applied sciences

MDPI

Article

Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack

Sarwar Sayeed and Hector Marco-Gisbert *

University of the West of Scotland, High Street, Paisley PA1 2BE, UK; sarwar.sayeed@uws.ac.uk

* Correspondence: hector.marco@uws.ac.uk; Tel.:+44-141-849-4418

Received: 1 April 2019; Accepted: 26 April 2019; Published: 29 April 2019

Abstract: The 51% attack is a technique which intends to fork a blockchain in order to conduct double-spending. Adversaries controlling more than half of the total hashing power of a network can perform this attack. In a similar way, *n* confirmation and selfish mining are two attack techniques that comprise a similar strategy to the 51% attack. Due to the immense attacking cost to perform the 51% attack, it was considered very unlikely for a long period. However, in recent times, the attack has befallen at a frequent pace, costing millions of dollars to various cryptocurrencies. The 51% attack strategy varies based upon the adopted consensus mechanism by a particular cryptocurrency, and it enables attackers to double-spend the same crypto-coin, restrict transactions, cancel blocks, and even have full control over the price of a cryptocurrency. A crypto-coin with a low hashing power is always jeopardized by the 51% attack due to the easily attainable hashing. In this paper, we analyze the real impact of the 51% attack, revealing serious weaknesses in consensus protocols that made this attack possible. We discuss the five most advanced protection techniques to prevent this attack and their main limitations. We conclude that in most cases, security techniques fail to provide real protection against the 51% attack because the weaknesses are inherited from the consensus protocols.

Keywords: 51% attack; double-spending; security techniques; consensus mechanism

1. Introduction

Blockchain is an emerging technology that allows performing digital transactions within a short period [1]. It is a secure medium which works by sharing information over the peer-to-peer (P2P) network. A piece of shared information to a single entity reaches all participants within the network, without the data being tampered. In addition to crypto-transactions, it is also leveraged for various other purposes, such as insuring intellectual property, generating financial contracts, tracing food production, and tracking supply chains [2]. The rise of this technology has been obstructed from time to time by various pernicious attacks. Attacks such as the Sybil attack, Eclipse attack, border gateway protocol (BGP) hijacking, and 51% attack originated from an attempt to strike the blockchain network. Amongst these, the 51% attack has been neglected by security researchers mainly due to the immense attacking cost. However, recent attacks have proven that the 51% attacks can be performed on various modern cryptocurrencies. The proof-of-work (PoW) consensus protocol is an immediate threat of the 51% attack compared to other consensus protocols. Recent attacks were mainly targeting crypto-coins that rely on PoW.

Bitcoin is the first cryptocurrency which was implemented in the blockchain network [3]. It is based on the PoW consensus protocol, and several cryptocurrencies inherited the consensus rules. After Bitcoin appeared, new cryptocurrencies evolved to take advantage of the blockchain network. The more this technology was adapted, the more it drew the attention of potential attackers.

The low hashing coins are more prone to this attack technique due to the gigantic costs on high hashing coins. As a result, the recent attacks were mostly targeting low hashing coins, such as Bitcoin

Gold (BTG), Verge (XVG) and Ethereum Classic (ETC). The dangerous part of a 51% attack is that there is no way to detect it until it is fully executed; hence, when an adversary is in possession of the required hashing power, the chances of success can be close to 100%.

In summary, the major contributions in this paper are:

- We discuss seven major security threats that jeopardize the blockchain network;
- We reveal the limitations of the consensus mechanisms by classifying them in several attacks;
- We define the majority hash rate problem and point out the consequences of the attack techniques;
- We analyze five security protection mechanisms specific to the 51% attack and demonstrate their limitations against the 51% attack exploitation.

This paper is organized as follows. Section 2 is the background section, which defines the concept behind blockchain technology. Section 3 illustrates seven attacks which can affect the blockchain network significantly. Section 4 discusses the three widely adopted consensus protocols and their limitations. This section also classifies the consensus based on various attacks. Section 5 discusses the majority hash rate problem in depth and points out the major consequences of this attack. In Section 6, we present the defense mechanisms to mitigate the 51% attack. Section 7 involves our analysis of the defense mechanisms to determine their robustness against the 51% attack. Finally, we conclude the paper in Section 8, pointing out the main weaknesses which suggest new modifications to the existing consensus protocols.

2. Background

To understand the significant contributions of this paper, it is necessary to elaborate on the consensus mechanism and blockchain technology in depth. This section enhances the quality of experience (QoE) of the blockchain network as well as discusses the mining and hashing context.

2.1. Blockchain Technology: The Digital Concept

Blockchain technology consists of records of data which are referred to as a ledger. It employs a distributed system for the verification of records. Blocks are verified by thousands of network participants around the globe to keep the network active. Here we discuss the full concept behind blockchain technology.

2.1.1. Consensus Mechanism

A consensus mechanism is a protocol which is in place to ensure that all the participants in the blockchain network are complying with the agreed rules [4]. It ensures that the transactions emerge from a legitimate source by having every participant consent to the state of the distributed ledger. The public blockchain is a decentralized technology, and no centralized authority is in place to regulate the required act. Therefore, the network requires authorizations from the network participants for the verification and authentication of any activities that occur in the blockchain network. The whole process is done based on the consensus of the network participants, and it makes the blockchain a trustless, secure, and reliable technology for digital transactions. Distinct consensus mechanisms follow different principles, which enables the network participants to comply with those rules. Several consensus mechanisms have been introduced considering the requirements of secure digital transactions. However, proof of work (PoW), proof of stake (PoS), and delegated proof of stake (DPoS) are the few consensus protocols used by the main cryptocurrencies.

2.1.2. Blockchain Functionality

Blockchain is a digital technology which stores digital information [5] in blocks. Each block is chained to the blocks adjacent to it, called a blockchain. Any information inside the blocks can never be changed due to the immutable feature. Altering a single piece of information of a block invalidates every block after the one that was altered. The block information is available publicly, and one can easily track almost all key information, such as client records, property contracts, and payment information. Every block comprises a digital signature which correlates with the strings in that particular block. The whole process occurs through a hashing procedure, and a change to a single digit of the block string produces an entirely new digital signature. The blockchain blocks are available for verification by anyone who is part of the network. As a result, any malicious alterations can be immediately detected by the network participants. Regardless of the failure of any part of the network, the blockchain network still keeps running as normal. A block in the bitcoin blockchain typically has a size of 1 MB, and it can contain many transactions as long as it is within the size limit.

Figure 1 presents a full layout of a bitcoin blockchain block. The block header size is 80 bytes, which includes the version, previous hash, Merkle hash, timestamp, difficulty level, and the nonce. All the information is then hashed to include the inside of the next block header.

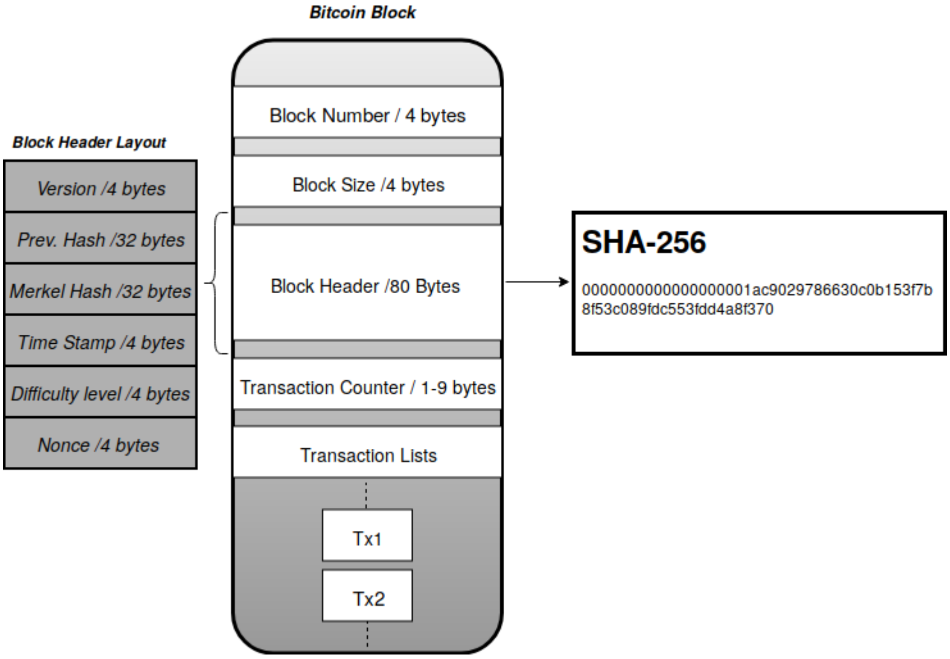


Figure 1. The layout of a bitcoin block. The block number contains a 4-byte arbitrary number confirming it as a bitcoin block, and the block size ensures the size of the block. A block header layout shows its contents. The block header is hashed using SHA-256 and the hash value to be added to the "previous hash" section of the next block header. The transaction counter counts the total number of transactions, and the transaction list contains the list of all transactions added to the block.

2.1.3. Hashing and Digital Signatures

A digital signature is a mechanism that is used to validate the accuracy and integrity of a data string [6]. Every block comprises one unique digital signature based on the strings that the block contains. Figure 2 presents a partial view of 3 blocks that are chained to each other. Each block produces a digital signature which is generated considering the contents, such as Merkle hash and the digital signature of previous blocks. A digital signature does not always qualify to validate the next block, as the bitcoin blockchain sets a level of difficulty to determine the block creation time. Hence, having fewer transactions in a block does not necessarily help to create a block faster than the other nodes. If the difficulty level requires having 17 zeros in front of the digital signature, then the miners require meeting that condition to validate a block. An attacker making modifications to the data string changes the digital signature and will fail to meet the requirement for the next blocks that are chained to it [7]. To overcome the scenario, a new signature must be generated for every subsequent block on the chain. The process becomes very costly and nearly impossible, as the attacker is required to generate new signatures not only for the blocks which have been corrupted but also any blocks that are being added on a regular interval.

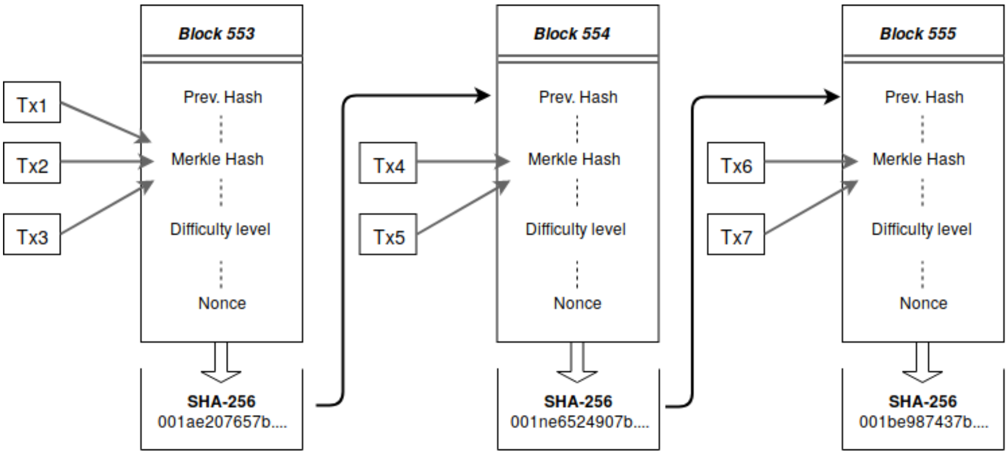


Figure 2. A partial layout of bitcoin blocks, where each block is chained to each other. Tx1, TX2, and TX3 are hashed through the Merkle tree process. The Merkle hash adds a nonce value sequentially to generate a new Hash and then compare it to the difficulty level. The entire data string produces a hash value, which is then added to the next block by forming a chain of blocks.

2.1.4. Blockchain Mining

Blockchain mining is a process which involves computing a new block to be added to the distributed ledger [8]. The mining is mainly correlated to bitcoin, as the block generation process differs on distinct cryptocurrencies. Mining computers are often powerful machines that are used in generating the correct hash values. Nodes that are involved with mining are required to solve a mathematical puzzle utilizing their machines to mine. As soon as a miner successfully produces a new block, the miner notifies the network about it. Every miner in the network stops mining that block and again restarts solving equations for the next block. In the mining process, a miner takes the hash Merkle root and adds it to the nonce value. A new hash is generated from the alteration of the nonce and then compared with the target each time. If the hash value is less than the target, the mathematical puzzle is solved. However, while the hash value is higher than the target, the nonce value needs to be changed and matched with the target value until the conditions are met. A mining pool involves hundreds of thousands of mining machines. Therefore, a pool usually comprises more hashing power than other miners and has the advantage to find the required hash faster than other miners [9]. The mining time of bitcoin is about 10 min, requiring extensive hardware for the process. Currently, miners receive a mining reward of 12.5 BTC for every successful block they generate and also the fees associated with each transaction. The reward reduces to half about every four years.

In this section, we presented the full overview of the blockchain technology. This technology is at a high risk and has been exploited by various attacks in recent time. Therefore, in the next section, we present various security threats to reveal their attacking strategies on the blockchain network.

3. Security Threats

In this section, we discuss the seven main security threats to blockchain technology. When those attacks are successfully executed, they result in the loss of large amounts of money or cause a denial of service to some blockchain nodes.

3.1. 51% Attack

The 51% attack is a technique that occurs when an attacker is in possession of 51% of the hashing power. This attack starts by creating a chain of blocks privately, which is fully isolated from the real version of the chain. At a later stage, the isolated chain is presented to the network to be established as a genuine chain. This is what enables the double-spending attack [10]. Since the blockchain policy complies with the longest chain rule [11], if attackers are able to get 51% of the hashing power or more, they will be in a position to drive the longest chain by persuading the network nodes to follow their chain. However, it is not strictly necessary to obtain 51% of the hashing power; if attackers get less than half of the hashing power [12], the double-spending attack is still possible but with less probability of success. The more hashing power the entire blockchain network comprises, the more costly the attack becomes. Thus, cryptocurrencies with high network hashing are assumed to be more secure against the 51% attack.

3.2. Long-Range Attack

A Long-range attack is a technique that appears due to the weak subjectivity model [13]. This attack technique comprises a similar approach to the 51% attack. However, instead of beating the 6 block confirmation, it tends to fork the chain from the genesis block [14]. The likelihood of this attack is nearly non-existent in bitcoin, but it can be destructive to proof of stake (PoS) and delegated proof of stake (DPoS) consensus. Considering a scenario at PoS consensus, where some attackers start with a limited number of coins soon after the Genesis block, they can privately mine their version of chain to conduct the attack. Though considering their limited stake, they are allowed to produce limited blocks at the beginning, through the process, they will be permitted to generate a longer chain. Since PoS does not define a limit on the augmentation of the chain, the chain can extend very long.

3.3. Distributed Denial-of-Service (DDoS)

Distributed denial-of-service (DDoS) is a type of cyber attack which is used to make resources unavailable to network participants by flooding with extreme traffic [15] in a distributed way. This attack has been carried out in the past two decades to cause damage to various networks [16]. Research indicates that the impact of DDoS is rising and costs more than $2 Million to enterprises on average on each attack [17]. DDoS is one of the most common attacks in the blockchain network used by attackers to obstruct authentic transactions so that invalid transactions can be executed. However, due to the decentralized nature of blockchain, DDoS can mitigate network activity only to a certain level.

3.4. P+ Epsilon Attack

The P + epsilon attack is a technique which leverages the dominant strategy of network participants. PoW-based blockchain is usually vulnerable to this type of attack [18]. In a scenario where attackers offer a payout to participants in order to gain an advantage, a payoff matrix is applied where the dominant strategy assists in order to succeed with the attacking goal. After the attack, nothing is paid to the participants, and the attacker gains all the profit. It is a simple statistical observation based on the uncoordinated choice model.

3.5. Sybil Attack

The Sybil attack aims to corrupt a P2P network by forming several fake identities [19]. The attack method was first brought to the world's attention by John Douceur [20], a researcher based at Microsoft. The attackers can establish several fake nodes that appear to be genuine to their peers. These fake nodes take part in corrupting the network to validate unauthorized transactions and to alter valid transactions. They can use several devices, virtual machines or internet protocol (IP) addresses as fake nodes for the attack. The P2P network assumes that each participating node comprises only one identity. Therefore, several fake nodes give attackers the capability to deny transmitted blocks [21] and to outvote honest nodes. When an adversary owns a large number of network nodes, it enhances the chances of double-spending. However, there is a large number of nodes in the bitcoin blockchain network resulting in a very expensive attack.

3.6. The Balance Attack

The balance attack is a technique which targets the nodes that comprise balanced mining power [22]. This attack can be executed to double-spend on PoW consensus. An attacker can utilize their limited hashing power to delay messages over the Ethereum blockchain. Only 5% of the total hashing power can be enough to carry out this attack. A delay is first introduced between the licit subgroups of nodes. The attacker then mines a vast amount of blocks to another subgroup, ensuring that the other subtree puts importance on the transaction subgroups. The ghost protocol is exploited by separating the blockchain branch from the other nodes in the network. Subsequently, the separated branch is produced to other nodes to have an impact over the branch selection process.

3.7. Border Gateway Protocol Hijacking (BGP)

Border gateway protocol (BGP) hijacking, also known as a routing attack, is a technique where the internet service provider (ISP) makes false announcements over the routing system to divert traffic [23]. There are two attack scenarios that can be leveraged by an attacker. The first one is to partition the bitcoin network to hijack IP prefixes, and the second one consists of obstructing the block propagation by 20 min. The possible consequence of this attack is the ability to perform the double-spending attack. Moreover, the exchanges and pools can also be prevented from conducting regular transactions. BGP attacks are being carried out at a large scale over the Bitcoin network, and at least 100 BGP exploitation occurs on a monthly basis [24]. Though the blockchain system is a decentralized network, from a routing perspective, it can be regarded as centralized as about 100 IP prefixes are managing about 20% of the bitcoin hosts.

The presented attack vectors can cause a severe effect over the blockchain network. An important limitation has been found in the consensus mechanisms. Therefore, it is essential to analyze them in order to reveal the weaknesses that can result in attacks targeting digital transactions.

4. Consensus Mechanism Weaknesses

In this section, we discuss three widely adopted consensus mechanisms and their weaknesses. Table 1 shows the main features of the consensus mechanisms and Table 2 categorizes each consensus towards the attacks discussed in Section 2. Our analysis indicates that the consensus mechanisms comprise severe limitations, resulting in a low quality of experience (QoE) of the network participants [25]. The analysis is constructed assessing various security experiments and reviewing attack methods based on particular consensus mechanisms.

Table 1. Main features of consensus mechanisms.

Consensus	Energy Cost	Decentralization	Processing Speed
PoW	High	High	Low
PoS	Low	High	High
DPoS	Low	Low	High

Table 2. Consensus mechanisms that are vulnerable to various attacks.

Consensus Mechanisms	51% Attack	Long Range Attack	DDoS Attack	P+Epsilon Attack	Sybil Attack	Balance Attack	BGP Hijacking
PoW	✓	✗	✓	✓	✓	✓	✓
PoS	✓	✓	✓	✗	✓	✗	✗
DPoS	✓	✓	✓	✓	✓	✓	✗

4.1. Proof of Work (PoW)

Proof of work (PoW) is a consensus mechanism that is based on solving a mathematical equation. PoW was first initiated by bitcoin, and then it was rapidly implemented by many major cryptocurrencies [26]. Miners are the main pillar of PoW consensus, and the process of authorizing and recording the transaction is approved by the miners. PoW consensus requires the miners to put a considerable amount of effort to mine a block. The process involves a random method of attempting answers on a trial and error basis. Hence, it may take one or even thousands of attempts to solve the equation. In order for the "target hash" to be recognized, it must contain a lower number than the hash of the block [27].

PoW consensus assumes that half of the network nodes are always honest miners; hence, obtaining more than half the hashing power makes this consensus vulnerable. One of the significant drawbacks of PoW is the cost of energy and hardware requirement. Research has shown that the amount of electricity consumption of the bitcoin mining process is a lot more than 159 countries [28]. However, the mining requirement and mining time may vary due to the algorithms used by individual cryptocurrencies.

The mining process of PoW is comparatively slow compared to that of other consensus protocols. Since a few mining pools dominate with a large amount of mining power, attacks to those pools can cause severe disruptions to the bitcoin network. Recent attacks proved that PoW is vulnerable to the 51% attack. Low hashing crypto-coins utilizing PoW consensus are more vulnerable to 51% attack, as the required hash can be acquired easily. Thr P + epsilon attack can be executed at no cost while in possession of the required budget [29].

In our analysis, we indicate that the Sybil attack can successfully exploit the PoW by forming a large number of malicious nodes. The Ethereum protocol and private blockchains are vulnerable to the balance attack [22,30]. Moreover, the DDoS attack and BGP hijacking can also be used to interrupt the regular stream of this consensus mechanism [23]. AntPool, BW.com, NiceHash, CKPool, and GHash.io are a few mining pools which have already been hit by DDoS attacks [31].

4.2. Proof of Stake (PoS)

Proof of stake (PoS) is a consensus mechanism which authorizes blocks based on the stakes a participant pours into the network. Miners in possession of a large number of coins possess more power than other participants [32]. Peercoin was the first cryptocurrency to use this consensus in 2012. A randomized process is followed to consider the creator of the next block. The process involves obtaining the detail about the total amount of the cryptocurrency, and also the duration for which it has been maintained. The advantage of PoS consensus is that it does not require participants to go through an expensive mining process such as PoW.

PoS is vulnerable due to its centralized attributes [33]. While staking a large portion of wealth consistently, a participant becomes a powerful entity within the network and also able to influence the well-being of the network. By achieving the majority of the supply, a malicious stakeholder can take advantage of the nothing-at-stake problem. PoS suffers from weak subjectivity, and the implementation process is also very complex and challenging [34]. To conduct a 51% attack, an adversary is required to achieve the 51% of the distinct cryptocurrency. However, the cost of achieving 51% of the total stake can be immense. Therefore, the threat level of the 51% attack can be low compared to PoW. Our study reveals that PoS can be exploited by the long-range attack [13]. The P + epsilon attack cannot be executed since an attacker needs to achieve a large budget to contribute as a security deposit for the participants while voting for the minority [29]. PoS can be exploited by a Sybil attack, and a DDoS attack can also disrupt part of the network.

4.3. Delegated Proof of Stake (DPoS)

Delegated proof of stake (DPoS) is a consensus mechanism that permits shareholders to vote for witnesses [35]. The main idea of DPoS is to reduce the wastage of energy and enhance the speed of transactions. The overall block generation process makes this consensus mechanism many times faster than the PoW consensus. DPoS comprises a one vote per share policy, which gives the stakeholders the option to cast more votes while they possess more coins. The witnesses are rewarded for generating blocks, but they are also penalized when they fail to perform the required task, resulting in them being unpaid and voted out. Witnesses must acquire the largest number of votes from random stakeholders in order to perform the instructed task. The stakeholders also vote for the delegates to reform and make changes in the network, which are reviewed for an ultimate decision.

DPoS was developed to bring up efficiency in transactions and overcome the limitations introduced by various other consensus mechanisms; however, it includes severe flaws. It fails to achieve adequate decentralization, and the network slows down due to the vast number of validators. Due to the centralized aspects, it can be a focal point of random attackers. DPoS is vulnerable to the 51% attack. The attacker can convince the stakeholders to obtain 51% voting power to execute a 51% attack [36]. This consensus mechanism is also vulnerable to other primary attacks, such as a long-range attack, DDoS attack, P + epsilon attack, Sybil attack, and the balance attack.

In the presented study, we pointed out that the three major consensus algorithms have significant limitations and are vulnerable to various attacks. The weakness in the consensus makes the digital transactions at a high risk of potential attacks. Table 2 presents our evaluation summary. It is worth noting that all three consensus mechanisms can be exploited by the 51% attack, making this attack very attractive for attackers, especially for the PoW, where obtaining the necessary hashing power is less costly.

5. The Majority Hash Rate Problem

An attacker in possession of a great amount of hashing power can cause a serious impact over a blockchain network. The 51% attack occurs due to the majority hash and can be devastating in the blockchain network [37]. It is very important to reveal the nature and possible sequel to the exploitation. This section involves discussing majority hash attacks and also presents the consequences by illustrating the double-spending issue and risks of mining centralization. Figure 3 presents eight major cryptocurrencies which have been affected from the 51% attack [38], and Figure 4 demonstrates the stages of a 51% attack technique by forking the blockchain.

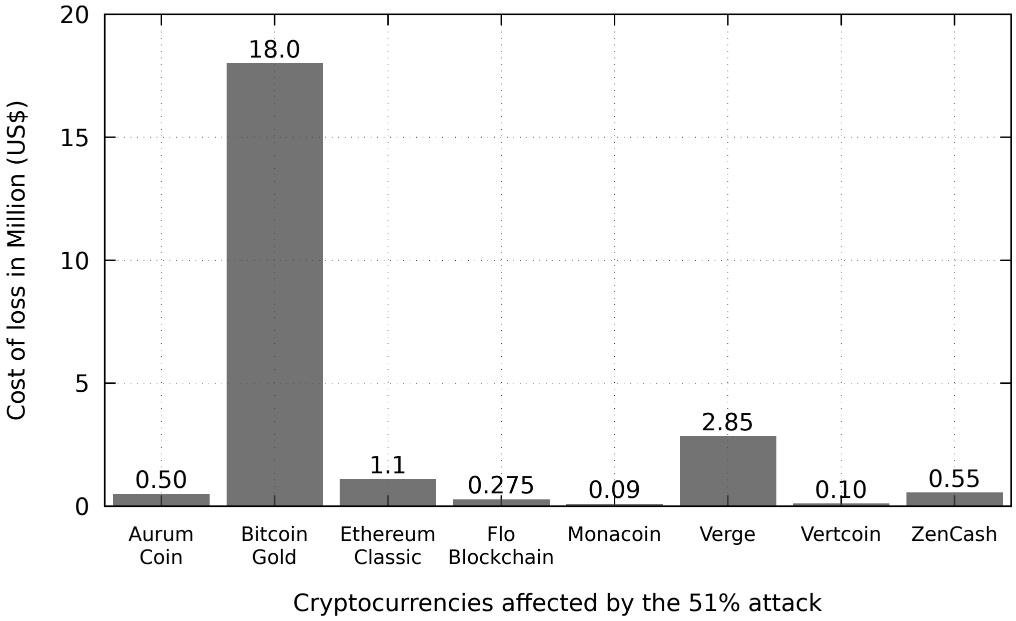


Figure 3. Loss from 51% attack on eight cryptocurrencies that have most recently been exploited.

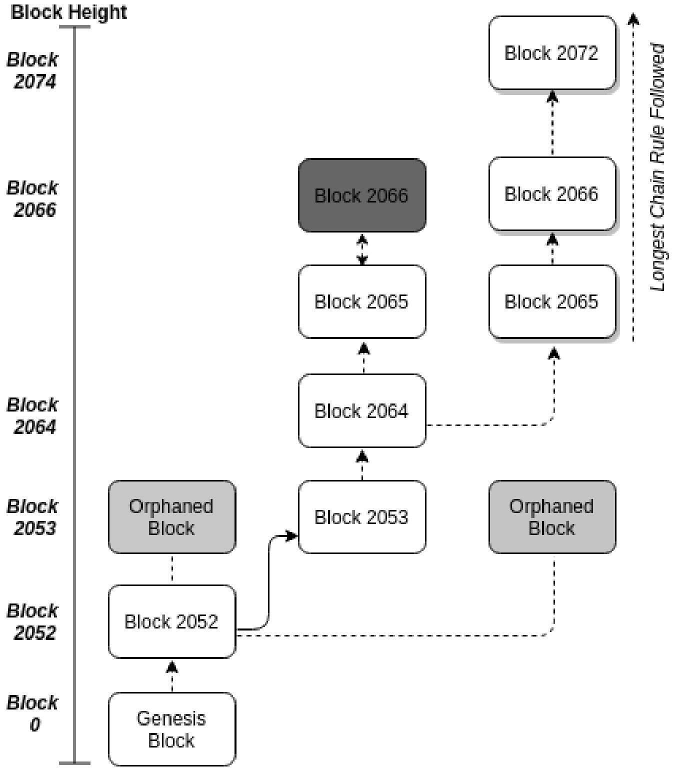


Figure 4. A scenario where three blocks are generated at the same block height 2053. Tow blocks became orphaned as the network chose to follow the block in the middle. Blocks 2065 to 2074 are privately mined blocks, which resulted in canceling transactions on the legit Block 2066. The network follows blocks from 2065 to 2074, broadcasted by the attacker, due to the longest chain.

5.1. The Majority Hash Attacks

The majority hash attacks have been a serious problem in recent times. A miner possessing a large amount of hashing power can influence the network to perform malicious activities. The 51% attack, selfish mining, and 34% attack can occur when an attacker achieves a large amount of hashing power.

The 51% attack requires an attacker to hold more than half of the hashing power [39]. A 51% attack against cryptocurrencies enables attackers to perform malicious actions, including double-spending, controlling market price or ruling over the mining strategy. We have selected the main eight crypto-coins that have been exploited most recently. Figure 3 presents the amount of losses encountered due to the 51% exploitation from April 2018 to January 2019. Verge (XVG) has been attacked twice in consecutive months losing $1.1 million and $1.75 million, followed by bitcoin gold (BTG), which is the most affected coin, losing around $18 Million. The rest of the coins also lost a significant amount from exploitation. The total loss makes an average amount of $2.5 Million per attack on individual currencies.

Selfish mining is another majority hash attack which is accomplished with approximately 25% of the total network hashing [40,41]. It can be carried out by miners or mining pools which comprise a large amount of network hash. In this attack technique, the miners become very selective in broadcasting their blocks to the network. They can decide either to discard their blocks by giving up their reward or to broadcast several blocks at once. This will cancel other miners' blocks, making them losie their reward as well as the transaction fees. During the process, independent nodes intend to join the attacker to increase their profits, and attackers gain more control over the network by having more hashing power.

Another attack is the 34% attack. This attack occurs due to a majority of network hashing. IOTA is a cryptocurrency developed for the Internet of Things. The IOTA is not based on blockchain and comprises unique storage known as Tangle [42]. Tangle is also a distributed ledger performing similar operations as the blockchain. IOTA comprises a centralized feature and us also vulnerable to 34% attack [43].

5.2. The Double-Spending Issue

Double-spending is a technique that is initiated to respend the same currency [44]. A weakness in the consensus mechanism uplifts the likelihood of a majority hash rate attack, and successful exploitation leads to double-spending by allowing attackers to cancel transactions and spend the same coin again. In order to carry out double-spending, attackers first spend their coins in the legit chain. After that, they start building another chain privately where the attackers' coins are not spent. Once the privately mined chain is long, the attackers present the new chain to the network. Since the chain is longer than the one being used, the new chain will be used by the network as a legit chain discarding the blocks where attackers spend their coins.

The probability of double-spending on PoW consensus varies depending upon the number of blocks an adversary is able to generate [12]. However, the more confirmations introduced, the less the chance of double-spending. If an attacker is in possession of a 10% hash rate, then double-spending is still possible but with a smaller possibility of success. Various exchanges grant a transaction approval after six confirmations to mitigate the double-spending issue; nevertheless, attackers with 51% hashing power can keep building blocks secretly at a faster pace and carry out double-spend regardless of the number of confirmations set by the exchanges.

5.3. Mining Centralization

Mining centralization is a significant issue in the PoW mining pools due to the dominance of the hashing power. Mining pools with powerful systems can compute more hashes, having a better chance of solving problems than others. Individual pools may involve hundreds or thousands of participants in the mining process being in possession of a large amount of the total network hashing power. Pools with immense hashing power can collaborate to make the network vulnerable. The seven major bitcoin mining pools, out of the top 10, are based on China. Hence, the dominating attributes by a few mining pools have structured the blockchain as a centralized network. Several mining pools were also attacked by DDoS attacks in the past, obstructing their mining activities and demanding a payment to discontinue the attack [31].

In July 2014, GHash.io reached more than 50% hashing power, becoming a great threat to Bitcoin and the exchanges [45]. They were in charge of the majority hashing for nearly 24 h. However, after breaching the threshold, various participants related to the pool halted their mining power for the sake of the security of the network. The main cause of reaching the majority of hashing was the combined hashing. However, at a later time, GHash.io announced not having accumulated 51% hashing. They agreed to stop accepting distinct mining resources and to implement a feature for participants to mine from various other pools. The pool stopped its mining operation since 2016.

Figure 5 defines the number of blocks created on 10 March 2019 by only six mining pools in a 24 h period [46]. A total number of 137 bitcoin blocks were generated, where 92 blocks were produced by the six mining pools, making it about 67% of the total blocks during that period. The block counts refer to the total number of blocks generated by a particular mining pool, and continuous block refers to the number of times a pool was able to generate blocks in a sequence. We present that F2Pool was able to generate 2 or more blocks on three occasions, whereas BTC.com also produced blocks in sequence 2 times. Antpool and ViaBTC generated blocks in sequence once. BTC.TOP and SlushPool could not generate a longer chain of blocks.

In recent times, the majority hash rate problem has been a serious issue to cryptocurrencies. The low hashing coins constitute higher threats of 51% exploitation. Attackers are focused on coins where the attack cost is minimal to maximize profit. Only a few mitigation techniques have been introduced in recent times to defend against a 51% attack. In the next section, we discuss those protection techniques to assess their effectiveness later.

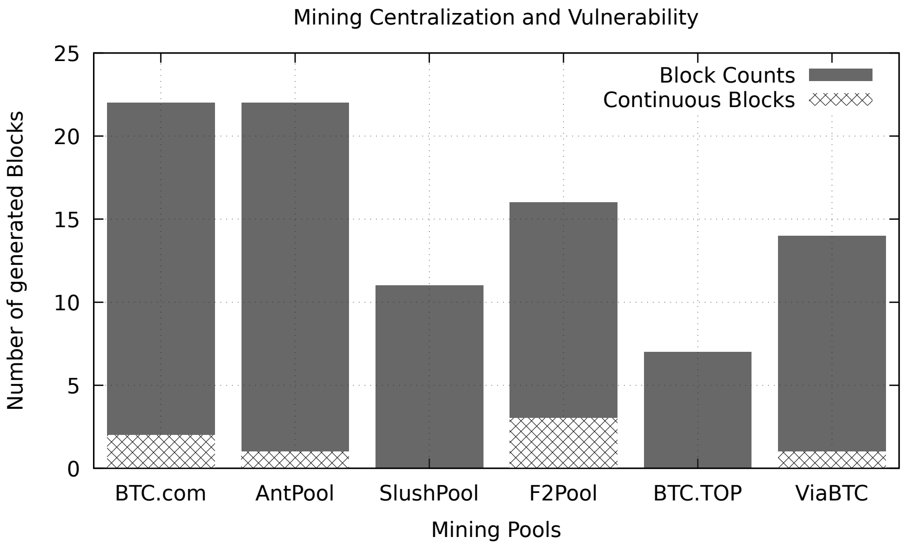


Figure 5. Total number of continuous blocks ≥ 2.

6. 51% Attack Mitigation Techniques

In this section, we discuss the five most recent defense techniques which are based on mitigating the 51% attack. We particularly chose these techniques as they are the most advanced and recent techniques introduced after the recent 51% exploitations.

6.1. A Penalty System for Delayed Block Submission

A penalty system for delayed block submission is a security proposal by Horizen [47]. The proposal suggests modifying Satoshi consensus to secure a network against the 51% attack. The penalty system proposes increasing the attacking cost extensively so that the potential advantage cannot be achieved towards exploitation. A penalty is applied considering the amount of time a block is hidden from the blockchain network. The time is calculated based on the interval duration between blocks. This security protection technique notifies the entire network about the continuous fork, and during that period, the participants, miners, and exchanges are restricted from performing fraudulent transactions until the delay is lifted. This defense mechanism primarily focuses on a privately mined chain and does not pay attention if the network suffers from a fork.

The penalty system follows Equation (1), a quadratic function which determines the level of penalty to be imposed. For example, assuming a genuine chain containing blocks from 553 to 558, and there is an attacker that managed to produce blocks from 553 to 559, then the penalty will be computed considering the first block height introduced by the attacker. That is, the n value in Equation (1) is calculated subtracting 553 from 558, obtaining 15 as a penalty delay.

$$DelayBlock = \frac{\sum_{i=1}^{n} n(n+1)}{2} \tag{1}$$

6.2. Delayed Proof of Work (dPoW)

Delayed proof of work (dPoW) is a security solution by Komodo. They developed dPoW to protect against the double-spending problem [48]. This security technique is already being utilized in about 20 blockchains. It is applicable to cryptocurrencies that are based on an unspent transaction output (UTXO). The dPoW consensus mechanism utilizes the assigned PoW blockchain to save the Komodo transactions [33]. Hence, to defend a 51% attack against the Komodo's blockchain, any existing copy of the Komodo chain permits the entire chain to take control of malicious activities. The prime attribute of this security chain is that it does not recognize the longest chain rule. It adds a security layer to prevent attackers from performing the 51% attack. However, it also offers to integrate notary nodes that justify whether the hash is secure for the network. The dPoW deploys 64 special nodes around the globe, and the nodes get elected every year to perform the desired task.

6.3. PirlGuard

PirlGuard is a security protocol developed to mitigate the 51% attack [49]. It modifies the consensus algorithm in order to protect against the 51% attack. The PirlGuard protocol is based on the attributes of Horizen's penalty protocol, but it is mainly built for Ethash. When an attacker starts peering with the network by confirming their privately built blocks, PirlGuard abandons the peer instantly by penalization to mine x number of blocks. The number of penalized blocks is determined by the number of blocks the adversary manages to mine in secret.

PirlGuard also introduces notary contracts, which are controlled by the master nodes. The main task of the master nodes includes notarizing the blockchain and penalizing the malicious actors by retrieving the legit consensus on the Pirl blockchain. The notary contracts are implemented on the Pirl and Ethereum blockchain.

6.4. ChainLocks

ChainLocks is a security technique developed to secure DASH. It results from the implementation of long living masternode quorums (LLMQs) to mitigate the 51% attack [50]. ChainLocks executes a network-wide vote process which comprises a "first-seen" policy. For each particular block, an LLMQ of a large number of master nodes is approved. It requires every participant to sign the noticed block so that the active chain can be extended. The majority of the participants, 60% or more, verify the distinct block and generate a P2P message (CLSIG) to notify every other node in the network about the event. The (CLSIG) message cannot be generated unless enough members comply with it. The message involves a valid signature for authenticity and verifiable by all the nodes within the network. In this security protection technique, the transaction gets confirmed after the first confirmation. Once confirmed, it cannot be reversed back as the signed block cannot be acknowledged at a later time. This security feature lifts the six confirmation aspects and enhances a secure transaction after just one confirmation. In addition to the 51% attack, ChainLocks also helps to mitigate other security issues, such as selfish mining described in Section 5.

6.5. Merged Mining

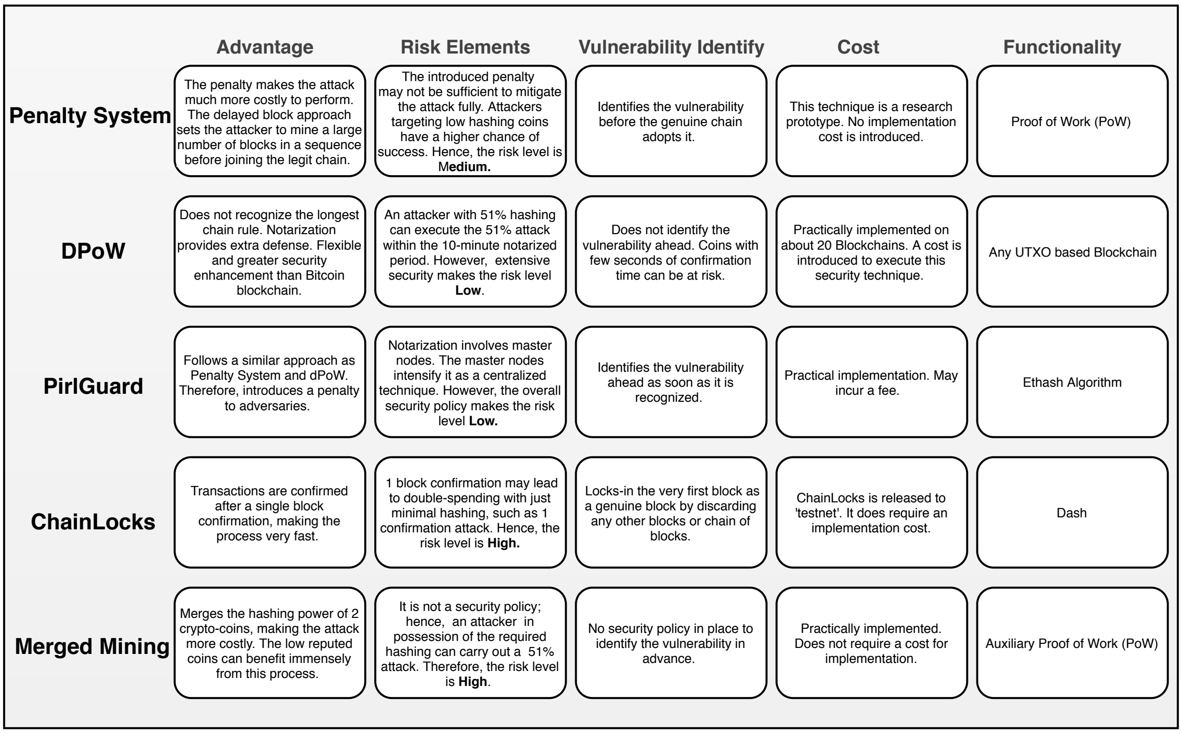
Merged mining is a technique which allows multiple cryptocurrencies to be merged to mine at the same time [51]. Low hashing cryptocurrencies that comprise the same consensus benefit from merged mining. They can increase the hashing power by bootstrapping on the other currency that comprises higher hashing power. Merged mining is not a security technique, but it is a method that, when employed, can help to mitigate the 51% attack. Transactions in both networks work in sequence, and the blockchains are classified as a parent and auxiliary blockchain. In addition to enhancing security, another benefit is the ability that miners can mine more than a block simultaneously. This technique builds up more security as the miner contributes to the entire hash rate of both currencies.

The Satoshi principle assumes that the blockchain network will always comprise a majority number of honest nodes. However, the assumption turns out to be entirely wrong, as it is observed that not only the mining pools but also the individual attackers are achieving about half of the network hashing. The destructive nature of the 51% attack exploitation drew the attention of various research groups to come up with advanced security protection techniques. Those security protection techniques were introduced to defend against the 51% attack, and in the following section, we are analyzing their effectiveness.

7. Analysis

In this section, we analyze the effectiveness of five security protection techniques against the 51% attack. Some of them are research prototype, and yet to be implemented on a real system. Figure 6 presents an evaluation framework, where we classify the risk elements of each security technique as low, medium or high. The security-based framework also presents the advantage, vulnerability, cost, and functionality of the mitigation techniques.

The penalty system for delayed block submission is a PoW-based security technique and yet to be implemented in the real network. This technique is a research prototype and includes various limitations. Based on the proposal, a block delay will be imposed over the privately mined chain. Assuming an adversary aims to beat the six confirmation times, the introduced block delay will be only 21 blocks. As a result, the attacker is forced to mine another 21 blocks in a sequence to lift the delay and get his mined blocks to be included in the normal chain. According to Rosenfeld, in any occasion, when an adversary owns 51% of the network hash, they will always succeed regardless of the enforced delay [12]. Therefore, the possibility to perform the 51% attack when this security mechanism is in place is very big, especially when targeting coins that have very low network hashing power. In addition, the delay process slows the overall transactions of the network and intensely impacts the regular transactions. Transactions that are added to the delay blocks will not be confirmed until the penalty is lifted. Thus, it may take a few hours or even a few days to confirm some transactions. Hence, this technique is not very appropriate to be implemented in a real network, it is not fully effective against 51% attack, and it has a medium level risk.



	Advantage	Risk Elements	Vulnerability Identify	Cost	Functionality
Penalty System	The penalty makes the attack much more costly to perform. The delayed block approach sets the attacker to mine a large number of blocks in a sequence before joining the legit chain.	The introduced penalty may not be sufficient to mitigate the attack fully. Attackers targeting low hashing coins have a higher chance of success. Hence, the risk level is **Medium.**	Identifies the vulnerability before the genuine chain adopts it.	This technique is a research prototype. No implementation cost is introduced.	Proof of Work (PoW)
DPoW	Does not recognize the longest chain rule. Notarization provides extra defense. Flexible and greater security enhancement than Bitcoin blockchain.	An attacker with 51% hashing can execute the 51% attack within the 10-minute notarized period. However, extensive security makes the risk level **Low**.	Does not identify the vulnerability ahead. Coins with few seconds of confirmation time can be at risk.	Practically implemented on about 20 Blockchains. A cost is introduced to execute this security technique.	Any UTXO based Blockchain
PirlGuard	Follows a similar approach as Penalty System and dPoW. Therefore, introduces a penalty to adversaries.	Notarization involves master nodes. The master nodes intensify it as a centralized technique. However, the overall security policy makes the risk level **Low.**	Identifies the vulnerability ahead as soon as it is recognized.	Practical implementation. May incur a fee.	Ethash Algorithm
ChainLocks	Transactions are confirmed after a single block confirmation, making the process very fast.	1 block confirmation may lead to double-spending with just minimal hashing, such as 1 confirmation attack. Hence, the risk level is **High.**	Locks-in the very first block as a genuine block by discarding any other blocks or chain of blocks.	ChainLocks is released to 'testnet'. It does require an implementation cost.	Dash
Merged Mining	Merges the hashing power of 2 crypto-coins, making the attack more costly. The low reputed coins can benefit immensely from this process.	It is not a security policy; hence, an attacker in possession of the required hashing can carry out a 51% attack. Therefore, the risk level is **High**.	No security policy in place to identify the vulnerability in advance.	Practically implemented. Does not require a cost for implementation.	Auxiliary Proof of Work (PoW)

Figure 6. A security-based framework of defense mechanisms based on the 51% attack.

Komodo blockchain appoints notary nodes for notarization. The nodes are appointed to retrieve the information from Komodo and save it in the bitcoin blockchain. In order to carry out double-spending, an attacker needs to rewrite the Komodo chain and bitcoin checkpoints. The attacker also needs to influence the majority of the notary network [52]. Hence, the whole process makes the technique quite robust. However, a limited number of nodes makes this security technique centralized, which introduces the widely known issue of a "single point of failure", where attackers know exactly what to attack. The dPoW is not cost-effective as it requires an implementation fee to be implemented to the blockchain. It can only be implemented to coins that are based on UTXO-based blockchain. Moreover, participants are required to wait for an explicit amount of time for the notarization process to be completed. It may discourage particular participants who aim to have a faster transaction. The notarization process is done every 10 min. This 10 min checkpoint time gives attackers a vast amount of time to conduct the 51% attack on crypto-coins in which the block confirmation time needs just a few seconds [52]. The attack risk of this security technique is low.

PirlGuard was developed to provide protection against 51% exploitation. This security technique is based on only the Ethash algorithm. It follows a similar approach to the "The Penalty System for Delayed Block Submission", which introduces a block delay. As discussed, the penalty system is vulnerable to the 51% attack; therefore, it is relatively easy for an attacker to achieve the required blocks. PrilGuard also involves master nodes for notarization, a centralized feature that makes the network weak because of the "single point of failure" security issue. PilGuard establishes that it mitigates the 51% attack to approximately 0.03%. Therefore, both the penalty system and master node feature have a low risk level.

ChainLocks also aims to provide protection against the 51% attack. The major limitation of ChainLocks is that it only protects one currency. Dash, having only 4100 master nodes, can be a prime target of a 51% attack due to the low hashing power [53]. It is very likely to conduct the 51% attack on low hashing currencies by simply renting the required hashing power [54]. Hence, the security features provided by ChainLocks are not robust enough to prevent the double-spending attack. Since only one confirmation is required to publish a block, attackers with much less than 51% of the hashing power can perform the double-spending attack, resulting in a more vulnerable Dash blockchain. Therefore, the risk level is classified as high.

Merged mining is a way to protect low reputed coins by making them more robust against the 51% attack. Merged mining is not a security technique itself, but due to the process of allowing two different cryptocurrencies based on the same algorithm to be mined simultaneously, it helps to mitigate the 51% attack. However, the process is quite complicated and often neglected by miners. The major limitation of this process is that the merged crypto-coins must be on the same consensus. Another drawback is that if two low hashing crypto-coins are merged, then they can still be exploited as long as the attacker achieves the required hashing power. Therefore, merged mining is just a process to increase the attacking cost by merging hashing power, and it does not provide an effective solution. We classify the risk level as high.

The longest chain rule is a key part of the protocol, but at the same time, it makes the blockchain vulnerable to the 51% attack and other variants. In an effort to mitigate those attacks, security techniques implementing specific policies were developed. Unfortunately, those policies contain weaknesses and fail to provide full protection.

As we discussed in Section 3.1, the longest chain feature is key in the blockchain protocol but without proper protection can be abused by attackers. We believe that in order to provide a secure protocol, the security policy must accept only a certain number of continuous blocks, regardless of the block generation time. This will mitigate 51% attack exploitation by preventing attackers from sending a free number of new blocks in a short period. Therefore, future security policies must discard blocks that violate an agreed threshold. Although the policy should be independent from cryptocurrencies, the threshold must be tuned to a particular one based on the total hashing power.

8. Conclusions

The assumption of having the majority of honest miners over the blockchain network has been underestimated resulting in realistic and practical 51% attacks to various cryptocoins. In fact, this encouraged attackers to perform the 51% attack. We have shown that the PoW consensus protocol comprises severe security risks and fails to protect against the 51% attack, uncovering that this and other consensus protocols are vulnerable.

We have also identified that the weaknesses which enable the 51% attack exploitation rely on the hashing power ability of mining pools and how this attack could cause immense damage to the blockchain network.

The presented security-based evaluation revealed the weaknesses of each technique by categorizing them in a three-tier risk level. In our analysis, we showed that all the security techniques fail to provide enough protection against the 51% attack. The implemented security policies lack robustness, and a sturdy policy must be in place to overcome the issue.

By studying the limitations of the consensus protocols and the protection techniques, we revealed the main weaknesses contained in them, suggesting that further research must be performed. A security policy accepting a limited number of blocks by totally ignoring the longest chain rule must be explored to mitigate the 51% attack effectively. For future work, we aim to develop an effective protection mechanism against the 51% attack by creating a robust consensus protocol without the weaknesses and limitations analyzed in this paper.

Author Contributions: Supervision, H.M.-G.; Writing – original draft, S.S.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Lafaille, C. What is Blockchain Technology. 2018. Available online: https://www.investinblockchain.com/what-is-blockchain-technology/ (accessed on 1 March 2019).
2. ComputerWorldUK. How Blockchain Is Being Used in Enterprise. 2018. Available online: https://www.computerworlduk.com/galleries/security/how-could-blockchain-be-used-the-enterprise-3628558/ (accessed on 1 December 2018).
3. Bitcoin.org. Bitcoin Is an Innovative Payment Network and a New Kind of Money. 2009. Available online: https://bitcoin.org/en/ (accessed on 1 August 2018).
4. Baliga, A. Understanding Blockchain Consensus Model. 2017. URL: https://pdfs.semanticscholar.org/da8a/37b10bc1521a4d3de925d7ebc44bb606d740.pdf (accessed on 1 August 2018).
5. What Is Blockchain. 2018. Available online: https://lisk.io/academy/blockchain-basics/what-is-blockchain (accessed on 1 July 2018).
6. Walker, H. How Digital Signatures and Blockchains Can Work Together. 2016. Available online: https://www.cryptomathic.com/news-events/blog/how-digital-signatures-and-blockchains-can-work-together (accessed on 1 August 2018).
7. Asolo, B. 51% Attack Exlpained. 2019. Available online: https://www.mycryptopedia.com/52-percent-attack-explained/ (accessed on 1 January 2019).
8. CoinDesk. How Bitcoin Mining Works. 2018. Available online: https://www.coindesk.com/information/how-bitcoin-mining-works (accessed on 1 August 2018).
9. Tuwiner, J. What Is Bitcoin Mining and How Does It Work? 2019. Available online: https://www.buybitcoinworldwide.com/mining/ (accessed on 1 March 2019).
10. Jimi, S. Blockchain: How a 51% Attack Works Double Spend Attack. 2018. Available online: https://medium.com/coinmonks/what-is-a-51-attack-or-double-spend-attack-aa108db63474 (accessed on 1 May 2018).
11. Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*; 2009. Available online: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.221.9986 (accessed on 15 May 2018)
12. Rosenfeld, M. Analysis of Hashrate-Based Double Spending. *arXiv* **2014**, arXiv:1402.2009.
13. Sharma, A. Understanding Proof of Stake Through Its Flaws. Part 3 Long Range Attacks. 2018. Available online: https://medium.com/@abhisharm/understanding-proof-of-stake-through-its-flaws-part-3-long-range-attacks-672a3d413501 (accessed on 1 June 2018).
14. Vitalik Buterin. Long-Range Attacks: The Serious Problem with Adaptive Proof of Work. 2014. Available online: https://blog.ethereum.org/2014/05/15/long-range-attacks-the-serious-problem-with-adaptive-proof-of-work/ (accessed on 1 September 2018).
15. ROWAN MARLEY. How Blockchain Can Fight DDoS Attacks. 2018. Available online: https://thechain.media/how-blockchain-can-fight-ddos-attacks (accessed on 1 January 2019).

16. Morgan, S. Blockchain Startup: 300,000 DDoS Attacks Will Cause 150B in Damages This Year. 2017. Available online: https://www.csoonline.com/article/3234775/security/blockchain-startup-300000-ddos-attacks-will-cause-150b-in-damages-this-year.html (accessed on 1 July 2018).
17. KASPERSKY. DDoS Breach Costs Rise to over 2M for Enterprises finds Kaspersky Lab Report. 2018. Available online: https://usa.kaspersky.com/about/press-releases/2018_ddos-breach-costs-rise-to-over-2m-for-enterprises-finds-kaspersky-lab-report (accessed on 1 January 2019).
18. Buterin, V. The P + epsilon Attack. 2015. Available online: https://blog.ethereum.org/2015/01/28/p-epsilon-attack/ (accessed on 1 June 2018).
19. Risberg, J. Yes, the Blockchain Can Be Hacked. 2018. Available online: https://coincentral.com/blockchain-hacks/ (accessed on 1 June 2018).
20. Douceur, J.R. *The Sybil Attack*; Revised Papers from the First International Workshop on Peer-to-Peer Systems; Springer-Verlag: London, UK, 2002; pp. 251–260.
21. Binance Academy. Sybil Attacks Explained. 2018. Available online: https://www.binance.vision/security/sybil-attacks-explained (accessed on 1 January 2019).
22. Natoli, C.; Gramoli, V. The Balance Attack Against Proof-Of-Work Blockchains: The R3 Testbed as an Example. *arXiv* **2016**, arXiv:1612.09426.
23. Maria, A.; Aviv, Z.; Laurent, V. Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. In Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2017.
24. Vervier, P.A. Why BGP Hijacking Remains a Security Scourge. 2018. Available online: https://www.symantec.com/blogs/feature-stories/why-bgp-hijacking-remains-security-scourge (accessed on 1 July 2018).
25. Reichl, P.; Egger-Lampl, S.; Schatz, R.; D'Alconzo, A. The Logarithmic Nature of QoE and the Role of the Weber-Fechner Law in QoE Assessment. In Proceedings of the 2010 IEEE International Conference on Communications, Cape Town, South Africa, 23–27 May 2010; pp. 1–5.
26. Tar, A. Proof-of-Work, Explained. 2018. Available online: https://cointelegraph.com/explained/proof-of-work-explained (accessed on 1 July 2018).
27. Lisk. Proof of Work. 2019. Available online: https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/proof-of-work (accessed on 1 March 2019).
28. Bitcoin Mining. 2017. Available online: https://powercompare.co.uk/bitcoin/ (accessed on 1 May 2018).
29. Wang, K. Cryptoeconomics: Paving the Future of Blockchain Technology. 2017. Available online: https://hackernoon.com/cryptoeconomics-paving-the-future-of-blockchain-technology-13b04dab971 (accessed on 1 June 2018).
30. Gautham. PoW Blockchain Could Be Vulnerable to Balance Attack. 2017. Available online: https://www.newsbtc.com/2017/01/29/pow-blockchain-balance-attack/ (accessed on 1 July 2018).
31. Stan Higgins. Bitcoin Mining Pools Targeted in Wave of DDOS Attacks. 2015. Available online: https://www.coindesk.com/bitcoin-mining-pools-ddos-attacks (accessed on 1 July 2018)..
32. Proof of Stake. 2018. Available online: https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/proof-of-stake (accessed on 1 July 2018).
33. Komodo. Komodo: Advanced Blockchain Technology, Focused on Freedom. 2018. Available online: https://komodoplatform.com/wp-content/uploads/2018/06/Komodo-Whitepaper-June-3.pdf (accessed on 1 March 2019).
34. Buterin, V. Proof of Stake: How I Learned to Love Weak Subjectivity. 2014. Available online: https://blog.ethereum.org/2014/11/25/proof-stake-learned-love-weak-subjectivity/ (accessed on 1 July 2018).
35. Asolo, B. Delegated Proof of Stake (DPOS) Explained. 2018. Available online: https://www.mycryptopedia.com/delegated-proof-stake-dpos-explained/ (accessed on 1 July 2018).
36. Solving the Byzantine Generals Problem with Delegated Proof of Stake (DPoS). 2018. Available online: https://www.radixdlt.com/post/what-is-delegated-proof-of-stake-dpos (accessed on 1 August 2018).
37. Matt. Bitcoin's Attack Vectors: 51% Attacks. 2018. Available online: https://medium.com/chainrift-research/bitcoins-attack-vectors-51-attacks-a96deac43774 (accessed on 1 January 2019).
38. Komodo. Komodo's Blockchain Security Service. 2019. Available online: https://komodoplatform.com/wp-content/uploads/2019/02/Komodo-Blockchain-Security-Service-Brochure.pdf (accessed on 1 March 2019).

39. Bastiaan, M. *Preventing the 51%-Attack: A Stochastic Analysis of Two Phase Proof of Work in Bitcoin*; 2015. Available online: https://pdfs.semanticscholar.org/0336/6d1fda3b24651c71ec6ce21bb88f34872e40.pdf (accessed on 1 March 2019)
40. Bai, Q.; Zhou, X.; Wang, X.; Xu, Y.; Wang, X.; Kong, Q. A Deep Dive into Blockchain Selfish Mining. *arXiv* **2018**, arXiv:1811.08263,
41. Vitalik Buterin. Selfish Mining: A 25% Attack Against the Bitcoin Network. 2013. Available online: https://bitcoinmagazine.com/articles/selfish-mining-a-25-attack-against-the-bitcoin-network-1383578440/ (accessed on 1 August 2018).
42. IOTA. What Is IOTA? 2018. Available online: https://www.iota.org/get-started/what-is-iota (accessed on 1 February 2019).
43. Daniel Barta. IOTA: The Currency of Skynet. 2018. Available online: https://hackernoon.com/iota-the-currency-of-skynet-281b6abaec5 (accessed on 1 March 2019).
44. Bitcoin.com. What Is Bitcoin Double-Spending? 2017. Available online: https://www.bitcoin.com/info/what-is-bitcoin-double-spending (accessed on 1 January 2019).
45. Jon Matonis. The Bitcoin Mining Arms Race: GHash.io and the 51% Issue. 2017. Available online: https://www.coindesk.com/bitcoin-mining-detente-ghash-io-51-issue (accessed on 1 September 2018).
46. Blockchain. Hash Distribution. 2019. Available online: https://www.blockchain.com/pools?timespan=24hours (accessed on 1 March 2019).
47. Alberto Garoffolo, Pier Stabilini, Robert Viglione and Uri Stav. A Penalty System for Delayed Block Submission. 2018. Available online: https://www.horizen.global/assets/files/A-Penalty-System-for-Delayed-Block-Submission-by-Horizen.pdf (accessed on 1 January 2019).
48. ChainZilla. Blockchain Security and How to Mitigate. 2019. Available online: https://medium.com/chainzilla/solutions-to-51-attacks-and-double-spending-71526be4bb86 (accessed on 1 February 2019).
49. Fawkes. PirlGuardInnovative Solution against 51% Attacks. 2018. Available online: https://medium.com/pirl/pirlguard-innovative-solution-against-51-attacks-87dd45aa1109 (accessed on 1 January 2019).
50. Alexander Block . Mitigating 51% attacks with LLMQ-based ChainLocks. 2018. Available online: https://blog.dash.org/mitigating-51-attacks-with-llmq-based-chainlocks-7266aa648ec9 (accessed on 1 March 2019).
51. Cryptocompare.com. What Is Merged Mining-Bitcoin & Namecoin-Litecoin & Dogecoin, 2015. Available online: https://www.cryptocompare.com/mining/guides/what-is-merged-mining-bitcoin-namecoin-litecoin-dogecoin/ (accessed on 1 January 2019).
52. ChainZilla. Blockchain Security and How to Mitigate. 2019. Available online: https://medium.com/chainzilla/solutions-to-51-attacks-and-double-spending-71526be4bb86 (accessed on 1 March 2019).
53. Edmund NG. A Dash to Mitigate 51% Attacks with ChainLocks. 2018. Available online: https://blockchainreporter.net/2018/12/01/dash-to-mitigate-51-attacks-with-chainlocks/ (accessed on 1 January 2019).
54. Nicehash. Largest Crypto Mining Marketplace. 2014. Available online: https://www.nicehash.com/ (accessed on 1 August 2018).