Journal of Cyber Security
DOI:10.32604/jcs.2021.016349
Article

Tech Science Press

A Survey on Security Threats and Solutions of Bitcoin

Le Lai[1,*], Tongqing Zhou[1], Zhiping Cai[1], Zhiyao Liang[2] and Hao Bai[1]

[1]National University of Defense Technology, Changsha, 410073, China
[2]Macau University of Science and Technology, 999078, Macau
[*]Corresponding Author: Le Lai. Email: laile19@nudt.edu.cn
Received: 30 December 2020; Accepted: 11 January 2021

Abstract: Bitcoin is known as the first decentralized digital currency around the world. It uses blockchain technology to store transaction data in a distributed public ledger, is a distributed ledger that removes third-party trust institutions. Since its invention, bitcoin has achieved great success, has a market value of about $200 billion. However, while bitcoin has brought a wide and far-reaching impact in the financial field, it has also exposed some security problems, such as selfish mining attacks, Sybil attack, eclipse attacks, routing attacks, EREBUS attacks, and so on. This paper gives a comprehensive overview of various attack scenarios that the bitcoin network may be subjected to, and the methods used to implement the attacks, and reviews the solutions and countermeasures proposed against these attacks. Finally, we summarized other security challenges and proposed further optimizations for the security of the bitcoin network.

Keywords: Bitcoin; blockchain; security; attack; P2P network

1 Introduction

As a new distributed accounting technology [1], bitcoin has attracted more and more attention in the past decade since its birth, and its price has risen from the earliest 0.06 US dollars to the highest 20,000 US dollars. Bitcoin uses the cryptography principle and the consensus mechanism of workload proof (POW) to realize the distributed data storage on the P2P network. Relying on blockchain technology, it provides a brand-new solution for the consistency in the distributed network, which has the characteristics of undeniable, non-tampering, decentralization, transparency. It creatively puts forward the method of separating from the third party in the distributed network and realizes the decentralized technical scheme. However, as the application of Bitcoin becomes more and more widespread, attacks against it happen from time to time. People are paying more and more attention to the security of Bitcoin itself.

Bitcoin prices have plummeted many times in history, many of them due to bitcoin was hacked. In 2014, the Bitcoin exchange Mt.Gox was hacked, 850,000 bitcoins were stolen, and the price of bitcoin fell from $867 to $439. In 2017, 60,000 Bitcoins were stolen in a hack of Liqui, the Ukrainian exchange, resulting in a 39.3 per-cent drop in bitcoin prices. Bitcoin has combined relevant knowledge from cryptography, game theory, economics, and other fields to create the world's first cryptocurrency based on blockchain technology. Bitcoin mining is based on solving specific mathematical problems, and the longest chain in the block is dug as a common chain, which also leads to the competition of computing power among users, resulting in mining attacks. In order to get a more stable reward, bitcoin miners form mineral pools to jointly dig mines. However, the income distribution mode in the pool is not fully considered, which may easily lead to selfish mining attacks and pool jumping attacks. Since bitcoin is a digital currency, there is the possibility of double-spending. The bitcoin author also took this into account and adopted the confirmation of 6 blocks to make this probability very small. At the same time, the P2P network of Bitcoin application makes the ledger of all nodes consistent, which is a good idea, but ignores

the various problems of the real network transmission: the selection vulnerability of the bitcoin system to connection nodes leads to the possibility that all the connected nodes may be malicious, thus causing the nodes to be attacked by the eclipse attack; When bitcoin nodes are propagated between autonomous systems (AS), they may cause routing hijacking attacks, resulting in the tampering of the transmitted data. What's more, the data transmitted by bitcoin nodes are not encrypted, which makes it easy for attackers to tamper with data by eavesdropping on the network. Other attacks such as DDOS attacks can also be applied to bitcoin systems. This shows that bitcoin has multiple attack threats in terms of consensus currency, encryption mechanism, network connection, incentive mechanism. This article discusses the currency facing all kinds of safety defects from the working principle of the currency, the security problem, and the corresponding solutions are proposed according to the corresponding problems and some suggestions for future research.

The organization of this paper is as follows: The second section briefly introduces the related knowledge of bitcoin and blockchain, including the cryptography knowledge involved in blockchain. The third section introduces the security threats encountered in the bitcoin environment and the ways to use them. In the fourth section, we discuss the countermeasures and solutions to the security problems of bitcoin. Section 5 analyzes other security challenges that the Bitcoin network may face. In Section 6, we summarize the whole paper.

2 Research Background

2.1 A Brief Introduction to Bitcoin

2.1.1 Bitcoin Block

Bitcoin is a kind of a specific data structure in the form of a chain according to the time sequence data onto the block combination, and ensure the tamper-resistant in cryptography and unforgettable decentralized, distributed shared general ledger system to trust [2]. It is a kind of distributed database solution, the miners around the world constantly maintained the blockchain, each miner is a peer node, don't need any third-party organizations. Nodes can join or exit at any time. When nodes join, they will download all blocks of the blockchain from the P2P network since its creation. This distributed ledger can realize the whole network record and traceability.

2.1.2 Consensus Mechanism

The bitcoin consensus protocol is responsible for keeping the blocks of the whole network nodes consistent, while the bitcoin network is a decentralized system in which all nodes are equal and share the functions of the transaction, communication block, verification block, mining and so on. The nodes in the Bitcoin network are dynamically changing, and any node can join or quit the bitcoin network at any time. Bitcoin nodes can also be malicious, deliberately delaying the sending of network data or sending the wrong data onto profit.

Traditional distributed systems mostly adopt CAP standard [3], that is, distributed systems cannot ensure consistency, availability and partition tolerance simultaneously. Some features are often weakened in actual requirements. The bitcoin network uses a consensus algorithm based on POW to keep the entire network consistent. POW is a probabilistic algorithm that contains a mathematical puzzle, similar to Hashcash [4]. The final confirmation of consensus is the existence in the sense of probability. The Bitcoin system believes that the block can only be considered as the final confirmation if there are more than six blocks. In the consensus algorithm based on POW, nodes obtain the packaging right of blocks through calculation forced competition. The higher the node calculation force is, the easier it is to obtain the billing right, but this consensus algorithm is vulnerable to 51% attack. Nodes can join the network without verifying their identity. This makes the Bitcoin consensus model extremely extensible.

2.1.3 Trading Mechanism

Transactions in bitcoin use the UTXO model, a transaction based on the UTXO model consists of

input and output and transaction information, both of which can be multiple. The bitcoin mining node is rewarded by the new block, at which point the transaction has only output, it is a coinbase transaction, and as the first transaction in the block, its output is an UTXO. The transaction fields include the bitcoin version, the transaction hash, the script PubKey, input, and output. You can only use UTXO if you know the lock script. The input to the transaction contains the user's public key and user signature to authorize, and the output of the transaction indicates a certain amount of bitcoin and meets the corresponding conditions to lock up the amount. When the output of a previous transaction is used by a new transaction, the bitcoin value of the output address must be fully spent, and the unused amount will be used as the difference to enter the new change address. With this approach, we can quickly identify unused Bitcoin in a user's address simply by looking at the output of previous transactions. For example, Alice has 10 Bitcoins and wants to pay Bob 3 bitcoins. At this time, Alice initiates a transaction with the addresses of 10 Bitcoins as input, one with the output of 3 bitcoins is transferred to Bob's address, and the rest of the output is returned to Alice's change address in addition to the transaction fee. After the transaction, Alice's initial input address balance is 0.

The bitcoin node validates each transaction by executing a locking script and a unlocking script. The locking script is P2PKH [5] and only the owner's signature is required to authorize transaction. Unlocking scripts is a combination of signatures and public keys. The transaction is valid only if the locking and unlocking script meets the valid conditions. When the block enters an inconsistent state, all nodes select the state that most miners agree to update the local copy of the blockchain, so as to achieve the unity of the blockchain.

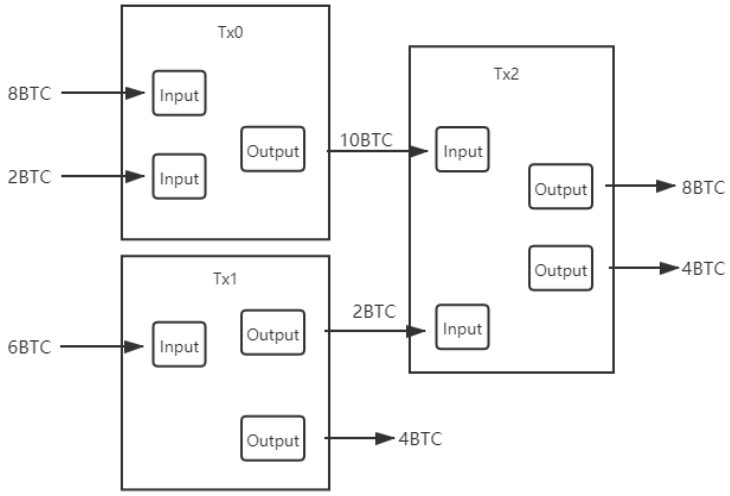

Figure 1: Bitcoin transaction model

2.1.4 P2P Network

Bitcoin nodes are based on peer to peer (P2P) network [6]. The nodes are connected by TCP protocol, and in general, port 8333 is used. A node can start up to 8 outgoing connections and can accept up to 117 incoming connections. Nodes only propagate and store nodes that have a public IP address. When a new connection is established by a node, the IP packet header is compared with the bitcoin version information to determine whether the other party has a public IP. The nodes put the saved IP list in the IP pool, and adopt a specific algorithm to disperse the IP segment of the same C class. When the incoming connections are less than 8, they will randomly select IP from the IP pool for connection. The Bitcoin network broadcasts INV messages to make new block announcements. When the miner finds that the number of blocks is less than that of other nodes, he requests a new block to the neighbor node by sending a GETDATA message. The neighbor node responds to the new block with a BLOCK message. To reach achieve consistency, recently discovered blocks are propagated over P2P network by flooding.

2.2 Knowledge of Cryptography in Blockchain

2.2.1 SHA-256 Algorithm

Bitcoin uses Proof-of-Work (POW) workload proof mechanism to determine who keep the accounts, thus ensuring the security of the system. The bitcoin's proof of work does turn out to be actually solving mathematical problems. The concrete implementation is to add nonce value to a basic string and perform SHA-256 operation on the newly formed string [7]. The hash result obtained takes the leading value of "0000" as the calculation success, and the whole process require a certain amount of computing power. The Bitcoin network adjusts the difficulty of nonce according to the computing power of the whole network dynamically, a block is generated about every 10 min.

SHA-256 is one of the SHA family of secure hashing algorithms. For messages of any length, SHA-256 produces 32 bytes of length data, called a message digest, and SHA-256 has strong resistance to collision and modification. Bitcoin transaction data and block header data use the SHA-256 algorithm to ensure data integrity and non-modifiable.

2.2.2 Public Key and Private Key

Bitcoin account addresses are created using a public-private key mechanism. The ownership of bitcoin is determined by the bitcoin address. The public key is calculated from the user's private key, and then the public key is compressed and encrypted by some algorithms to generate a specific Bitcoin address. The essence of the private key is a 256-bit binary random number. The total number of private keys are about 10^{77}, while the number of visible atoms in the universe is about 10^{80}, which ensures that the repeatability of the private key is almost impossible. The private key is held by the user and cannot be disclosed. Otherwise, there is a risk that the bitcoin in the account will be lost. Public keys can be posted online and made available to anyone. Data encrypted by the public key can only be decrypted with the corresponding private key and used for the user's Bitcoin address. The private key is often used for digital signature to verify the user's legal identity.

2.2.3 Merkle Tree

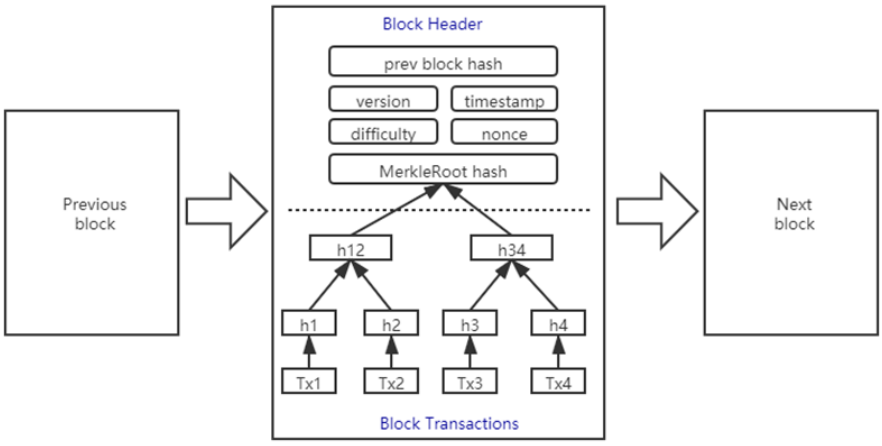

Figure 2: Bitcoin Merkle tree in blockchain

The Bitcoin block is composed of Merkle tree [8]. Merkle tree is a binary tree composed of a root node, intermediate node and leaf node. Each transaction is each leaf of the tree, and the hash value of the node is computed by hashing the two children below it, recursively layer by layer, and finally the root hash of the Merkle tree. Any transaction of a leaf node is modified, and the leaf node hash value changes, causing the final root node to change. Therefore, as long as the value of the root node does not change, you can guarantee that the transaction of each node does not change.

Bitcoin adopts a Merkle tree structure. To verify the existence of a transaction, nodes only need to calculate the existence of the final root node hash in the block layer by layer. With the Merkle tree, each transaction can be deleted individually, only the hash value of the transaction can be saved, and more transaction data can be stored in memory.

3 Bitcoin Security Issues

3.1 Mining Attack

3.1.1 Selfish Mining Attacks

Selfish mining is a mining strategy against the bitcoin POW workload proof mechanism, in which miners do not broadcast new blocks when they find them, but deliberately delay the new blocks when they find them, and publicize them at an appropriate time, in order to undermine the profits of honest miners. The concept of selfish mining was first proposed in the literature [9]. The article pointed out that selfish mining attack is an abnormal mining strategy, whose purpose is to invalidate the largest block mined by other miners in the network. The author believes that this mining strategy will break the Bitcoin protocol.

The selfish mining attack strategy in literature [9] is as follows:

(1) The attacker records the private chain corresponding to the bitcoin public chain. When a block is dug in the private chain, the attacker does not immediately broadcast it. When an honest miner also digs the block, the attacker immediately broadcasts the block it has dug. At this point, the bitcoin network has two chains competing to become the main chain.

(2) If the advantage of selfish miners is two blocks when an honest miner finds a block, the attacker immediately broadcasts the two blocks dug before, then the whole network will switch to the bifurcated chain where the attacker is.

(3) If the selfish miner's advantage is greater than two blocks, when the honest miner digs a block, the attacker immediately releases a block and continues to compete with the new honest block.

Assuming that the proportion of the adversary's hash rate and the total network hash rate is α, and the proportion of honest miners following private mining is γ, when α and γ meet the Formula (1), the attacker can get extra income than honest mining. The values of α range are (0,1/2). When γ = 100%, that is, when all honest miners follow the attacker's private chain, no matter how much the attacker's calculation force is ($\alpha > 0$), the attacker can get more income than the honest mining; When γ = 0%, that is, when all honest miners do not follow the attacker, the attacker's computing power needs to be greater than 1/3 of the total network computing power to obtain additional benefits ($\alpha > 1/3$); In general, honest miners randomly choose the public chain and the attacker's private chain, that is, γ = 50%, when the attacker's computing power needs to reach 1/4 of the total network computing power, the adversary can get an extra income.

$$\frac{1-\gamma}{3-2\gamma} < \alpha < \frac{1}{2} \tag{1}$$

Literature [9] proposes a specific deviation between the selfish mining attack and the standard protocol (SM1 policy). The Bitcoin protocol requires nodes to broadcast discovered blocks immediately, but the high computing power node can obtain higher returns by retaining the created blocks and selectively delaying their release. In this paper, the markov model is adopted, but the problem of persistent attack time is not considered. Therefore, SM1 model has some defects.

Literature [10] puts forward the profit threshold, that is, the minimum resources needed for the attack to obtain profits. The authors analyze the lower bound of system security against attack and evaluate the sensitivity of protocol modification to selfish mining. Finally, the selfish mining problem with communication delay is studied, and it is pointed out that under the model considering delay, the profit threshold disappears.

3.1.2 Mining Pool Attacks

Bitcoin based on computing power mining, and mining machine has become the mainstream of mining market, mining machine is popular, mining alone is difficult to get rewards, so miners must join up to become mining pool, to have a chance to get the rewards distributed by the mining pool. After the mining pool gets the block, a profit is paid according to the proportion of the miners' workload. The pool is managed by the pool manager, who, so as to estimate the computing power of the miners, gives the nonce value less difficult than that of the Bitcoin network to the miners. The miners calculate the part of proof of work (PPOW), while the actual nonce of Bitcoin is the full proof of work (FPOW). Through the development of a series of measures to ensure the fairness of miners' income, Rosenfeld [11] analyzed several mainstream mining pool incentive income models. In the early stages of the bitcoin pool, a proportional reward mechanism was adopted, taking the time between the two blocks found in the pool as a cycle, and the block reward was calculated by calculating the proportion of shares shared by miners. This method is unfair and can lead miners to use Pool hopping [12] to get more profits. PPS (Pay-per-share) model is based on the share submitted by miners. By calculating the proportion of computing power, miners can obtain real-time income, and obtain stable income based on the proportion of computing power. The PPLNS model takes N shares of distribution reward before block discovery, which is proportional to the optimization of the model and prevents the miners' jumping behavior. Literature [13] and literature [14] propose different mining methods and incentive systems. Fig. 3 [15] illustrates the current distribution of mining pool computing power in 2020.

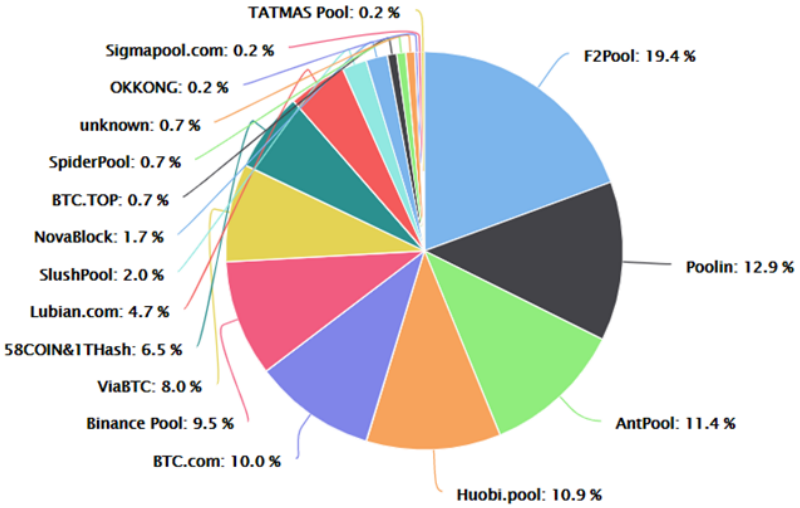

Figure 3: Pool Distribution in Present Market in 2020 [15]

After the pool is formed, the attacks on the mineral pool have been increasing. The literature [11] puts forward pool-hopping, pointing out that the expected income of a pool changes with the state of the capital pool. For the sake of getting the maximum income, miners dig when the attraction of the Pool is high, and choose another Pool with high income to dig when the attraction is low.

Selfish mining behavior can also occur in mining pool. The profit of selfish mining attack is related to the attacker's hash rate and network environment. When the attacker's computing power exceeds 1/3 of the total network, he can get extra income than normal mining, which is still a high requirement for computing power. Aiming at the shortcomings of the selfish mining, literature [16] proposed the stubborn mining, it points out that the selfish mining for complex parameter space strategy is not the best, according to different environmental parameters, the stubborn mining strategy can be 25% higher than selfish mining profits.

3.1.3 BWH Attacks

A more classic attack in the mining pool is called the block withholding attack. This attack method was first proposed in the literature [17]. When the attacker joined the pool, he would submit only PPOW and discard FPOW. In this way, the miner would not contribute any income, but would receive dividends from other miners in the pool. Two block interception schemes, sabotage and lie in wait, are proposed in this paper. In the first case, the attacker does not submit any blocks, this will reduce the benefit to the pool and other miners. The second type is lie in wait, in which the attacker uses a cover-up attack. Both attacks are irrational, in that they yield less than honest mining.

Literature [18] improved the classic block interception attack, enabling the attacker to gain more income than normal mining through block interception attack. In the scheme, the attacker's calculation force is divided into two parts: one part carries out block interception attack inside the mining pool, and the other part carries out honest mining outside the mining pool. It is proved by calculation that when the calculation force is reasonably distributed, the profit will be higher than that of honest mining. It is further verified that the maximum benefit is obtained when a block interception attack is carried out with half computing power.

We note that BWH attack did not occur on a large scale in the Bitcoin network, mainly because of the miners' dilemma. This view was first proposed in the literature [18]. Miner's dilemma refers to a strategy in which two mining pools can take normal mining or attack each other to maximize their profits, similar to the prisoner's dilemma. This article defines a game in which mining pools can use the miners in the pool to penetrate other pools to attack. For any number of pools, poolless attacks can reach the Nash equilibrium, and if there are no other pool attacks, a pool can gain additional benefits by attacking other pools. In the case of two pools, both sides can attack each other when faced with the miner's dilemma. When a pool chooses to attack, the pool gains will be reduced. The pool gains can be increased by retaliating attacks. However, when both players attack, both players gain less in the Nash equilibrium than when both players do not attack. A similar situation occurs with symmetric equalization for multiple pools of equal size. If that balance is broken, the revenue from the open pool will be reduced, making it unattractive for participating miners.

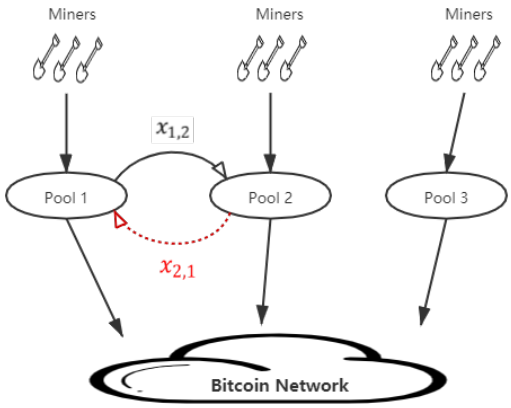

Figure 4: The Miner's dilemma

3.1.4 FAW Attacks

In the literature [19], a combination of BWH attack and selfish mining attack is proposed, which is called FAW attack. At the beginning of the attack, the attacker did the same work as the BWH attack. When the attacker discovered FPOW, unlike the BWH attack, he kept the FPOW and did not submit. When a miner discovers a new block outside the pool, the attacker immediately submits FPOW to form a new fork.

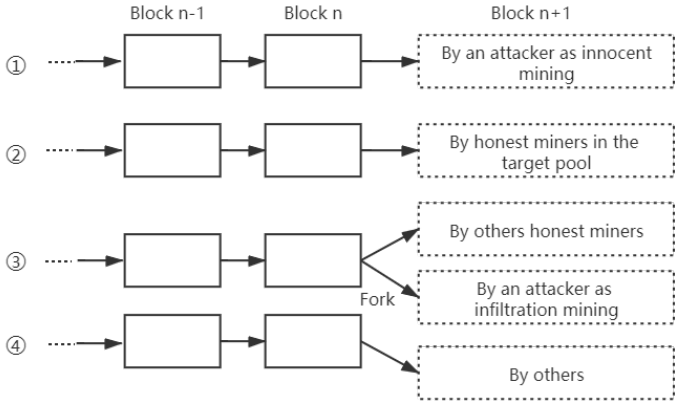

Figure 5: Four scenarios of FAW attack. The attacker can earn benefits in cases ①, ②, ③

A FAW attack can gain more than a BWH attack because the attacker's fork has a probability of forming the main chain. The authors show that FAW attacks receive rewards greater than or equal to BWH attacks, and that FAW attacks per pool are four times as frequent as BWH attacks. When multiple pools are taken into account, FAW's bonus is approximately 56% higher than the BWH attack bonus. Also, when two pools engage in FAW attacks against each other, the miner's dilemma may not hold: in some cases, it may be related to the calculation forces between the pools, and the larger pool can continue to win [20]. What is different from selfish mining is, the FAW attack is more actual when it comes to bifurcating and can yield additional benefits.

Table 1: Summary of Mining attack

Attack	Attack condition	Adverse effects
Selfish mining	Adversary controls more than 33% Hashrate	Double spending
Pool-hopping attack	Expected earnings vary according to the pool's current state	damages the overall attractiveness for participants who mine continuously
Stubborn mining	Adversary controls more than 33% Hashrate and under certain conditions	Double spending; 25% more revenue than selfish mining
BWH attack	Adversary choose the right proportion of Hashrate	Decreases the pool and honest miners' revenue
FAW attack	Adversary controls certainly Hashrate and better network condition	Decreases the pool and honest miners' revenue; double spending

3.2 Double Spending Attack

In digital cash, the most important is to solve the problem of double-spending, that is, the same digital cash will not be paid twice in different transactions. In the bitcoin white paper, the author mentioned the concept of double-spending attack and applied a series of mechanisms such as distributed timestamps [20] and consensus protocol [21] to solve this problem, but the problem is still not completely solved.

3.2.1 51% Attack

The concept of a 51% attack was put forward in the Bitcoin white paper. The principle is that a node in the network has more than 51% of the whole network computing power. Thus, we can recalculate the identified blocks and determine the generation of new blocks. A double spending attack is achieved by invalidating a recognized block.

The specific implementation of 51% attacks is as follows: Assume that the attacker has more than 51%

of the computing power, when attacker A initiates a transaction to merchant B (A,B), trading on the main branch of the currency, because the attacker has more computing power than the rest of the entire network, so attackers can generate blocks faster than the remaining nodes in the entire network, it can also create A branch, A branch can be longer than the main branch, the attacker A launch another transaction (A,C), C and A are the address of the attacker, this transaction uses the same Bitcoin as (A,B) transaction, because branch A longer, so will be the main branch, This invalidates the transaction on the original main branch (A, B). In this way, a double-spending attack is achieved by mastering more than 51% of the computing power.

3.2.2 Finney Attack

Finney attack is proposed by bitcoin user Hal Finney, refers to when A miner to dig into A block, not broadcast immediately, but in the block contains transaction from A to B (A and B are attackers address), and then find A accept zero confirmed trading businesses, set up A to C transaction, when stores after the confirmation, immediately announced new blocks, so A to C transaction void. In this way, a double spending attack of the same kind of transaction is realized.

Finney attacks target merchants that accept zero-confirmation transactions, which are very insecure. According to Nakamoto's white paper on Bitcoin, transactions that have been confirmed in six blocks have greatly improved security. At the same time, the Finney attack is also very costly, because the discovery block is not broadcast at the same time, other miners are likely to generate blocks, causing the block found by the attacker to become invalid, therefore, the transaction that the attacker uses to purchase the immediate shipment from the merchant will be valid.

3.3 P2P Network Attack

The bitcoin network is a peer-to-peer network, to establish a decentralized network with equal status among all nodes. However, the order in which nodes join and the network topology between nodes affect the fairness of the Bitcoin network, in recent years, attack methods increase on the bitcoin network, such as bitcoin network DDOS attacks, Sybil attack [22], eclipse attack [23], BGP hijacking attack [24], and the network partition attack [25], etc.

3.3.1 DDOS Attack

DDOS attack [26] is a relatively common attack mode in the network. It uses the attacked computers in the network to carry out continuous attacks on the target at the same time, and consumes the network resources of the target on a large scale, making it unable to provide normal services. DDOS attacks are inexpensive to launch, but can be extremely destructive. In DDOS attacks, attackers consume network resources to bring effective competitors out of the network, thus improving the effective mining rate of malicious miners. Literature [27] puts forward the game theory competition model between DDOS attackers and defenders, and discussed the trade-offs among these strategies.

3.3.2 Sybil Attack

Sybil attack is a form of attack on P2P networks. The attacker uses a single node to forge multiple identities in P2P networks and weakens the role of redundant backup by controlling most nodes of the system. In a Bitcoin network, an attacker wants to separate a user and disconnect the user-initiated transaction, otherwise the user can only select blocks controlled by the attacker. At the same time, if there are no other nodes to confirm the transaction, the user is isolated, and the user's input can be used in a double-spending attack.

3.3.3 Eclipse Attack

Unlike sybil attacks, eclipse attack is an attack on a single node. Literature [23] puts forward the concept of eclipse attacks: the attacker by controlling a sufficient number of the network node to monopoly victims all incoming and outgoing connection, make the network isolation between bitcoin network and victims, deceive the victim, and attack its bitcoin mining and consensus system, including

zero confirmed double spending, selfish mining, forks in the block. The paper quantifies the resources involved in the attack through probability analysis, Monte Carlo simulation and real-time experiments of Bitcoin nodes, and proves that the number of IP required by botnet is less than that required by an infrastructure attack.

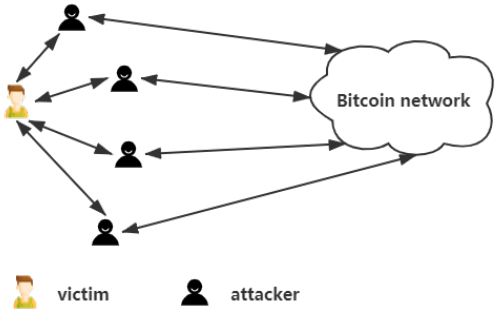

Figure 6: Eclipse attack

3.3.4 BGP Hijacking Attack

Bitcoin network is composed of the nodes in the Internet, nodes are connected by routing devices in their respective autonomous systems. Literature [24] first proposed a method to attack Bitcoin via Internet routing infrastructure, namely through hijack BGP protocol or natural intercept traffic, autonomous systems (ASes) can intercept and control much of the bitcoin flow, based on a single node of the small-scale attack and attack by the entire network, introduces the routing attacks on the impact of the bitcoin, confirmed the feasibility of routing attacks become two key features: the routing operation efficiency and the centralization of mining. Specifically, even if the pool is multi-hosted, any attacker can isolate 50% of the computing power by hijacking less than 100 BGP prefixes. The research also shows that due to the unencrypted nature of bitcoin messages, network attackers on the path can interfere with very few Bitcoin messages to significantly slow down the spread of blocks, causing nodes to waste part of the mining capability. The harm of BGP hijacking attack includes isolating part of network or delaying block propagation, wasting a lot of computing power and double spending attack. Finally, the author puts forward some countermeasures to eliminate these effects in practice.

3.3.5 EREBUS Attack

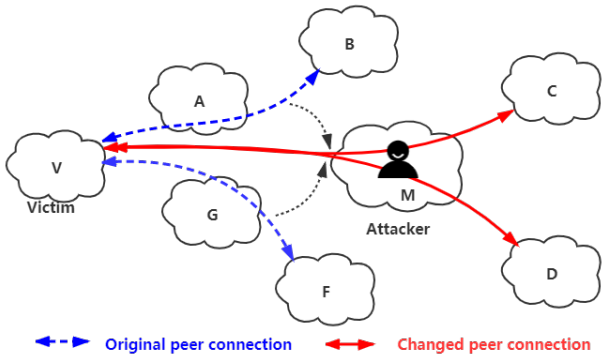

Figure 7: EREBUS attack

An adversary can use BGP hijacking to split a Bitcoin peer network, but the attack is obvious and the attacker's identity is easy to discover. Literature [28] proposed EREBUS attack, which is more covert. It divides the Bitcoin network without any routing operation, making the control layer and even the data layer unable to detect the attack. The article points out that network opponents can influence peer-to-peer decisions of Bitcoin nodes by using abundant network address resources for a long time at negligible cost.

In the simulation test, the author found that by sending low-speed attack traffic, EREBUS attacks can be successfully launched against Tier-1 and Tier-2ases in about 4–5 weeks. EREBUS attacks can be launched by national adversaries, who are willing to patiently execute complex attack strategies to damage cryptocurrency. Finally, the author provides some suggestions for the core modification of Bitcoin to effectively deal with the EREBUS attack.

Table 2: Summary of attacks to Bitcoin network

Attack	Description	Adverse effects
DDOS attack	Exhaust network resources	Deny services to miners
Sybil attack	Single node to forge multiple identities	Isolate the miners; double spending attack
Eclipse attack	Forced network isolation between the Bitcoin network and the victim	selfish mining, N-confirmation double spending; make forks in the blockchain
BGP attack	Hijack routing to split Bitcoin's P2P network	Separating the Bitcoin network; Slowing down the spread of block
EREBUS attack	Split Bitcoin’s P2p network stealthier	Same as BGP attack

3.4 Bitcoin Privacy Leak Attack

3.4.1 Global Ledger Privacy Issues

Blockchain systems store transaction books in a publicly available global ledger, accessible to anyone, and every transaction can be traced. This creates a risk of privacy leakage [29]. Although the bitcoin transaction address is encrypted with the private key, and a user can generate many transaction addresses, with the rise of big data and data mining, it is not difficult to mine the relationship between user addresses. Literature [30] analyzes this relationship and can use a complete blockchain analyzer to link bitcoin users to a set of public addresses. Literature [31] proposes a method to create bitcoin-IP address mapping using only 5 months of real-time transaction traffic. Literature [32] evaluated the bitcoin privacy issue by analyzing the public blockchain. Literature [33] points out that the use of multi-signature addressing technology has an impact on user privacy.

3.4.2 Authentication and Encryption Issues

In Bitcoin, the private key is the primary authentication token. Bos et al. [34] pointed out that it is not enough to use elliptic curve cryptography to export bitcoin addresses to users, and there is no randomness required. Ateniese et al. [35] proposed a bitcoin authentication system, which provides an opt-in guarantee, only sends and receives Bitcoin to authenticated users, and trusted institutions control the creation of bitcoin addresses. Through this method, a third-party institution is introduced, which violates the original design intention of Bitcoin. However, this method improves the dependability of real social entities on the system.

3.4.3 Privacy Issues on the Tor Network

Tor network is a kind of anonymous network. When a user accesses an address of the network through Tor, the nodes he passes through are randomly selected in the Tor node, thus ensuring the anonymity of the user. However, Biryukov’s et al. [36] research has shown that using the currency in the Tor network does not increase the anonymity, the attacker can completely control with low resources selection in the Tor network using the currency flow of information between all users, in particular, the attacker regardless of what the user use pseudonyms can be the user’s transaction link together, and control which the currency block and trading are forwarded to the user, users can also delay or discarded the trading and block. The article also shows how to fingerprint users and identify their IP addresses when they connect directly to the Internet, which further aggravates the issue of privacy leakage.

4 Solutions to Bitcoin Security Problems

In this part, we will discuss the latest solutions according to various bitcoin security issues proposed in Section 3, and add improvements to Bitcoin and underlying technologies to cope with various attacks against the Bitcoin network.

4.1 Mining Attack Countermeasures

4.1.1 Selfish Mining Countermeasures

Selfish mining destroys the mechanism of the Bitcoin network, deceives the incentive mechanism of the Bitcoin network, and threatens the trust system of the Bitcoin network. To deal with the threat brought by selfish mining, literature [9] proposed a solution, that is, to make simple and backward-compatible changes to the protocol. This approach would reduce the capacity of the selfish pool.

To improve the countermeasures against selfish mining, literature [37] proposed a new defense measure against selfish mining, increasing the minimum mining power share required for selfish mining profit from 25% to 32%. The article suggested the concept of "Freshness Preferred", a strategy in which the Bitcoin protocol was modified to invalidate any chunk of data that did not have a timestamp, or that was older than that. Because selfish mining uses a block-holding tactic, the application of this strategy will reduce the incentive for selfish mining as the detained blocks will become invalid. Another defense against selfish mining is proposed in the literature [38], in which the miner is required to issue a less difficult intermediate block (block-in-block), and when bifurcation occurs, the branch with the greatest total effort will be used instead of the longest chain. This defense is based on a key observation: selfish miners may find a longer chain than the standard chain, but the total amount of work in this chain must be less than the common chain. In this scheme, selfish miners need half the computing power of the network to gain an advantage, so selfish mining is no longer a threat.

4.1.2 Pool Attacks Countermeasures

Because of the Pool-hopping in the mining pool, literature [39] proposes several methods. The first method is the Maximum pay-per-share (MPPS), in which two balances, PPS balance and proportional balance, are reserved for participants. PPS balance increases each time a participant submits a share; Each time a block is found in the pool, the proportional balance of the participant increases. The second is the PPLNS (Pay-per-last-N-shares) approach, which abandons the concept of "rounds" based on traditional pools. By doing so, it eliminates the notion of early mining for profit and prevents pool hopping.

4.1.3 BWH Attacks Countermeasures

Aiming at the BWH attack of mine pool, the literature [39] proposed a solution to "Oblivious shares", which needs to modify the protocol and allow the shares to be oblivious-a miner cannot find that the shares submitted by himself are valid blocks. Literature [40] proposes the concept of a "special reward", which is a scheme designed to give additional rewards to miners who actually discover blocks.

4.2 Double Spending Countermeasures

According to the Bitcoin white paper, double spending can be restricted for malicious miners through consensus algorithm and timestamp mechanism based on PoW. The purpose of PoW is to synchronize the blocks of network nodes, thus avoiding double spending attacks on users. The timestamp mechanism ensures that the time sequence of transactions in the block is fixed and prevents tampering of the block. The most effective way to prevent double spending is to wait for confirmation of multiple blocks, and transaction with six block confirmations is considered stable.

Literature [41] proposes a lightweight countermeasure to detect double spending attacks in fast transactions. The article summarizes the strategy recommended by bitcoin developers to resist the double spending of using a listener period and inserting an observer. Also, an effective countermeasure based on double spending "alert" message is proposed. In a countermeasure with a listener period, the seller

correlates the listener period with each transaction and monitors whether any received transactions attempt to reuse the bitcoin received by the seller. Insert observer technique is based on using the listening period extension, and insert a group of observers in the currency network to relay the seller receives all transactions, this method helps detect double spending, because all the affairs of double spending received by at least one observer in a few seconds, but extra cost increased to maintain the observer. The third strategy is to convey a double spending alert between peers: a bitcoin peer propagates an alert when it receives two or more transactions that have the same input. The advantage of this approach is that the alert cannot be avoided by an attacker and does not impose additional costs on the seller. Because most bitcoin peers are honest, when they receive two transactions with the same input, an alert is immediately broadcast to the entire network peer, which reaches the seller within seconds, so that the attacker's double spending can be detected.

Literature [42] proposes the introduction of decentralized non-secured contracts in Bitcoin to punish fraud in distributed systems. The core of these contracts is an encryption primitive called a "responsible assertion", in which the payer seals some coins in the deposit when making a transaction with the payee. Payers of double spending will be punished by losing coins.

4.3 P2P Network Protection

4.3.1 DDOS Attack Countermeasures

Literature [43] proposes to detect botnet activities by monitoring network traffic and determine which part of the network has problems. Therefore, this part can be isolated to prevent damage to the network. Literature [44] puts forward Proof of Activity, which is robust to DDOS attacks. Other ways to prevent DDoS attacks include: (1) Securely configuring the network to disable malicious data from other ports, and (2) Monitor the network through other DDoS protection schemes.

4.3.2 Eclipse Attack Countermeasures

Literature [23] for eclipses attack in a series of defensive measures are put forward, including: (1) Improved the expulsion process of node address, put the new address in a bucket deterministically, in this way, the attacker can't increase the number of storage addresses by repeatedly inserting the same address multiple times, to reduce the storage in the tried table attack address. (2) Improving the selection process of IP address and randomly selecting addresses from the tried table and new table. (3) Test before evict. Before attempting to store an address in the bucket you have determined to select, first check that whether the bucket contains an old address. If yes, simply try to connect to the old address, and if the connection succeeds, the old address will not be evicted from the tried table; The new address is stored in the tried table only if the connection fails. (4) Feeler connections. When an outgoing connection is added, a new randomly selected address is set up for a short-term connection test. If the connection is successful, drive out the new table and insert the tried table; Otherwise, drive out the new table. This method cleans up garbage addresses. (5) Design more buckets to store IP addresses and make more external connections.

4.3.3 BGP Hijacking Attack Countermeasures

Literature [24] proposed short-term and long-term measures for BGP hijacking. Short-term measures are (1) to increase the ways of node connections. The node obtains additional connections through multi-homed form and using services such as VPN to ensure that traffic in and out of the node passes through different ASes. (2) Select the bitcoin peer while considering the route. The nodes send traceroutes to their peers, analyze the frequency of the same autonomous system, and establish additional random connections if the same AS occurs. (3) Deploy the anomaly detection mechanism by monitoring RTT time and other statistical information to identify sudden abnormal connections. Long-term measures are (1) Encrypt bitcoin communication. Encryption prevents eavesdropping and uses message authentication codes to verify that the message content has not been modified. (2) Use different control and data channels. Bitcoin uses the default port (8333) for data transmission, which is easier to be identified by AS-level attackers through filtering. If a random set of TCP ports is negotiated after connection and used

to exchange Bitcoin data, an AS level attacker will not be able to track all ports to monitor Bitcoin traffic. (3) Request the same block from different nodes. Bitcoin clients prevent malicious nodes from deliberately delaying block propagation by requesting blocks from multiple peers. (4) Use UDP heartbeat. Bitcoin clients can send UDP messages with confirmation data regularly. they will make the node aware of the connection being blocked and establish a new connection.

Table 3: Summary of attack countermeasures

Attack	Possible measures
Selfish mining	Supervise mining pools for changes in computing power; wait for several confirmation blocks.
Pool-hopping attack	Use PPLNS method or MPPS method.
BWH attack	Use "Oblivious shares" method.
Double spending attack	Using a "Listening Period" and Inserting Observers in the Network.
DDOS attack	Detect botnet activity by monitoring network traffic.
Eclipse attack	Use whitelists, disabling incoming connections.
BGP attack	Use different control and data channels; Encrypted Bitcoin communication.

5 Other Challenges of Bitcoin Security

5.1 Balance between Privacy Protection and Regulation

Bitcoin is a decentralized system without third-party supervision, which also leads to the frequent use of bitcoin in various criminal activities, such as the global outbreak of "WannaCry" ransomware in 2017, the author uses the bitcoin address for payment. Due to its anonymity, Bitcoin is often used to provide trading tools for criminals on the Dark web. The Dark web is a network hidden under the regular Internet, which, because of the anonymity of Bitcoin, generates more criminal or money laundering activities. Due to political and various aspects reason, bitcoins in many countries are not recognized as a currency. The decentralized nature of currencies also makes many countries cautious about it. Strengthen the balance between privacy protection and reliable regulation can make the currency system get better development.

5.2 Incentives for Miners

According to the currency consensus mechanism, miners achieve the proof of work by constantly calculating the hash value of the specified conditions, then get rewards, which are halved every four years. Based on the current price of bitcoin, the electricity bills used by miners for mining have accounted for most of the market value of bitcoin rewards [45]. In the future, the rewards received by mining will continue to decrease. The income from mining by miners may be greater than the expenditure. In this case, there will be fewer and fewer new miners, and the mining power will be concentrated in large mining pools, which is not conducive to the decentralization of bitcoin.

6 Conclusion

Since its birth, Bitcoin has been attracting people's attention. Blockchain technology has also changed people's lifestyle in various fields. However, the security problems of the bitcoin system are not to be underestimated. This paper makes a systematic introduction to the working principle of Bitcoin, the security problems faced by the bitcoin system and the countermeasures to deal with various security problems, and discusses other challenges that Bitcoin may face. The Bitcoin system is faced with the possibility of various attacks in the aspects of consensus mechanism security, protocol security and mine pool security. Although we have proposed some methods to avoid attacks, there is still no guarantee that there will not be new attacks. We hope people will pay more attention to the security of Bitcoin.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008. [Online]. Available: http://bitcoin.org/bitcoin.pdf.

[2] A. D. Liu, X. H. Du, N. Wang and S. Z. Li, "Research progress of blockchain technology and its application in information security," *Journal of Software,* vol. 29, no. 7, pp. 2092–2115, 2018.

[3] S. Gilbert, N. A. Lynch, "Brewer's conjecture and the feasibility of consistent," *ACMSIGACT News*, vol. 33, no. 2, pp. 51–59, 2002.

[4] A. Back, *Hashcash-A Denial of Service Counter-Measure*, 2002. [Online]. Available: ftp://sunsite.icm.edu.pl/site/replay.old/programs/hashcash/hashcash.pdf.

[5] G. Andresen, *Bip 16: Pay to Script Hash*, 2012. [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0016.mediawik.

[6] E. K. Lua, J. Crowcroft, M. Pias, R. Sharma and S. Lim, "A survey and comparison of peer-to-peer overlay network schemes," *IEEE Communications Surveys Tuts*, vol. 7, no. 2, pp. 72–93, 2005.

[7] D. Eastlake, III and T. Hansen. *U.S. Secure Hash Algorithms (SHA and SHA-Based HMAC and HKDF)*, 2011. [Online]. Available: http://www.ietf.org/rfc/rfc6234.txt.

[8] R. C. Merkle, "A digital signature based on a conventional encryption function." in *Conf. on the Theory and Application of Cryptographic Techniques*, pp. 369–378, 1987.

[9] Eyal and E. G. Sirer. "Majority is not enough: Bitcoin mining is vulnerable," *Financial Cryptography*, pp. 436–454, 2014.

[10] A. Sapirshtein, Y. Sompolinsky and A. Zohar, "Optimal selfish mining strategies in bitcoin," *Int. Conf. on Financial Cryptography and Data Security*, Springer, pp. 515–532, 2016.

[11] M. Rosenfeld, "Analysis of Bitcoin pooled mining reward systems," arXiv preprint arXiv:1112.4980. 2011.

[12] M. Rosenfeld, "Mining pools reward methods," *Presentation at the Bitcoin Conf.* 2013. [Online]. Available: https: //epicen-ter.tv/episode/049/.

[13] A. Laszka, B. Johnson and J. Grossklags, "When bitcoin mining pools run dry," *Int. Conf. on Financial Cryptography and Data Security,* Heidelberg, Berlin: Springer, pp. 63–77, 2015.

[14] O. Schrijvers, J. Bonneau, D. Boneh and T. Roughgarden, "Incentive compatibility of Bitcoin mining pool reward functions," in *Proc. 20th Int. Conf. Financial Cryptography and Data Security*, pp. 477–498, 2016.

[15] Pool Distribution, 2020. [Online]. Available: https://btc.com/stats/pool.

[16] K. Nayak, S. Kumar, A. Miller and E. Shi, "Stubborn mining: Generalizing selfish mining and combining with an eclipse attack," *IEEE European Symp. on Security & Privacy*. IEEE, pp. 305–320, 2016.

[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," *2015 IEEE 28th Computer Security Foundations Symp.,* Verona, pp. 397–411, 2015.

[18] I. Eyal, "The Miner's Dilemma," *2015 IEEE Symp. on Security and Privacy*, San Jose, CA, pp. 89–103, 2015.

[19] Y. Kwon, D. Kim, Y. Son, E. Vasserman and Y. Kim, "Be selfish and avoid dilemmas: Fork after withholding (faw) attacks on bitcoin," in *Proc. of the 2017 ACM SIGSAC Conf. on Computer and Communications Security*, pp. 195–209, 2017.

[20] S. Haber and W. S. Stornetta, "How to time-stamp a digital document," in *Conf. on the Theory and Application of Cryptography*, vol. 3, no. 2, pp. 99–111, 1991.

[21] D. Malkhi, "Byzantine quorum systems," *Distributed Computing*, vol. 4, no. 4, pp. 203–213, 2012.

[22] J. R. Douceur, "The sybil attack," in *Int. Workshop on Peer-to-Peer Systems*. Heidelberg, Berlin: Springer, pp. 251–260, 2002.

[23] E. Heilman, A. Kendler, A. Zohar and S. Goldberg, "Eclipse attacks on bitcoin's peer-to-peer network," in *24th {USENIX} Security Symposium ({USENIX} Security 15)*, pp. 129–144, 2015.

[24] M. Apostolaki, A. Zohar and L. Vanbever, "Hijacking bitcoin: Routing attacks on cryptocurrencies," *2017 IEEE Sym. on Security and Privacy (SP)*, IEEE, pp. 375–392, 2017.

[25] M. Tran, I. Choi, G. J. Moon, A. V. Vu and M. S. Kang, "A stealthier partitioning attack against bitcoin peer-to-peer network," in *IEEE Sym. on Security and Privacy (S&P)*, 2020.

[26] J. Bonneau, "Why buy when you can rent?" *Financial Cryptography and Data Security*, pp. 19–26, 2016.

[27] B. Johnson, A. Laszka, J. Grossklags, M. Vasek, and T. Moore, "Game-theoretic analysis of DDoS attacks against Bitcoin mining pools," in *Int. Conf. on Financial Cryptography and Data Security*, pp. 72–86, 2014.

[28] M. Tran, I. Choi, G. J. Moon, A. V. Vu and M. S. Kang, "A stealthier partitioning attack against bitcoin peer-to-peer network," *2020 IEEE Sym. on Security and Privacy (SP)*, IEEE, pp. 894–909, 2020.

[29] M. C. K. Khalilov and A. Levi, "A survey on anonymity and privacy in bitcoin-like digital cash systems," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2543–2585, 2018.

[30] D. Ron and A. Shamir, "Quantitative analysis of the full bitcoin transaction graph," in *Int. Conf. on Financial Cryptography and Data Security*, pp. 6–24, 2013.

[31] P. Koshy, D. Koshy and P. McDaniel, "An analysis of anonymity in bitcoin using p2p network traffic," in *Int. Conf. on Financial Cryptography and Data Security*, pp. 469–485, 2014.

[32] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer and S. Capkun, "Evaluating user privacy in Bitcoin," in *Proc. 17th Int. Conf. Financial Cryptography and Data Security*, pp. 34–51, 2013.

[33] S. Goldfeder, R. Gennaro, H. Kalodner, J. Bonneau, J. A. Kroll *et al., Securing Bitcoin Wallets Via A New DSA-ECDSA Threshold Signature Scheme*, 2016. [Online]. Available: https://www.cs.princeton.edu/steve-nag/threshold sigs.pdf.

[34] J. W. Bos, J. A. Halderman, N. Heninger, J. Moore, M. Naehrig *et al.,* "Elliptic curve cryptography in practice. " in *Int. Conf. on Financial Cryptography and Data Security*, pp. 157–175, 2014.

[35] G. Ateniese, A. Faonio, B. Magri and de B. Medeiros, "Certified bitcoins," in *Int. Conf. on Applied Cryptography and Network Security*, pp. 80–96, 2014.

[36] A. Biryukov and I. Pustogarov, "Bitcoin over Tor isn't a good idea," in *2015 IEEE Sym. on Security and Privacy*. IEEE, pp. 122–134, 2015.

[37] E. Heilman, "One weird trick to stop selfish miners: fresh Bitcoins, A solution for the honest miner (poster abstract)." in *Int. Conf. on Financial Cryptography and Data Security*, pp. 161–162, 2014.

[38] R. Zhang and B. Preneel, "Broadcasting intermediate blocks as a defense mechanism against selfish-mine in Bitcoin," vol. 2015, pp. 518, 2015.

[39] M. Rosenfeld, "Analysis of Bitcoin pooled mining reward systems," arXiv preprint arXiv:1112.4980, 2011.

[40] S. Bag and K. Sakurai, "Yet another note on block withholding attack on bitcoin mining pools," in *Int. Conf. on Information Security.* Cham: Springer, pp. 167–180, 2016.

[41] G. O. Karame, E. Androulaki and S. Capkun, "Double-spending fast payments in bitcoin," in *Proc. of the 2012 ACM Conf. on Computer and Communications Security*, pp. 906–917, 2012.

[42] T. Ruffing, A. Kate and Schrouml, "Liar, liar, coins on fire! Penalizing equivocation by loss of bitcoins," in *Proc. of the 22nd ACM SIGSAC Conf. on Computer and Communications Security (CCS'15)*, pp. 219–230, 2015.

[43] P. Camelo and J. Moura, "CONDENSER: A graph-based approach for detecting botnets," arXiv preprint arXiv:1410.8747, 2014.

[44] I. Bentov, C. Lee, A. Mizrahi and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake," *ACM SIGMETRICS Performance Evaluation Review*, vol. 42, no. 3, pp. 34–37, 2014.

[45] Y. Sompolinsky and A. Zohar, "Secure high-rate transaction processing in bitcoin," in *Int. Conf. on Financial Cryptography and Data Security*, pp. 507–527, 2015.