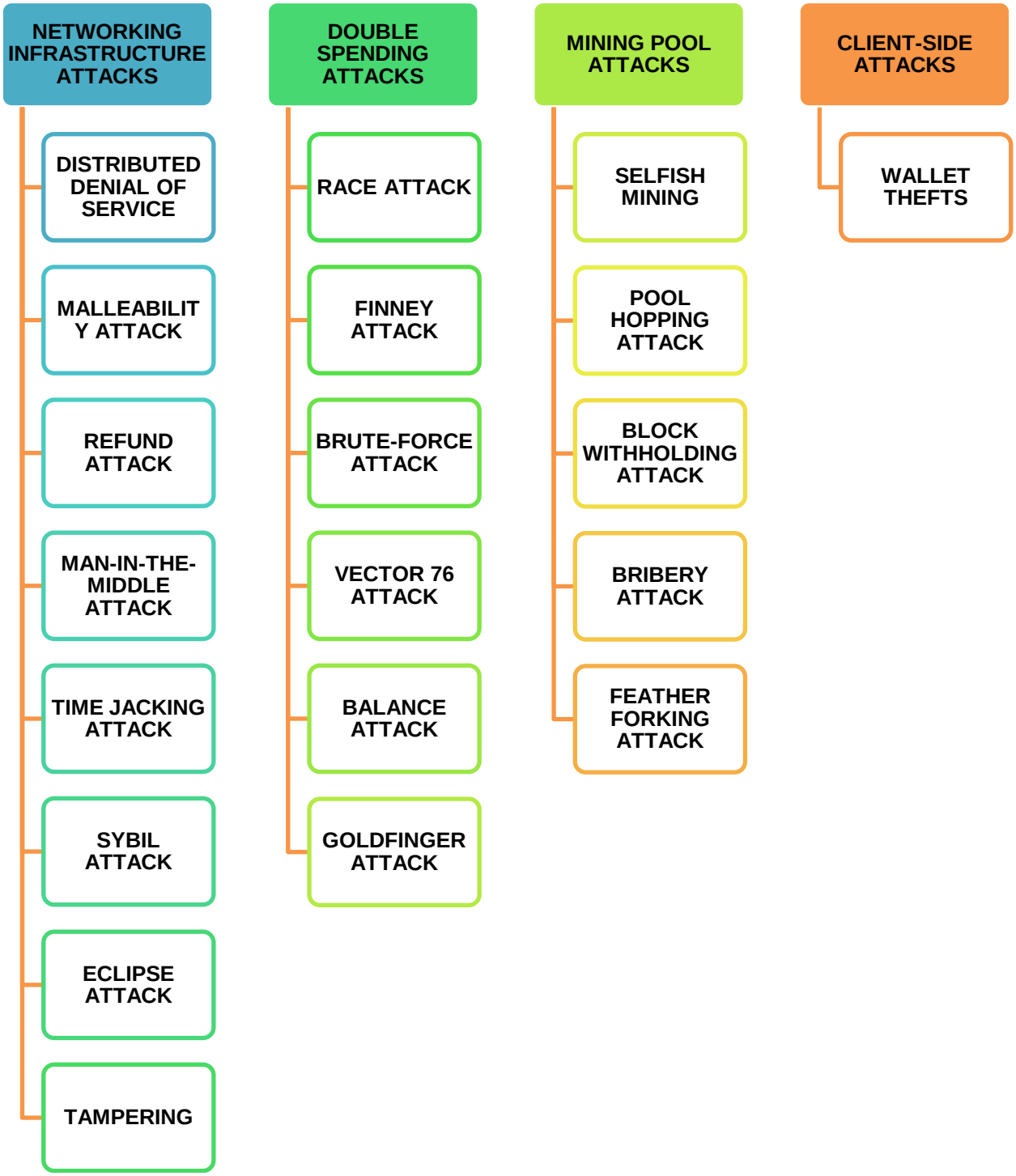

Figure 3. Cyber Attacks in Bitcoin System

are payment services which provide the exchange and wallet service providers with a platform and infrastructure to operate in a secure environment. The refund attack takes place by exploiting the authentication vulnerability present in BIP70. In this attack, the user wallet is under the control of a malicious bitcoin node. Whenever the customer begins trading his bitcoins, his wallet address is sent to the malicious node. On the completion of trading the malicious user

requests a refund from the node with which the customer traded. In the refund address of the refund request, the malicious user puts in his own wallets address and the bitcoins get refunded to him. The customer lies unaware of all these transactions taking place in his name. This happens because the merchant using BIP-70 protocol lacks secure authentication of who is sending the refund requests.

3.4. Man-In-The-Middle attack

Network infrastructure attacks in bitcoin system also comprise of Man-In-The-Middle(MITM) attack [29]. In this the attacker traps the victim by attracting him to a website which poses as a trustable merchant website helping in making secure bitcoin payments but clicking on webpage reveals victim's identity which includes victim's wallet address. Whenever the any customer engages in making any kind of online payment then he is directed to a legitimate payment gateway. Let us say customer C just bought something from the victim, them the victim's payment gateway page will be opened in customer's browser. This page is under the attackers control and the details of customer C will be known to the attacker without the victim noticing any of these practices. After customer C pays to the victim, then the attacker sends a refund request in the name of customer C and the refund amount will be sent to the attacker. The customer remains unaware about the refund and the victim loses his coins. Thus, making MITM attack successful.

A revision in BIP-70 protocol is required to prevent this. All the nodes in the bitcoin network have an internal clock maintaining the time count. This is of two kinds- median time and system time. Median time is the time sent to the newly connected node by the adjacent peer nodes at the time of joining the bitcoin network. It is sent in the version message shared by the adjacent nodes. System time is nodes own timer clock which is allowed a maximum deviation of 70 minutes from the median time. It is reset every time the maximum deviation limit exceeds.

3.5. Time jacking attack

In the time jacking attack [30, 31], the attacker brings inaccuracy in the timestamps by fake median time to the peer nodes. The attacker may also plant fake nodes for this purpose. This will either lead to abrupt increase or decrease in the timers of the peer nodes. A classic kind of attack involves making the timer of the victim node the slowest by increasing the timers of co-peers. The maximum duration by which the victim can be made to lag is 140 minutes. Acceptance of any blockchain depends on the network time so by altering the timestamps the attacker confuses the peer nodes. The victim nodes then start mining on an older blockchain fork which is already discarded by the rest of the network, thus wasting their time and computation power. This leads to a lag in confirmation rates of bitcoin transactions and the nodes may have to wait for more than 6 minutes to entrust that the transaction just validated is not going roll back.

3.6. Sybil attack

In sybil attack [32, 34] , the malicious node compromises a part of the network by forming a group of dummy nodes. Their motive is to partition the victim node from the bitcoin network and isolate it so that all the transactions of the victim node are blocked from entering the public

blockchain. This is achieved by collaboration in timing attack which leads to higher time in performing the encryption process and thus the delay in confirmation of victim's transactions. The input of the victim's transaction stands waiting in the network for validation which increases the vulnerability of these inputs being used for double spending attack [35].

3.7. Eclipse attack

In eclipse attack [33] , the attacker posses multiple IP addresses to perform spoofing. The victim is selected by the attacker after which all the IP address the victim node tries to contact are diverted to the attacker's IP address thus blocking the nodes which the victim wishes to connect to. Eclipse attack is further classified into two kinds- infrastructure attacks and botnet attacks. Infrastructure attack takes place on Internet Service Provider(ISP) which is forced to manipulate the addresses of multiple bitcoin client nodes. In botnet attack, the attacker manipulates the address of a specific range like private IP addresses affect the peers connected in that private network. This attack is performed by an army of botnets which work on the instructions of the attacker. After a new block is mined, the information about this newly mined block is broadcasted in the bitcoin network. This information is shared at set intervals of time. The attacker in the tampering attack [36] delays the propagation of this broadcasted information by congesting the network route and by overloading the client node by sending multiple requests.

3.8. Double spending attacks

Double spending attack [14] means spending of the same bitcoin for two different transactions. In the bitcoin network, it is the function of the miners at work to verify and process the transactions in the network. They must ensure that only unspent coins are referred as inputs in any transaction. This is achieved by distributed time-stamping and distributed Byzantine consensus protocol. For example Alice creates a transaction Tx directed towards Bob at time t1 using her bitcoins B_{alice} . Alice broadcasts this transaction in the bitcoin network. Then at time t2 which is almost parallel to t1, Alice creates another transaction Ty using the bitcoins B_{alice} again. This time directed towards a wallet address which is already owned by her. Alice will be successful in using the same bitcoins twice if Bob accepts transaction Tx and provides the goods or services because Bob is at the risk of being unable to redeem those bitcoins. In the bitcoin network it is the dynamic responsibility of miners to ensure that only unspent bitcoins are used in any transaction. When any miner X will receive two transactions having same bitcoins in the input script then miner X must verify only one of them hence rejecting the other.

Even after strict ordering in bitcoin transactions and proof-of-work, the bitcoin environment remains vulnerable to double spending attack. Double spending attack is successful only when the following four conditions are fulfilled consecutively. Firstly, when a part of the miners in the bitcoin network approves of Alice's transaction Tx and Bob receives the approval confirmation after which Bob releases his products and services later realizing the rollback of approved transaction. Secondly, simultaneously the remaining part of the miners in the bitcoin network approve of transaction Ty thus forking the existing blockchain. Thirdly, Bob receives the approval confirmation of transaction Ty after he has shipped the product or services to Alice. Lastly, more that 50 percent of the bitcoin miners must start mining on the blockchain which accepted Ty as the valid transaction. If all these conditions are met then Alice will be successful in using the same set of bitcoins twice for different goods and services. Double spending attack

takes place with varying levels of difficulties and complexities which can be divided into six sub-categories as shown in the figure 3.

3.9. Finney attack

In finney attack [37] Alice beforehand mines the block having Ty transaction. Alice then creates the transaction Tx directed towards Bob using the same bicoins B_{alice}. Alice keeps the pre-mined block private and does not broadcast it to the bitcoin network. Alice waits until the miners accept her transaction Tx and declares it valid. Bob on getting the validity confirmation of transaction Tx from the network miners releases the goods and services. When Alice receives the goods and services from Bob she then broadcasts her pre-mined block into the network creating a fork in the blockchain which is of equal length. If the majority of bitcoin miners start working on this newly created forked blockchain then Alice will be successful in making the transaction Ty valid and Tx invalid because according to bitcoin protocol, the miners will work on the longest blockchain when a fork arises.

This creates a race condition between the two blockchain forks and Alice on winning the race will end up getting the bitcoins back to wallet address. To avoid this race condition, Bob should have waited for multiple confirmations from the bitcoin miners before releasing his goods but that will only make the attack harder for Alice and not finish its possibilities.

3.10. Brute-force attack

In the brute-force attack [38], the attacker is one step ahead. Here the attacker Alice controls x nodes in the bitcoin network who work together to pre-mine n blocks on the newly forked blockchain. These n blocks are not broadcasted in the bitcoin network. To prevent the finney attack if Bob waits for n confirmations then Alice will be able to provide him with n confirmations on releasing these pre-mined blocks. On doing this Alice's forked blockchain becomes the longer one and the miners make a shift to Alice's blockchain making her successful in double spending attack.

3.11. Vector-76 attack

Another form of double spending attack occurs in the case of bitcoin exchanges. It is known as vector-76 attack [39]. In this attack Alice pre-mines the block having the transaction of bitcoin deposit in the bitcoin exchange. When the next block confirmation information is flooded in the network, then Alice releases its pre-mined block in the network along with another mined block which comprises the transaction of the withdrawal of the deposited bitcoins. This increases the length of Alice's forked blockchain by one block. Abiding by the bitcoin protocol, the network miners then consider the longest chain as the valid branch and start mining on Alice's forked blockchain. Due to this the deposit transaction is rolled back and withdrawal transaction is validated leading to loss of the bitcoins from the bitcoin exchange.

3.12. Balance attack

Another kind of double spending attack known as balance attack[40] exploits the proof of work feature of the bitcoin protocol. Its basis is that if the miner is able to generate the proof of work at a faster speed than the fellow miners then its probability of success in double spending

increases multiple folds. This will be possible if the miner has additional computing power which helps him to solve the proof-of-work at a faster rate. In balance attack Alice will try to delay the network communication among the mining groups. The success of balance attack depends not only on the delay generated but also on how much of the computing power relies with Alice.

3.13. Goldfinger attack

The last kind of double spending attack is the goldfinger attack also renowned as 51 percent attack. It is a theoretical attack which if successfully executed will lead to instability in bitcoin system. This may take place in worst- case scenario when more than 50 percent of the computing power will reside with a single miner or mining pool. Below is the graph showing relationship between the number of confirmations, computing power and double spending.

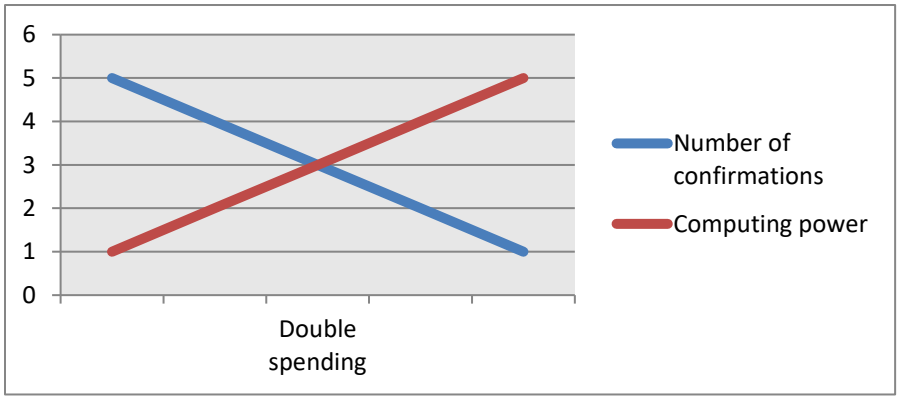

Figure 4. Graph showing double spending dependencies

3.14. Mining pool attacks

The next category of cyber attacks in bitcoin system is the mining pool attacks [62]. Bitcoin miners clubbed together their resources to increase their computing hash power which will directly lower the verification time of the set of transactions they choose to put in their proposed block. Lately, the research area of mining strategies has gained a lot of attention. Mining pool attacks can be broadly classified into two kinds- internal and external. In the internal attacks, the miners of the pool become dishonest and try to take more that fair share of rewards in the transaction fees. In some of the internal attacks, the dishonest miners disrupt the working of the pool by keeping them away from successfully generating the next block in the blockchain. Whereas, in the external mining pool attacks the in-pool miners are not involved. They are performed by external miners who take undue advantage of their higher hash power to initiate the double spending attack. Researchers have used a game-theoretic approach for showing instances of selfish mining attack in which the correct block is discarded by a majority of miners in the bitcoin network.

It is a fact that every participating miner in the bitcoin network is there for the purpose of gaining rewards only, but they do this in an honest and fair manner without harming the co-miners. But in selfish mining attacks the dishonest miners purposefully hide the information of

the block they have already mined successfully. Their purpose is dual-fold. First, they want unfair share of rewards won by the mining pool. This means that the reward instead of being distributed according to the mining work done by individual miner, gets unfairly distributed. The dishonest miner gets a share more than the computing power he spent on mining. The second purpose of these dishonest miners is to confuse the co-miners which leads to their resources being expended on the wrong blockchain.

To understand this better, let us assume Alice is the dishonest miner of the mining pool. Alice has kept the information of the pre-mined block with herself. She then keeps on mining on her private blockchain. She releases her private blockchain in the mining pool only when her private blockchain exceeds the length of the public blockchain the rest of the pool is mining on. This creates a fork in the blockchain, then as a rule of the bitcoin protocol, all of the miners need to switch on the longest chain which is Alice's newly broadcasted blockchain. Doing this the rewards given to the honest miners on adding block to the previous blockchain are taken back by the mining pool manager. Thus, leading to wastage of the time, power and money of the honest miners. The attack gets stronger if Alice is able to make her own dishonest sub-pool in the mining pool by collaborating with other dishonest co-miners which may further lead to 51 percent attack.

3.15. Pool hopping attack

The next mining pool attack is the pool hopping attack. In this attack the attacker analyses the mining share entries the co-miners submit to the mining pool manager. At many instances what happens is that a large number of co-miners submit their mining shares but the mining pool is unable to find the next block. In this case even if the block is found at a later stage then the reward is going to be distributed according to the mining share entries which are very large in number, so the individual share will be negligible. In such cases the attacker dynamically switches his pool or starts mining independently.

3.16. Block withholding attack

Another mining pool attack is called the block withholding attack [41, 42] in which the attacker never broadcasts the block mined by him. It can be of two types- sabotage attack and lie-in-wait attack. In sabotage attack the purpose of the attacker is not to gain the rewards, but to make the co-miners lose the rewards. In lie-in-wait attack the attacker's purpose is to gain the rewards by intentionally concealing the pre-mined block as in selfish mining. The lie-in-wait attack is not economically viable in short duration but it can do enormous damages in the long run leading to mining pools losing a lot of money in a few months. The next attack a mining pool is vulnerable to is bribery attack. In this attack the attackers bribes and lures the co-miner to share their computing resources with the attacker who might end up gaining control of the majority of resources in the mining pool. Although the duration for which the attacker owns the majority of computing power is less but it is a threat to the reward gains of the mining pool.

4. Security and Privacy issues in Bitcoin Protocol

With increasing computational power and advancing cryptanalysis techniques, the cryptographic primitives are at risk of being broken [46]. These primitives weaken over a time and rarely undergo abrupt breakage. Although some of the attacks discussed below are theoretical [47] but it is crucial to anticipate their impact so that rigorous contingency plans can be put in place. The flowchart ahead shows the process which bitcoin protocol follows to verify the cryptographic primitives of the next proposed block. Due to variation in mining activities, network delays and presence of dishonest miners, the correct state of the blockchain gets disputed leading to a fork in the blockchain. To prevent forking checkpoints are introduced in the blockchain so when a dispute arises the blockchain is reset to the last checkpoint. These checkpoint entries begin from the first block in the blockchain called the genesis block. This way consensus is maintained among the miners who then continue to mine only the longest blockchain [48].

But these kinds of temporary forks increase the potential of the double spending attack to occur. In simple language, double spending occurs when the attacker firstly credits the bitcoins from his wallet in return of services, then he reorganizes the transaction ledger in such a way that the initial amount credited is debited allowing him to use them in some other transaction. Technically, the adversary attempts exploit this temporary split in the network. In this attack the adversary places two different transactions with same input script in two different branches of the blockchain. This is prevented only when the consensus is reached and one of the branches is chosen as the valid branch. For this the receiver must wait for many confirmation blocks before

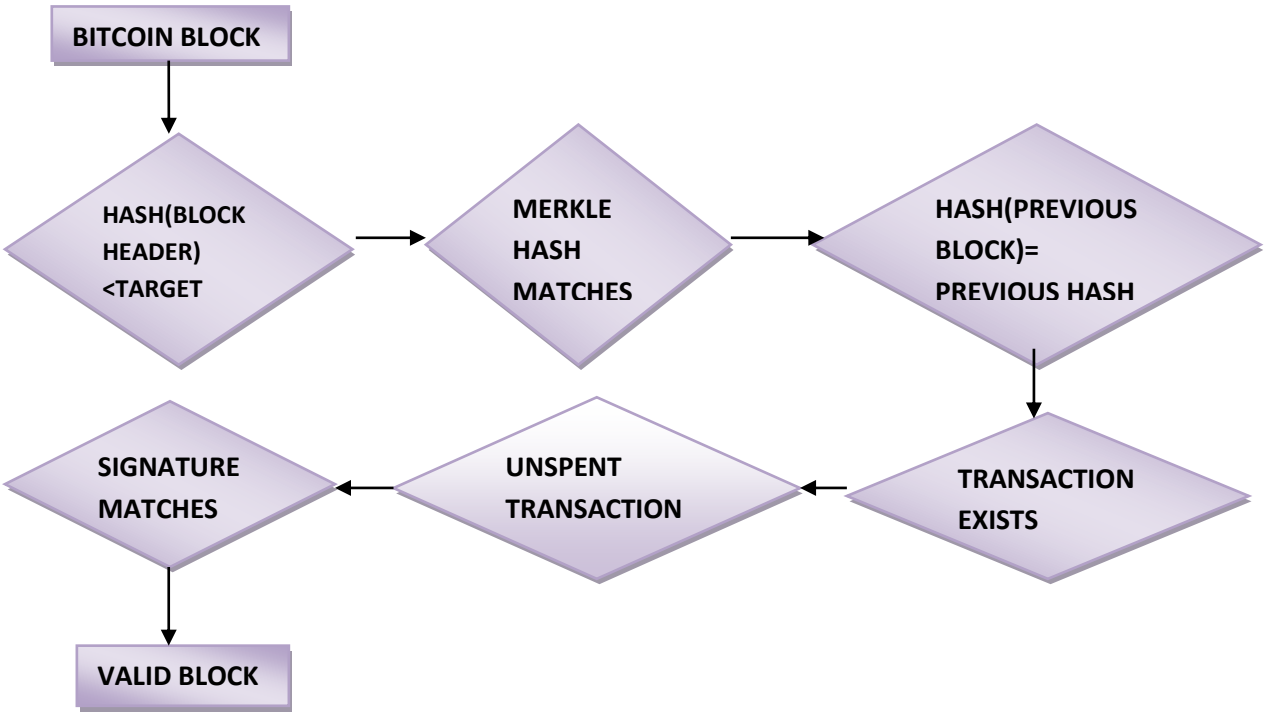

Figure 5. Bitcoin cryptographic primitives

committing. Satoshi Nakamoto has explained that the bitcoin system has the ability to withstand the double spending attack if the receiver waits for the sender's transaction to advance ahead in the blockchain by some N blocks, then the probability of the sender being able to reorganizing the public blockchain drops exponentially by a factor of N.

Another major security issue in the bitcoin system is when more than half of the computational power resides with a single miner. This leads to instability in the system and the chances of this kind of attack have increased many folds after the concept of mining pools was introduced. In a mining pool, a group of miners is created who then collaborate and work together to find the nonce value. The mining rewards are then distributed in proportion to the work done by each member miner. Once a transaction is verifies the accepted block details is flooded across the network. There is no need for all the nodes to download the full blockchain at its end, they can just download the block headers of the corresponding Merkle tree and become lightweight clients which follow Simple Payment Verification(SPV). Over the time new updates and security enhancements are made in the bitcoin protocol by the bitcoin community by forking the blockchain. When this fork is backward-compatible with the previous version of the protocol then it is known as a soft fork. It is less strict as not all nodes need to upgrade to the latest version. When this fork is not backward-compatible then it is known as hard fork. In case of a hard fork all the nodes need to upgrade to the latest version in order to participate as the new transactions are rejected by the previous version of the bitcoin protocol.

4.1. Hashing

Hashing in bitcoin is done at two places [49, 50]. Primary hash function has a 256-bit output and the secondary has a 160-bit output. Primary hash function has three functions. Firstly, it is the hash which is by miners to generate PoW. Secondly, it is used to generate the hash of transactions in a block which is then stored in Merkle tree. Thirdly, it is used while signing transactions with the private key. In primary hash function the Secure Hash Algorithm is applied twice on the input. Secondary hash function is used in two scripts- P2PKH and P2SH. In secondary hash function first the input is hashed with SHA-256 and then with RACE Integrity Primitives Evaluation Message Digest(RIPEMD-160). A robust hash function must ensure three properties- pre-image resistance, second pre-image resistance and collision resistance. Pre-image resistance means even if the attacker knows the output, still it is hard to find the input on which hashing is done. Second pre-image resistance means that given an input and a hash equal to its hash, it is impossible to find a different input value. Collision resistance means that it is computationally infeasible to find two different inputs whose hash is same.

For attacking collision and second pre-image resistance property only one of the hashes, either primary or secondary needs to be revealed whereas for attacking the pre-image resistance property, both the hashes need to be known to the attacker. When the hash breakage leads to compromised collision resistance of the primary hash then the bitcoins are stolen and destroyed. And when collision resistance of the secondary hash is compromised then the transaction is repudiated. The compromised second pre-image resistance property leads to double spending and compromised pre-image property uncovers the user addresses and leads to complete failure of the blockchain.

4.2. Digital Signature Scheme

Digital signature scheme used by the bitcoin protocol is Elliptical Curve Digital Signature Algorithm(ECDSA) [51, 52] using secp256k1 parameters. It is used in signing the primary hash value. When a signature scheme is broken, it will lead to transaction malleability attacks. In this attack the attacker is able to encode the same transaction in multiple ways without validating the signature. The three parameters to measure the robustness of the digital signature scheme are- unforgeability, integrity and non-repudiation. Unforgeability means that without knowing the secret key it is impossible to generate the signature. When the unforgeability property is compromised then it leads to four kinds of breakage- total break, universal forgery, selective forgery and existential forgery. Universal forgery enables the attacker to forge all the messages. Selective forgery enables the attacker only to forge some messages of his choice. This risks the bitcoin wallets and the attackers are able to drain them.

Existential forgery is the ability of attacker to generate a valid signature for a new message but this is not effective because the new message may not be a valid message. A valid message is the hash of a valid transaction. Integrity ensures that the signature is binded to one transaction and cannot be concatenated to another. When the integrity is compromised then the claimed payment is not received. It is of two types- collision integrity and second pre-image integrity. Collision integrity is compromised when attacker knows that which public key is used to generate the transaction, he is then able to forge a valid signature for another transaction. Second pre-image integrity is compromised when the attacker knows the public key and the message generated by it, the attacker generates a parallel new transaction for which the same signature is valid.

Non- repudiation is a proof to all the nodes regarding the actual owner of the bitcoins being transferred. Non-repudiation can only be compromised when the secondary hash is broken. These properties are interdependent and breakage in one leads to breakage in others. These two figures explain the conventional privacy model and bitcoin privacy model. In any conventional method of exchanging money like in a bank, the sender does not send it directly to the receiver. There is always an intermediary authority between the sender and receiver. The details and information of who is sending how much money to whom relies only with the trusted authority and is not accessible to public which ensures pseudo privacy because the sharing of personal information is dependent on the trusted bank.

In the second figure the privacy model of bitcoin is shown. In bitcoin system all the transactions are in the public domain as public blockchain but still full privacy is ensured. This

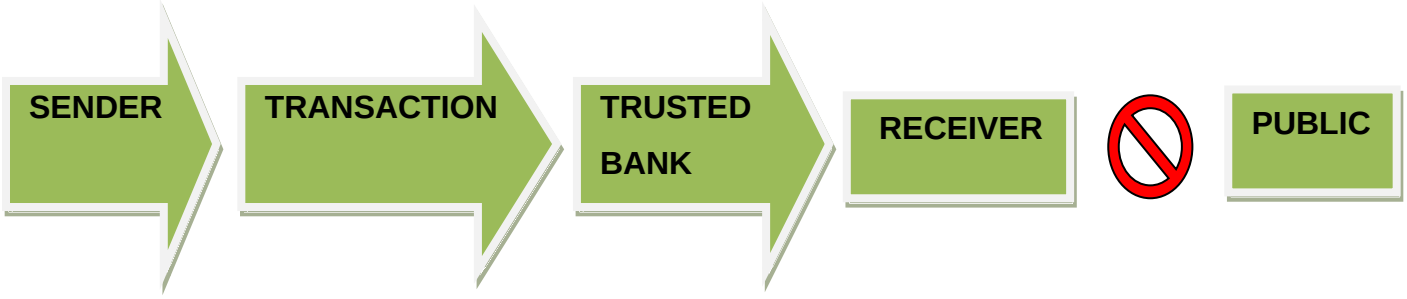

Figure 6. Conventional Privacy Model

happens because all the entities communicate using their public keys and mapping of these public keys to real world entities is a computationally infeasible task. This makes the real world entities anonymous. So although the attacker can gain information like how many bitcoins are transferred at what time but the linking of transactions to any parties is not possible because the real identities remain in the hidden domain. A new public key is used for every new transaction making the traceback harder.

4.3. Theft in Bitcoin Exchanges

Bitcoins are prone to theft in bitcoin exchanges. Some mining applications which miner partners use for collective mining in a mining pool are malicious as they are compromised by the hacker's distributed corrupt code. An example of such malicious act can be traced back to 2013 when the Skype video call application was held responsible for spreading Trojan Horse virus. It started with India due to poor cyber security and then it went on to infect western countries. A malicious program was embedded in the Skype messages exchanged so whenever the victim clicked on that message the linked program was executed making the machine a bitcoin miner which led to overloaded sloth CPUs. The attacker was rewarded bitcoins in proportion to the decreased CPU throughput. The processing power of individual PCs was exploited to mine more bitcoins leading to crash of the user PCs. Bitcoin mining viruses have been accused of stealing

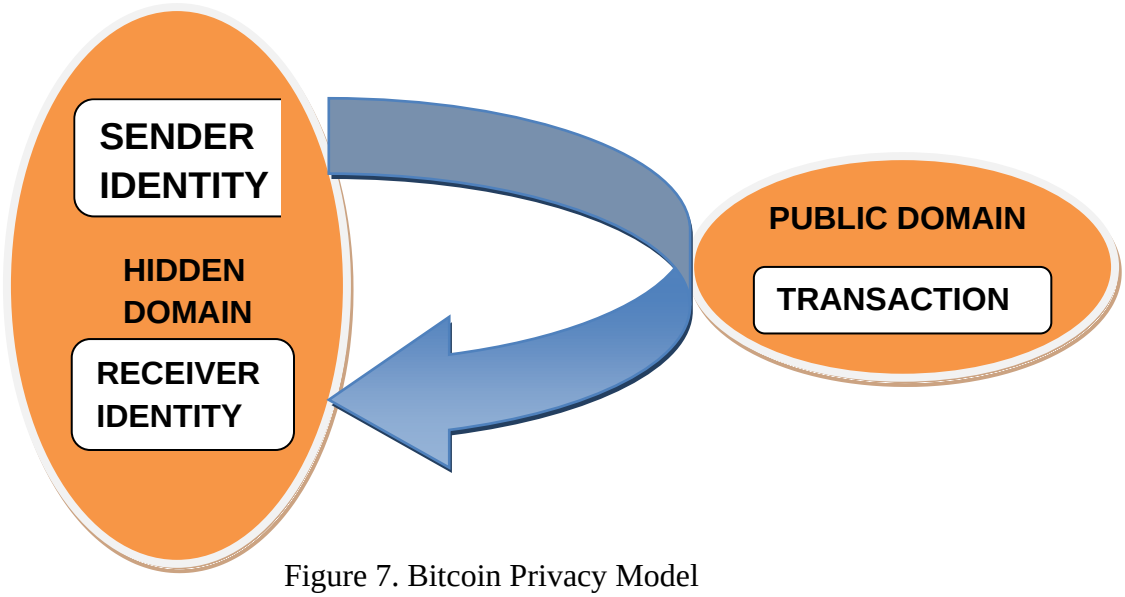

Figure 7. Bitcoin Privacy Model

bank details by installing Zeus in the backend. They has been accused of converting PCs into botnets by installing Andromeda. Bitcoin wallet malwares [53] have been found adjacking the user's browser which then uncontrollably clicks on link of the corrupt website which generate them income for clicks. Almost 2 million computers were infected for three days, each one generating 12,000 clicks a day.

4.4. Extortion of money from Bitcoin Wallets

Extortion of money is done by hackers by extorting the bitcoin wallet of the user. Online gaming was one of the first industries to accept payments in the form of digital cash transactions.

Game accounts contain points which are extorted by hackers by spreading malicious files having gaming account extortion function. Similar file versions have been found executing bitcoin account extortion function to extort bitcoin exchanges in Korea. Malicious code was distributed by trapping the user by downloading an image file that never existed in reality. So instead of image file the user is looking for, he becomes a victim and ends up downloading the malicious program.

Bitcoin exchanges have also been the victims of Distributed Denial of Service(DDoS) attacks [54]. They are lucrative attack options because of the amount of currency exchange they cater to. In DDoS attack, the attacker's main motive is to disrupt the services offered by a server by overloading its bandwidth and exhausting its resources. The attacker exploits the vulnerabilities in system. The compromised systems then are controlled by the attacker itself to expand its army of zombie machines. The compromised machine acts as master which then further exploits the vulnerabilities in other systems to gain control of it. All these form the slave machines which act on the commands of the master machine which act on the commands of the attacker to launch attack against the victim machine. The victim machine is flooded with multiple requests of malicious packets.

BTC China, a famous bitcoin exchange became a victim of large scale DDoS attack in 2014. It was a SYN flood attack which lasted for 9 hours and traffic level went up to 100 gigabit. Instead of army of zombie machines, a network of multiple compromised servers was used to initiate the DDoS attack. Similarly, Bitstamp and BTC-e bitcoin exchanges also became the victims of DDoS attack in 2014 and they had to suspend the transactions for 48 hours incurring huge losses.

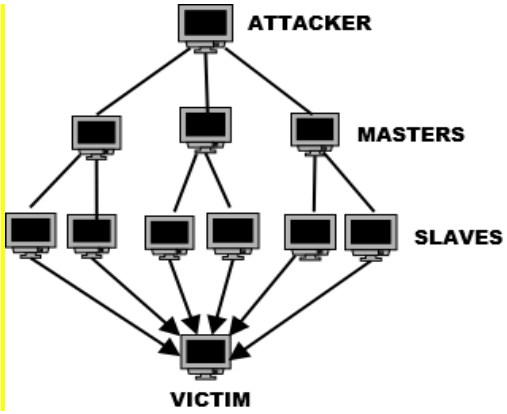

Figure 8. DDoS attack scenario

5. Taxonomy of Defense Mechanisms for Bitcoin Security

Increasing popularity of bitcoin cryptocurrency has attracted many users to it. For a user to participate in the bitcoin system, he must have a bitcoin wallet which operates as the bitcoin client node. For secure transactions proper key-management strategies [44] must be adopted for public-private bitcoin wallet keys. This is of utmost importance because if once the user forgets or misplaces these keys then the bitcoin associated with them are also lost. A compromise on the confidentiality of these keys is called wallet theft which is caused by using compromised wallet software. Bitcoin protocol uses Elliptical Curve Digital Signature Algorithm(ECDSA) [45] to

secure the transactions by digitally signing them. A different private key is used for every new transaction to keep the things very random and dynamic. For stealing bitcoins the attackers target on breaking the hash value and the signature scheme. So we can say that unlike traditional currency systems, bitcoin makes use of public-key cryptography to ensure security. This draws attention to safe storage and management of these keys.

Figure 9. Hardware wallet.[63]

Users have a variety of wallet options to choose from like- hot wallets, cold wallets, paper wallets and brain wallets. Nowadays almost all the online wallets have mobile apps which allows easy of access to the users. Although hot wallets are more prone to cyber hacks but the cold wallets are not of much usability. The more advanced wallets are paper wallet in which the private key is written and stored in a physically secure space. Brain wallets are also used which makes use of user's memory and the key is remembered by the user in a form of phrase or a sentence.

.

The biggest bitcoin exchange ever, Mt. Gox was hacked losing bicoins worth 450 million dollars. After this incident people lost trust in bitcoin exchanges and started keeping the bitcoins in their wallets. A technique named provisions is adopted by most of the bitcoin exchanges in which the exchange have to show their input transaction list to ensure that they have enough currency to pay back customers bitcoins. This is just as the traditional banks have to maintain a reserve balance amount in their treasure. There is no body to govern the security of bitcoin exchanges so the users are themselves responsible for their missing bitcoins. Security loopholes in the user's PC makes the personal information vulnerable to extortion threats so safe guarding the user's bitcoin wallet is important. Users must ensure that they are using the latest version of the bitcoin wallet software, the recent version comes with the security patches of new malwares. The backup of the bitcoin wallet must be stored frequently as an encrypted file in external storage.'

The bitcoin wallets can be divided into two categories- cold wallet and hot wallet. Cold wallets are offline wallets. Hot wallets are online wallets. Users have both of them [55]. It's like one keeps majority of one's money is savings account and keeps only a limited amount in current account for making purchases. In a similar manner majority of one's bitcoins are stored in cold wallets where the hackers cannot access them. The hot wallets are more vulnerable to security breaches due to their continuous connectivity to the internet. But the bitcoin users are suggested to keep only limited amounts of money in their hot wallet because then the hacker won't be keen on wasting its resources to get hold of a small amount of money. Bitcoin exchanges fall in the category of hot wallets because in that case the bitcoins are stored in their servers. Although intensive security practices are ensured in exchanges [56], but still it is not advisable to store all your bitcoin collection in there due to unceasing risks of zero day attacks.

Another kind of hot wallet in use is the desktop wallet. The difference is that in desktop wallets the private key is not stored at the server of the bitcoin exchange, instead it is stored on owners PC. But the bitcoins are still vulnerable if the hacker is able to compromise owners system. There are different cold wallets available, the most common being the hardware wallets. These are hacker-proof physical devices that are connected to the PC only at the time of making a transaction. To protect the private key from getting exposed, it is stored in an analog medium instead of electronic one. If the bitcoin user wants to use only hot wallet then he must ensure that

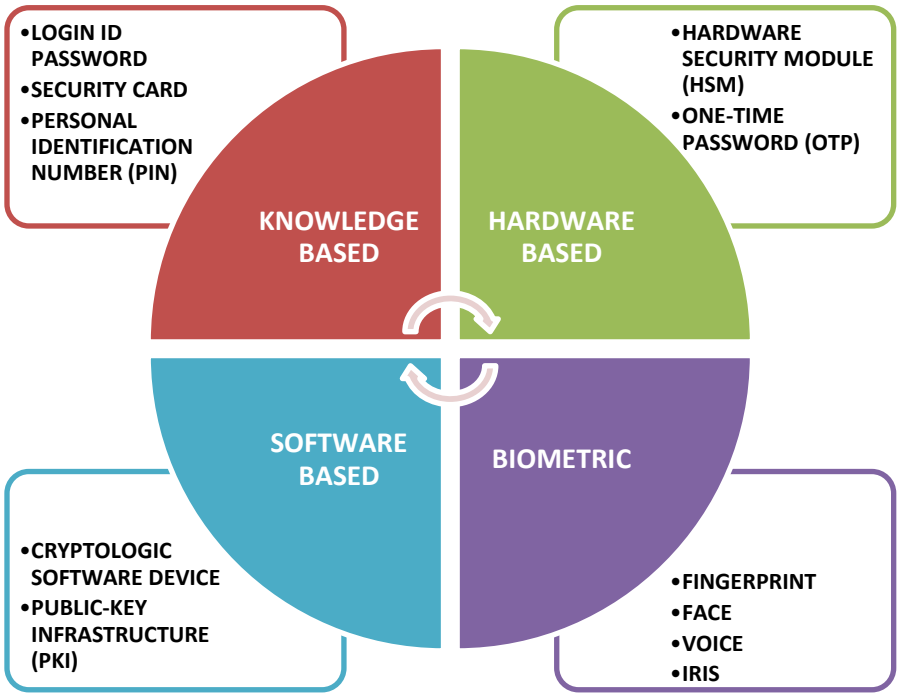

Figure 10. User authentication methods for e-financial transactions.

he uses an application which has been time-tested by the peer users and make sure that the password set is complex and long enough. It should be a combination of numbers, characters, and special symbols. And refrain from using generic details like address, phone number, and registration numbers as passwords.

Where in some countries use of bitcoins is free and legal, in some others it is a banned currency. If we talk about India, then although not illegal, it is not one of the regularized currency because of which users refrain from making transactions using bitcoins. For the transactions to take place from a bitcoin wallet, user authorization is required. Figure 10 below shows different authentication methods by which the bitcoin owner approves of the financial transaction. Each one of them can be used independently as well as in combination with one another. When they are used independently then it is called single-factor authorization. When a combination of two techniques-like login id password and one-time password both are needed to

approve a transaction then it is called two-factor authentication. Similarly, when more than two factors are required then it becomes multi-level authentication [57].

5.1. Biometric technology

Application of biometric technology in security and surveillance field is increasing day by day. Its increased use can also be seen in internet banking, smartphones, cloud computing and e-commerce. Biometric [57, 58] comprises of two words-bio and metric. Bio means life and metric means to measure. Biometric system takes into account intrinsic behavioral and physiological traits of an individual. This includes DNA, iris recognition, fingerprint, face recognition and heartbeat recognition. A statistical analysis of these features is done by the biometric system and a match is declared only when the stored data and the input data matches sufficiently. Voiceprints are a new addition wherein the characteristics of the air expelled while speaking is taken into account. There are many advantages of biometric systems over traditional authentication techniques like pin, passwords, keys and cards.

The main advantage being that it biologically belongs to one person only so it cannot be easily compromised. It is user friendly and takes away the burden of remembering PIN and passwords. Although the initial cost of setting up the biometric system is high but due to simplified user management biometric system helps in cost saving in the long run. Also the speed of finding a positive match from a large collection of data is handled by fast computers running established algorithms like image based algorithms, minutiae based algorithm. Biometric system can be integrated with existing access control systems to enhance the security levels.

5.2. Hardware Security Module

Hardware Security Module(HSM) is a tamper resistant device which is used to store, process and manage the cryptographic keys [59]. Its main responsibility is the protection of these stored keys. The processing of keys involves encryption, decryption, authentication and generation of digital signatures. They are customizable according to the application requirement. Nowadays, there is a provision of crypto hypervisors which provide on-demand cryptographic services using cloud environment.

One-Time Password(OTP) [60] is another hardware based solution in which the user needs to enter a password which is newly generated every time the user tries to log in the account. This prevents identity theft as the generated password cannot be used for a second time. Although OTP is a convenient method to ensure strong authentication, but it is prone to cyber attacks like phishing, man-in-the middle attack and keyboard logging. OTP is generated using grid cards and transaction numbers lists. Although this method is cheap, but it is slow as well. A faster way is to generate OTP using a hardware device. Nowadays microprocessor based smart cards are used for generating the OTP. They have the advantages of more processing power, portability and data storage.

5.3. Knowledge based techniques

A Personal Identification Number(PIN) is a code used to verify the identity of a user. Unlike passwords, it comprises only of numeric characters. In earlier days, PIN was only used for

transactions in Automated Teller Machine(ATM), but now its use has expanded to unlocking doors and smartphones. The user should avoid using PIN is series like 1234, 0000 and should also refrain from using generic information like date of birth, vehicle number as PIN. Longer PIN is more robust as the attacker needs to try more permutations and combinations to crack the PIN. Remembering many PINs for different cards is a tiresome job for the user, here is where the role of password managers comes in. They store the records of the account and its corresponding PIN. There are many innovative ways to create PIN like picking up numeric base against alphabets. E.g.- bitcoin will translate to 2920315914. More complex mathematical ways may also be adopted like taking modulus of user's date of birth and so on.

5.4. Public-Key Infrastructure

Some smart security cards employ Public-Key Infrastructure(PKI) [61] for strong authentication capabilities, so it is a combination of all three-hardware based, knowledge based and software based techniques as shown in the above figure. PKI is a software based authentication method used in e-financial transactions. The management and distribution of the keys used to perform encryption, decryption of bitcoin addresses and digital signatures of the bitcoin client, all is handled by PKI. It distributes accredited certificates to the participating nodes which identify them as the bonfires of the bitcoin being transferred. Each issued comprises of an electronic fingerprint.

PKI has two parts- certificate authority and registration authority. Certificate authority has to issue accredited digital certificates in sync with the PKI framework. It checks the background of the applicant to prevent any fraud. The certificate authority signs the certificate with its private key and gives its public key to the entities which want to be certified. Registration authority works as subordinate certifying authority. A certificate database is maintained which saves all the certificate requests, issued and cancelled certificates. PKI is widely used in smart card logins, Enterprise Resource Planning(ERP) and for client authentication in Secure Socket Layer(SSL). It is based on the concept of chain of trust model which is a centralized model and requires a governing body, but decentralized working is the main characteristic of bitcoin system so PKI used in here is based on a decentralized trust model called web of trust model instead of chain of trust model.

6. Conclusion

Since the advent of bitcoin in 2008, its monetary value has been through many surges, sometimes skyrocketing and crashing the other times. The bitcoin system is vulnerable to many threats as proven by multiple instances of security breaches over the time. The system has been under DDoS attack, the personal wallets and the exchanges have been hacked. Due to anonymity of users and public availability of the blockchain, it has been widely used in illegal activities such as drug trafficking and money laundering. However, the importance of digital currencies cannot be ruled out in this era of internet. Till now there is no systematic procedure or security model to ensure the safety of digital currencies but a minimum two-level authentication process is suggested.

References

1. Luisanna Cocco, Michele Marchesi,“Modeling and Simulation of the Economics of Mining in the Bitcoin Market”, Published online 2016 Oct 21.
2. N. Szabo, “Secure property titles with owner authority,” Available: http://nakamotoinstitute.org/ secure-property-titles/ , 1988.
3. Ron, Dorit, and Adi Shamir. "Quantitative analysis of the full bitcoin transaction graph." In International Conference on Financial Cryptography and Data Security, pp. 6-24. Springer, Berlin, Heidelberg, 2013.
4. Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, Nov 2008.
5. G. Wood, “Ethereum: A secure decentralised generalised transactionledger,” yellow paper, 2015
6. Florian Tschorsch, B Scheuermann, “Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies”, IEEE Communications Surveys & Tutorials, 2 March, 2016.
7. M. Rosenfeld, “Analysis of bitcoin pooled mining reward systems,” Cornel university library, vol. abs/1112.4980, 2011.
8. Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, Edward W. Felten,“SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies”, IEEE Symposium on Security and Privacy 2015.
9. V. S. Miller, “Use of elliptic curves in cryptography,” in Lecture Notes in Computer Sciences; 218 on Advances in cryptology—CRYPTO 85. Springer-Verlag New York, Inc., 1986, pp. 417–426.
10. S. your wallet:, “The bitcoin wiki,” Available: https://en.bitcoin.it/wiki/Securing your wallet, Mar. 2014.
11. J. Garay, A. Kiayias, and N. Leonardos. The Bitcoin Backbone Protocol: Analysis and Applications. Technical report, Technical report, 2014.
12. J. A. Kroll, I. C. Davey, and E. W. Felten, “The economics of bitcoin mining, or bitcoin in the presence of adversaries,” 2013.
13. M. Rosenfeld, “Mining pools reward methods,” Presentation at Bitcoin 2013 Conference, 2013.
14. A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton, NJ, USA: Princeton University Press, 2016.
15. G. Andresen, “Bip 16: Pay to script hash,” Available:“https://github.com/bitcoin/bips/blob/master/bip-0016”.mediawik , Jan. 2012.
16. Back A, “Hashcash- a denial of service countermeasure” http://www.hashcash.org/papers/hashcash.pdf (09.04.2011), Semantic scholar 2012
17. L. Luu, R. Saha, I. Parameshwaran, P. Saxena, and A. Hobor, “On power splitting games in distributed computation: The case of bitcoin pooled mining,” in 2015 IEEE 28th Computer Security Foundations Symposium, July 2015, pp. 397–411.
18. D. Malkhi, “Byzantine quorum systems,” Distributed Computing, vol. 4, p. 203213, Jan. 2012
19. Garay, Juan A., Aggelos Kiayias, and Nikos Leonardos, "The Bitcoin Backbone Protocol: Analysis and Applications." In EUROCRYPT (2), pp. 281-310. 2015.

20. B. Johnson, A. Laszka, J. Grossklags, M. Vasek, and T. Moore, “Game-Theoretic Analysis of DDoS Attacks Against Bitcoin Mining Pools”. Springer Berlin Heidelberg, 2014, pp. 72–86.
21. I. Eyal and E. G. Sirer, “Majority is not enough: Bitcoin mining is vulnerable,” Cornel university library, vol. abs/1311.0243, 2013.
22. G. G. Dagher, B. B¨unz, J. Bonneau, J. Clark, and D. Boneh, “Provisions: Privacy-preserving proofs of solvency for bitcoin exchanges,” in Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security, ser. CCS ’15. ACM, 2015, pp. 720–731.
23. C. Decker and R. Wattenhofer, Bitcoin Transaction Malleability and MtGox. Springer International Publishing, 2014, pp. 313–326.
24. “Malleability attack a nuisance but bitcoin not broken, pundits say,” Available:http://www.financemagnates.com/ cryptocurrency/news/malleability-attack-a-nuisance
25. “The bitcoin malleability attack how can it undermine the blockchains credibility?” Available: http://www.coinwrite.org/ , 2017.
26. M. Andrychowicz, S. Dziembowski, D. Malinowski, and Ł. Mazurek, On the Malleability of Bitcoin Transactions. Springer Berlin Heidelberg, 2015, pp. 1–18.
27. B. J., “Why buy when you can rent?” Financial Cryptography and Data Security. FC 2016. Lecture Notes in Computer Science, vol 9604. Springer, Berlin, Heidelberg, 2016.
28. P. McCorry, S. F. Shahandashti, and F. Hao, “Refund attacks on bitcoins payment protocol,” 2016, http://eprint.iacr.org/2016/024.
29. T. Moore and N. Christin, Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk. Springer Berlin Heidelberg, 2013, pp. 25–33.
30. Corbixgwelt, “Timejacking and bitcoin,” Available: http://culubas.blogspot.de/2011/05/ timejacking-bitcoin 802.html, Mar. 2011
31. S. Haber and W. S. Stornetta, “How to time-stamp a digital document,” Journal of Cryptology, vol. 3, no. 2, pp. 99–111, 1991.
32. J. R. Douceur, “The sybil attack,” in the First International Workshop on Peer-to-Peer Systems, ser. IPTPS ’01. London, UK: Springer-Verlag, 2002, pp. 251–260.
33. E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, “Eclipse attacks on bitcoin’s peer-to-peer network,” in Proceedings of the 24th USENIX Conference on Security Symposium, ser. SEC’15. USENIX Association, 2015, pp. 129–144.
34. G. Bissias, A. P. Ozisik, B. N. Levine, and M. Liberatore, “Sybil resistant mixing for bitcoin,” in Proceedings of the 13th Workshop on Privacy in the Electronic Society, ser. WPES ’14. ACM, 2014, pp. 149–158.
35. G. O. Karame, E. Androulaki, and S. Capkun, “Double-spending fast payments in bitcoin,” Proceedings of the 2012 ACM Conference on Computer and Communications Security, ser. CCS ’12. New York, NY, USA: ACM, 2012, pp. 906–917
36. A. Gervais, H. Ritzdorf, G. O. Karame, and S. Capkun, “Tampering with the delivery of blocks and transactions in bitcoin,” in Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security, CCS ’15. ACM, 2015, pp. 692–705.
37. H. Finney, “Best practice for fast transaction acceptance how high is the risk?” Available: https://bitcointalk.org/ index.php?topic=3441.msg48384#msg48384, 2011.
38. J. Heusser, “Sat solvingan alternative to brute force bitcoin mining,” Available: https:// jheusser.github.io/2013/02/03/ satcoin.html , 2013.

39. Vector67, “Fake bitcoins?”
Available: https://bitcointalk.org/ index.php?topic=36788.msg463391#msg463391,2011
40. C. Natoli and V. Gramoli, “The balance attack against proof-of-work blockchains: The R3 testbed as an example,” Cornel university library, vol. abs/1612.09426, 2016.
41. N. T. Courtois and L. Bahack, “On subversive miner strategies and block withholding attack in bitcoin digital currency,” CoRR, vol. abs/1402.1718, 2014.
42. S. Bag, S. Ruj, and K. Sakurai, “Bitcoin block withholding attack : Analysis and mitigation,” IEEE Transactions on Information Forensics and Security, vol. PP, no. 99, pp. 1–12, 2016.
43. M. Vasek, M. Thornton, and T. Moore, Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem. Springer Berlin Heidelberg, 2014, pp. 57–71.
44. S. Eskandari, D. Barrera, E. Stobert, and J. Clark, “A First Look at the Usability of Bitcoin Key Management,” 2015. [Online]. Available: http://people.inf.ethz.ch/barrerad/files/usec15-eskandari.pdf
45. Al Imem Ali, “Comparison and evaluation of digital signature schemes employed in NDN network”, International Journal of Embedded systems and Applications(IJESA), June 2015
46. Giechaskiel, Ilias, Cas Cremers, and Kasper Bonne Rasmussen. "On Bitcoin Security in the Presence of Broken Crypto Primitives." IACR Cryptology, February 2016.
47. L. Bahack, “Theoretical bitcoin attacks with less than half of the computational power (draft),” CoRR, vol. abs/1312.7013, 2013.
48. Mauro Conti, Sandeep Kumar, Chhagan Lal,Sushmita Ruj, “A Survey on Security and Privacy Issues of Bitcoin”, Cornelle university library, Published online July 2017.
49. J. W. Bos, J. A. Halderman, N. Heninger, J. Moore, M. Naehrig, and E. Wustrow, Elliptic Curve Cryptography in Practice. Springer Berlin Heidelberg, 2014, pp. 157–175.
50. I. Giechaskiel, C. Cremers, and K. B. Rasmussen, On Bitcoin Security in the Presence of Broken Cryptographic Primitives. Springer International Publishing, 2016, pp. 201–222.
51. P. Gallagher and C. Kerry, “Federal information processing standards (fips) publication 186-4: Digital signature standard (dss),” Available: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf , July, 2013.
52. N. A. Howgrave-Graham and N. P. Smart, “Lattice attacks on digital signature schemes,” Designs, Codes and Cryptography, vol. 23, no. 3, pp. 283–290, 2001.
53. P. Litke and J. Stewart, “Cryptocurrency-stealing malware landscape,” Technical report, Dell SecureWorks Counter Threat Unit, 2014.
54. A. F. Neil Gandal, Tyler Moore and J. Hamrick, “The impact of ddos and other security shocks on bitcoin currency exchanges: Evidence from mt. gox,” The 15th Annual Workshop on the Economics of Information Security, vol. abs/1411.7099, June 13-14, 2016.
55. Chinmay A. Vyas, Munindra Lunagaria, “Security Concerns and Issues for Bitcoin”, International Journal of Computer Applications- National Conference cum Workshop on Bioinformatics and Computational Biology, NCWBCB- 2014
56. J. J. Hoch and A. Shamir, On the Strength of the Concatenated Hash Combiner When All the Hash Functions Are Weak. Springer Berlin Heidelberg, 2008, pp. 616–630.
57. Lim, Il-Kwon, Young-Hyuk Kim, Jae-Gwang Lee, Jae-Pil Lee, Hyun Nam-Gung, and Jae-Kwang Lee. "The Analysis and Countermeasures on Security Breach of Bitcoin." In International Conference on Computational Science and Its Applications, pp. 720-732. Springer, Cham, 2014.

58. Yeom, H.-Y., Jo, H.-J., Lee, D.-H., Jeong, Y.-G., Jang, G.-H., Lee, S.-R.: Research on security criteria for extension to electronic authentication method usage-based. Final Research Report, Korea internet & security agency (December 7, 2011)
59. T. Bamert, C. Decker, R. Wattenhofer, and S. Welten, BlueWallet: The Secure Bitcoin Wallet. Springer International Publishing, 2014, pp. 65–80.
60. Wu, Longfei, et al. "An Out-of-band Authentication Scheme for Internet of Things Using Blockchain Technology." (2017).
61. J. Kroll, I. Davey, and E. Felten, \The economics of Bitcoin mining, or Bitcoin in the presence of adversaries," in Proceedings of the Twelfth Annual Workshop on the Economics of Information Security (WEIS'13), Washington, DC, Jun. 2013.
62. T. Neudecker, P. Andelfinger, and H. Hartenstein, “A simulation model for analysis of attacks on the bitcoin peer-to-peer network,” in 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), May 2015, pp. 1327–1332.
63. https://www.amazon.co.uk/Keepkey-Simple-Bitcoin-Hardware-Wallet/dp/B0143M2A5S/ref=sr_1_10?ie=UTF8&keywords=bitcoin%20wallet&qid=1491224892&sr=8-10