ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 10, October 2022

Review on Types of Attacks on Bitcoin and Ethereum crypto currencies

[1] Naman Shah, [2] Sonal R Dave
[1] Student Scholar, Department of Computer Engineering, LD College of College of Engineering, Ahmedabad, Gujarat
[2] Research Guide, Ahmedabad, Gujarat
[1] Namans1910@gmail.com, [2]xpertinfotek@gmail.com

Abstract*— Among the new way of exchanging money, using crypto currency has been very popular. Its also an investment to get good returns over the period of time. Cryptocurrency has grown to more than 120 million investors around the world as per a survey of 2021. Its growing at the 15 to 20% ratio around the world every year. This fact leads to a serious consideration of security and its vulnerabilities in block chain. Apart from market risks, high volatility, lack of rules and regulations, cyber risks are one of the most required types which needs proper attention and technical understanding. Because the crypto currencies are fully decentralized the risk of attacks is exposed and in most of the cases defenseless. Proof of stake and proof of work are two major algorithms followed by almost all crypto currencies to allot stocks to the holders. In this paper, different types of risks and attacks with POS and POW are explained with its mitigation. The problems and outcomes are examined, reviewed and conferred in case of Ethereum and Bitcoin crypto currencies. These currencies decentralized frameworks and anonymity attracts unlawful activities. Recognizing and preventing them needs understanding of the mechanism of attacks which are discussed in easiest possible ways for even a new-bee or an outsider person.

***Index Terms*— Blockchain, Bitcoin, Ethereum, Cryptocurrency, Attacks.**

I. INTRODUCTION

The transfer of control and decision-making from a centralized network to a decentralized network is referred to as decentralization in blockchain. As a consequence, in order to facilitate the validation and verification of any actions initiated by the blockchain network, it requires agreement from the network participants. Because of the entire system relies on network stakeholder consent, blockchain is a trustless, secure, and trustworthy method for online currencies.

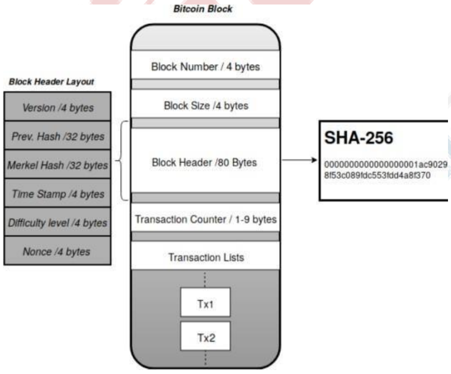

Fig 1. Structure of Block

With the introduction of blockchain technology, such as those used in bitcoin and other digital currencies, decentralized framework have attracted considerable attention. These systems incorporate cryptographic protocols and Markov chains to establish consent for financial transactions that exist in the system. As a result, there is no need for a centralized banking institution because a distributed ledger of transactions can be verified. The cryptocurrency system is decentralized, despite the fact that the ledger is distributed to all bitcoin users.The process mining with block chain technology.A blockchain is a digital record that enables transactions between participants without the requirement for a central authority or other dependable third party. However, the bulk of current blockchains employ the calculated Proof of Work (PoW) mechanism. Other consensus techniques proposed in blockchain include Proof of Stake and Proof of Elapsed Time. Blocks with a hash-based Proof of Work (PoW) algorithm are used by Bitcoin to assure transaction security.

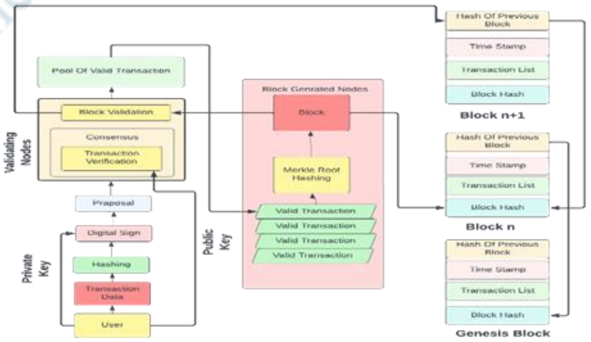

Fig 2. Transaction Flow in Blockchain

To prevent spam and Distributed Denial of Service (DDoS) attacks, PoW is a constructive protocol that checks all input data. Blockchain technology can keep decentralized transaction data in the past, with each linked computer storing the same data. It is required to analyze the performance of the transaction process in necessary to undertake an effecient transaction process [1].

Because it just provides payment services, Bitcoin is a term frequently used to describe blockcahin1.0. The digitization in the Bitcoin system is its consensus protocol, which enables disparate nodes in a peer-to-peer network to eventually come to some agreement on the result after carrying out payment transactions. Unlike previous consensus methods, participants come from an open network and are rewarded with Bitcoins (or BTCs), which are "mined" using a smart cryptographic hash function called Proof-of-Work (PoW), which was first developed as an anti-spam approach.Ethereum is the second most popular crypto currency, serving as a platform for digital money, international payments, and applications.

The community has spawned a robust digital economy, as well as novel new methods for creators to earn money digitally. The fundamental purpose of digital currency is decentralization; when accessing the network for trades, users may stay anonymous. To operate an Ethereum application, they do not need to disclose their personal information..

II. BACKGROUND

A.MECHANISM OF ETHEREUM

The most basic explanation of Ethereum is that it is a series of accounts each with a value in digital money, that constitute Ethereum's global presence. Accounts are recognized by a 160-bit address that is connected to a secret key that designed to validate any transactions made on their behalf. Ether is the cryptocurrency employed by Ethereum for transfers between these alleged external accounts. Transactions comprise source or destination addresses, the value in form of Ether, and a digital verification that authenticates the request, among other factors. Smart contracts enable the establishment of sub-currencies (tokens), wallets, independent administration, and peer to peer gambling/lottery applications, among other things[2].

B.MECHANISM OF BITCOIN

Hashcash is the PoW method used by Bitcoin. Hashcash was designed to protect email systems against denial of service attacks. This was accomplished by asking the prospective sender to pay some attention to completing a computationally challenging task before being able to send an email. The deployment of Hashcash in Bitcoin requires the potential miner to calculate a SHA-256 hash value for the header together with a random integer so that the hash value is below a certain threshold. In the Bitcoin network, this is a controllable parameter. The lower the number, the more challenging the problem. The Hashcash PoW method has two major consequences. One reason for this is because miners are now required to use specialized hardware, like as ASIC miners, and/or participate in mining pools, where the effort and incentive are shared across numerous people. More significantly, PoW discourages attempts to introduce faulty blocks into networks. Due to erroneous rectification, these blocks have a strong likelihood of being refused by the network, which would cause the potential miner to end up wasting a lot of resources[1].

C.HOW MINING WORKS

Blockchain mining is the process of calculating a new block for inclusion in the distributed ledger [8]. Because the block creation method changes amongst cryptocurrencies, mining is mostly associated with bitcoin. Mining computers are typically powerful devices used to generate the right hash values. While utilizing their devices to mine, mining nodes are expected to perform out a mathematical puzzle. A miner notifies the network when they generate a block. A block's equations are no longer being worked on by any miners in the network, and they must be regenerated for the subsequent block. During the mining process, the hash Merkle root is added to the nonce value. Each time the nonce is changed, a new hash is created and compared to the target. If the value of hash is small compared to the threshold, the mathematical problem has been resolved. If the hash value exceeds the threshold, the nonce value must be modified. and compared to the target value until the requirements are fulfilled. Hundreds of thousands of mining equipment are used in a mining operation. As a result, a pool generally has higher power compare to other miners in the network and has the benefit of finding the requisite hash more quickly. Bitcoin mining takes roughly 10 minutes and requires specialized technology. For each successful block they produce, a 12.5 BTC mining payout is given to miners in addition to the transaction fees every four years, the award is cut in half [6].

D.VALIDATING TRANSACTIONS IN PoW AND PoS

A consensus amongst the nodes is required whenever a new block is added to a blockchain. By solving a challenge of varying difficulty, each node is required by the Proof of Work (PoW) algorithm to earn the ability to add a new block to the existing chain. PoW is the reward for the node that successfully computed the hash.This node is referred to as a mining node or miner, and the act of resolving the mathematical riddle is referred to as mining. Miners have total control over each block in both consensus protocols and utilize the transaction pool to add transaction to their blocks, which they can prioritize as they see right. Furthermore, because block size is limited, this prioritizing is frequently dependent on transaction costs. To that aim, with PoW, nodes contribute their processing power in the expectation of receiving a network reward. In order to avoid wasting the remaining nodes' time and processing power, they can only do this if they are the first to finish the task. The blockchain system itself may provide the network incentive in the form of a block reward. For instance, when a block is created and uploaded to the main chain, the blockchain releases a specific number of tokens as compensation for work done by miner. Another kind of compensation is through transaction fees. Users can charge an additional charge to their account as a reward for having their transaction executed with a greater priority due to the congestion of blockchain networks [2].

The Proof of Work approach is discriminatory since not all miners have the same infrastructure.While some handle data and information using very advanced technology, others just have the most basic tools, which gives the first ones an edge because solving the riddle requires a lot of computational power. The methods based on Proof of Stake (PoS) attempt to address this disparity. The primary idea underlying PoS algorithms is to use the concept of a gamble or participation size to choose which miner will be able to produce the succeeding block in the chain. There is a benefit to using prior involvement as evidence: any node with a lot of prior engagement is more trustworthy, and it is presumed that this node will not opt any fraudulent tactics to undermine the chain that comprise a major percentage of its revenue. Additionally, the main advantage of PoS is, a double-spending attack requires at least 51 percent of all stakes in the network to be active, which is quite challenging [9].

Transactions from the transaction pool are selected by a miner or validator in a blockchain system and appended to their block. The miner in a PoW system must go above and above and complete a hashing challenge, whereas the validator in a PoS system simply needs to broadcast the block. That expense will be carried by the interested miner, who will then have to mine for them without knowing if their efforts would be fruitless or profitable.

III. CONCERNS AND ATTACK ON CONSENSUS PROTOCOLS

A.51% ATTACK

The 51 percent attack is a strategy used when an attacker has 51 percent of a target's resources. When an attacker obtains 51 percent of the hashing power, a 51 percent attack occurs. In order to launch this attack, a chain of blocks that is entirely distinct from the genuine chain is built privately. After being separated, the chain is sent into the network to be acknowledged as a real chain. The double-spending attack occurs in this manner. Attackers that have 51 percent of the hashing power or more will be able to bring down the network since the blockchain policy adheres to the longest chain rule [8].

A 51 percent attack on cryptocurrencies allows attackers to undertake fraudulent behaviors like as double-spending, market price control, and mining strategy control. We have chosen the top eight crypto-coins that have lately been attacked. Figure 3 depicts the total amount of damages incurred as a result of the 51 percent exploited between April 2018 and January 2019. Following bitcoin gold (BTG), which has lost almost $18 million, Verge (XVG) has had two attacks in the past two months, suffering losses of $1.1 million and $1.75 million, respectively. The rest of the coins suffered considerable losses as a result of exploitation. The overall loss averages $2.5 million per assault on individual currencies[4].

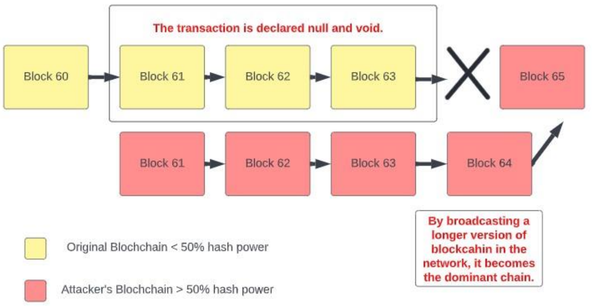
The transaction is declared null and void.
Block 60
Block 61
Block 62
Block 63
Block 65
Block 61
Block 62
Block 63
Block 64
By broadcasting a longer version of blockcahin in the network, it becomes the dominant chain.
🟨 Original Blochchain < 50% hash power
🟥 Attacker's Blochchain > 50% hash power

Fig 3 51% Attack

B.SYBIL ATTACK

In the sybil attack attacker can create multiple fake nodes that appears genuine to other nodes. To validate unauthorized transactions and to alter valid transactions, these fake nodes are used. They can carry out the attack using a few devices, virtual computers, or internet protocol (IP) addresses. They can use a small number of devices, virtual computers, or internet protocol (IP) addresses to carry out the attack .According to their hypothesis, every node in the P2P network that is active shares a single identity. Attackers can therefore block transmitted blocks and modify trustworthy nodes owing to a number of fake nodes. The possibility of double spending rises when a malevolent person possesses a significant number of network nodes. In order to increase the likelihood that attackers would accomplish double spending, a research suggested extending the Sybil attack method by combining Sybil and 51 percent attacks.

In summary a P2P system can be compromised if a significant portion of its nodes, which are intended to be safe and belong to diverse individuals, are instead controlled by one person who operates covertly.

Geographic routing systems, which are connected to share information between nodes and their neighbours to efficiently route the geographically addressed packets, are negatively impacted by this kind of attack. By causing buffer overflows or routing self-loops, tempering or resending the routing information might prevent the network from providing its services. It is difficult to identify the attack because of the attacker's highly mobile, unexpected, and convoluted pathways [2].

C.POOL HOPING ATTACK

In pool hoping to attack The pool management shifts its processing power to the ETH-based blockchain network once it determines that it can provide more revenue than other blockchain networks.. The pool manager can collect additional revenue because the miners' revenue distribution plan is still the original scheme. Based on the different levels of difficulty, a pool hopping attack technique was described in a different study for use across many blockchain networks. Using this strategy, the attacker utilizes more computer resources to block mining if the blockchain network's complexity value is small. When the network's difficulty value exceeds a certain level, the attacker immediately withdraws processing power from the blockchain network in order to recognize other blockchain networks in which difficulty values are smaller than the blockchain network, maximizing the attacker's revenues.

The effect of pool hopping on other pool users is caused by a movement in one mining factor without a matching shift in the other: time vs. hash rate. Without hoppers, the value of shares in a proportionate pool varies with time - shares submitted early in a round are worth much more than those submitted later - but as long as hoppers are absent, the value of shares averages out to a fair value. While hoppers have no effect on the average amount of shares per block or the number of shares submitted by an honest miner, they do shorten the time of the higher-paying sections of a round. With the most profitable part of the round requiring far less time to complete A miner that submits shares at a steady pace will have considerably more shares on average in the less profitable sections of a round than in the most profitable, lowering their total average share value. The more hoppers there are, the shorter the lucrative span and hence the more striking the effect [14].

D.P+ EPSILON ATTACK

A miner that submits shares at a steady pace will have considerably more shares on average in the less profitable sections of a round than in the most profitable, lowering their total average share value. The more hoppers there are, the shorter the lucrative span and hence the more striking the effect.

E. BALANCE ATTACK

The balancing attack is a tactic that concentrates on nodes with evenly distributed mining power. Double spending on PoW consensus may be accomplished using this method. On the Ethereum network, an attacker may employ their little hashing power to delay communications. With just 5% of the available hashing power, this attack may be executed. A delay is initially added in between the genuine node groups. The attacker mines a substantial number of blocks towards another subgroup in order to ensure that the other subtree favours the transaction subgroups. Through the use of the ghost protocol, the blockchain branch is kept isolated from the other nodes in the network. In order to affect the branch selection process, the split branch is subsequently forwarded to additional nodes[13].

F. BLOCK WITHHOLDING ATTACK

When a miner on a pool intentionally does not submit any blocks they find to the pool, this is referred as a Block Withholding attack. The goal of the attack is to diminish the mining pool's profitability. If continued for a long enough amount of time, this form of attack can bankrupt a pay-per-share pool. Because of the random nature of mining, mitigating a Block Withholding attack is difficult, but certain countermeasures have been devised, such as various cryptographic commitment techniques paired with hash functions. These systems often prohibit the pool administrator from cheating on the whole pool and make it hard for pool miners to differentiate between partial and complete proofs of work.

When a miner discovers a block in a victim pool and decides to forgo presenting it to the pool operator right away, he or she utilizes all of their available mining power to concentrate on the victim pool in order to raise the number of relative shares in the pool. After some time has passed, the blocker releases the previously discovered block. This is guarded by utilizing oblivious jobs, which prevent the miner from distinguishing between a full solution and a share.[12]

The attackers introduce the new chain onto the network once the discreetly mined chain has substantially developed. The new chain, which is longer than the current chain, will be seen as a genuine chain, and the network will disregard the blocks where attackers invest their money. The perpetrator wants to execute a transaction, wait for the seller to accept it, and then undo it so that they may spend the same money again. On blockchains, this might be done by presenting a contradictory transaction, perhaps in a different branch.

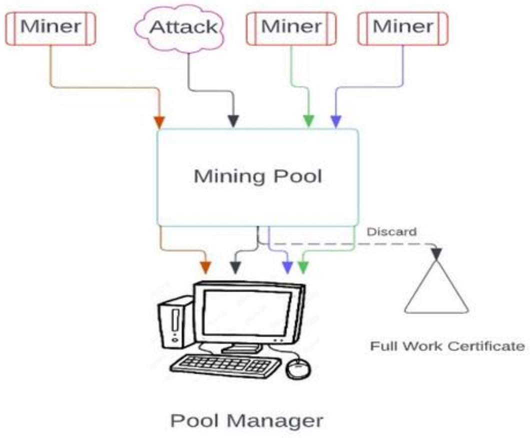

Fig 4. Block Withholding Attack

H. LONG RANGE ATTACK

The poor subjectivity model leads to long-range attacks. In terms of tactics, this attack strategy is exactly like the 51 percent attack. Despite the extremely low probability of this attack in Bitcoin, it may nonetheless be deleterious to the PoS and DPoS consensus procedures. When using a limited amount of coins rapidly following the Genesis block, in a PoS consensus scenario, some attackers may secretly build their own variant of the chain to conduct the attack. Despite the fact that, due to their small investment, they are only permitted to generate a restricted number of blocks at first, they will be capable of creating more when the process progresses. At first, they may create limited blocks due to less participation, but as the process progresses, they'll have the ability to create a longer chain. The chain can go incredibly extensive considering PoS does not set a limit on how quickly it can expand [7].

I. DOUBLE SPENDING ISSUE

The phenomena of double-spending occurs when a money unit is spent more than once at the same moment. As a result, there is a discrepancy between the cost balance sheet and the available currency.

Attackers engage in double spending by first using their coins in the legal chain. After then, they silently start constructing a new chain without using the attackers' money[12].

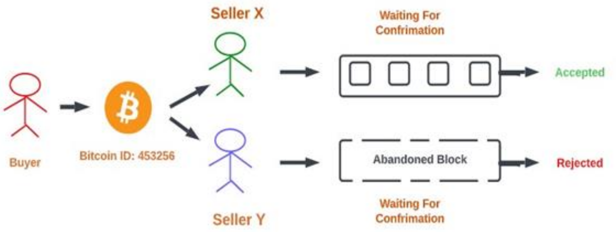

Fig 5. Double Spending Issue

J. LIVENESS DENIAL ATTACK

In PoS protocols, The Denial-of-Service attack is known as Liveness Denial. During this attack, some or all of the validators made the decision to intervene and deliberately obstruct transactions by halting the broadcast of blocks. The blockchain will come to a complete stop if validators are unable to accomplish their validator jobs because future blocks cannot be validated and broadcast. A liveness requirement that gradually depletes the stake of dormant validators will make sure that the network is not compromised even if the majority of validators remain unavailable or engaging in a liveness denial attempt. In circumstances when liveness cannot be determined, the community will have the option of forking the blockchain and removing inactive validators. Validators that engage in this form of attack risk their position as validators and their interest in the network if a shredding condition arises[5].

K. FAW (FORK AFTER WITHHOLDING) ATTACK

A FAW attack is a new kind of attack that incorporates selfish mining and block withholding. It involves target mining, malicious mining, and a variety of network mining pools. While certain miners are kept by the malicious mining pool to attack the target mining pool, other miners are kept to mine honestly. If the malicious mining pool utilizes an honest miner to successfully mine a block, it will instantly publish the block to the blockchain network and make money. If a miner being used by the malevolent mining pool effectively mines a block in the target pool, the concern of whether other mining pools have found the block must be answered. The miner does not broadcast the block if no other mining pools are mining it; otherwise, the miner publishes the block. A network fork happens when a miner broadcasts a block to the blockchain network rather than holding it locally if other mining pools do not participate in the transaction. To summarize, an FAW attack can assist the attacker in obtaining the income of a block withholding attack as well as extra earnings following network forking. As a result, some research has been dedicated to optimizing the FAW attack approach.The attacker spends enormous amounts of computing power on the target pool with low revenues since the traditional FAW attack just modifies the attacker's computing power allocation. Research suggested a PAW attack based on the FAW attack.

The full proof of work is sent to the pool administration by suspicious miners sent by the malicious mining pool if they discover it across several target mining pools. Another research offered a better FAW attack approach to boost the income of the forked network caused by the FAW attack. In this method, a miner designated to a rogue mining pool that forks the network quickly shifts from the FAW attack to legitimate mining. Additionally, the miner modifies the technique to counter the FAW attack after successfully mining the next block[14].

IV. CONCLUSION

In this paper literature survey is presented of different attacks over bitcoin and Ethereum crypto currencies in the modest way. The attacks like 51% attack, long range attack and double spending attack uses privately created mined chain that hides the original chains and pretend to be an authentic chain. Moreover, smart contracts in Ethereum helps in solving these issues at such extent, that exploits the vulnerability of attacks. For example: reentrancy and exception of disorders. Similarly, bitcoin suffers from unpredictable state and time constraints setbacks. The crypto currency owners and researchers can be aware of such risks and get solution to such threats by well understanding the above given literature review.

REFERENCES

[1] Simon joseph aquilina a , fran casino b,c , mark vella a,* , joshua ellul a,d , constantinos patsakis b,c, ‘‘etherclue: digital investigation of attacks on ethereum smart contracts,’’ in elsevier blockchain: research and applications 2 (2021) 100028.

[2] Moritz platt ∗ , peter mcburney, ‘‘sybil attacks on identity-augmented proof-of-stake,’’ in elsvier computer networks 199 (2021) 108424.

[3] Joseph j. Kearney, carlos a. Perez-delgado, ‘‘vulnerability of blockchain technologies to quantum attacks,’’ in elsevier array 10 (2021) 100065

[4] Sarwar sayeed and hector marco-gisbert *, ‘‘assessing blockchain consensus and security mechanisms against the 51% attack,’’ in appl. Sci. 2019, 9, 1788; doi:10.3390/app9091788.

[5] Sharyar wani 1,* , mohammed imthiyas 2 , hamad almohamedh 3,*, khalid m alhamed 4 , sultan almotairi 5,* and yonis gulzar, ‘‘distributed denial of service (ddos) mitigation using blockchain—a comprehensive insight’’ in symmetry 2021, 13, 227. Https://doi.org/10.3390/ sym13020227.

[6] Yourong chena,d , hao chenb , yang zhang b , meng hanc,d,∗ , madhuri siddulae , zhipeng cai, ‘‘a survey on blockchain systems: attacks, defenses, and privacy preservation,’’ in elsvier high-confidence computing 2 (2022) 100048.

[7] Evangelos deirmentzoglou,georgios papakyriakopoulos,constantinos patsakis ‘‘a survey on long-range attacks for proof of stake protocols,’’ in ieee access volume 7, 2019.

[8] Fredy andres aponte-novoa 1,2, ana lucila

[9] Sandoval orozco 1,3 , ricardo villanueva-polanco

[10] 1 , and pedro wightman 4 „ ‘‘the 51% attack on blockchains: a mining behavior study,’’ in ieee access volume 9, 2021.

[11] Gusti ayu kusdiah gemeliarana, riri fitri sari, ‘‘evaluation of proof of work (pow) blockchains security network on selfish mining,’’ in ieee 2018 international seminar on research of information technology and intelligent systems (isriti).

[12] Antonio lópez vivar, ana lucila sandoval orozco, luis javier garcía villalba, ‘‘a security framework for ethereum smart contracts,’’ in elsevier omputer communications 172 (2021) 119–129.

[13] Xiao yi,daoyuan wulingxiao jiang, kehuan zhang, wei zhang, ‘‘diving into blockchain’s weaknesses: an empirical study of blockchain system vulnerabilities,’’ in arxiv:2110.12162v1 [cs.cr] 23 oct 2021.

[14] Jehyuk jang and heung-no lee. ‘‘profitable double-spending attacks.’’ in appl. Sci. 2020, 10, 8477; doi:10.3390/app10238477.

[15] Christopher natoli, vincent gramoli, ‘‘the balance attack against proof-of-work blockchains: the r3 testbed as an example,’’ in arxiv:1612.09426v1 [cs.dc] 30 dec 2016

[16] M. Conti, e. S. Kumar, c. Lal, and s. Ruj, ‘‘a survey on security and privacy issues of bitcoin,’’ ieee commun. Surveys tuts., vol. 20, no. 4, pp. 3416–3452, 4th quart., 2018.

[17] M. Conti, s. Kumar, c. Lal and s. Ruj, "a survey on security and privacy issues of bitcoin", ieee communications surveys & tutorials, 2018.

[18] S. Bag, s. Ruj and k. Sakurai, "bitcoin block withholding attack: analysis and mitigation", ieee transactions on information forensics and security, vol. 12, no. 8, pp. 1967-1978, 2017.

[19] B. Biais, c. Bisiere, m. Bouvard and c. Casamatta, "the blockchain folk theorem", 2018.

[20] G. O. Karame, e. Androulaki and s. Capkun, "double-spending fast payments in bitcoin", proceedings of the 2012 acm conference on computer and communications security, pp. 906-917, october 2012.

[21] M. A. Javarone and c. S. Wright, "“modeling a double-spending detection system for the bitcoin network”", 2018.

[22] C. R. Davis, j. M. Fernandez, s. Neville and j. Mchugh, "sybil attacks as a mitigation strategy against the storm botnet", malicious and unwanted software 2008. Malware 2008. 3rd international conference on, pp. 32-40, october 2018.

[23] Bissias, a. P. Ozisik, b. N. Levine and m. Liberatore, "sybil-resistant mixing for bitcoin", proceedings of the 13th workshop on privacy in the electronic society, pp. 149-158, november 2014.

[24] E. Heilman, a. Kendler, a. Zohar and s. Goldberg, "eclipse attacks on bitcoin's peer-to-peer network", usenix security symposium, pp. 129-144, august 2015.

[25] D. Germanus, s. Roos, t. Strufe and n. Suri, "mitigating eclipse attacks in peer-to-peer networks", communications and network security (cns) 2014 ieee conference on, pp. 400-408, october 2014.

[26] Y. Kwon, d. Kim, y. Son, e. Vasserman and y. Kim, "be selfish and avoid dilemmas: fork after withholding (faw) attacks on bitcoin", proceedings of the 2017 acm sigsac conference on computer and communications security, pp. 195-209, october 2017.