PalArch's Journal of Archaeology of Egypt / Egyptology

SECURITY THREATS AND PROPOSED CONTAINMENT SOLUTION FOR BLOCKCHAIN: ASSESSMENT USING CASES

Sohail Shaikh[1], Madhavi Damle[2]

[1,2]Symbiosis Institute of Digital and Telecom Management, Symbiosis International (Deemed University), Pune, India.

Email: [2]mdamle@sidtm.edu.in

Sohail Shaikh, Madhavi Damle: Security Threats and Proposed Containment Solution for Blockchain: Assessment using cases -- Palarch's Journal Of Archaeology Of Egypt/Egyptology 17(6). ISSN 1567-214x

Keywords: Security, Smart Contract, Blockchain, Cryptocurrency.

ABSTRACT

Blockchain is a time-stamped series of immutable records of data that is not controlled by any single body. Since, the advent of Bitcoin, blockchain has found application in various industries such as healthcare, music, real estate, fintech, logistics, and others. The fact that blockchain ensures more dependable and convenient services is critical to consider the privacy and security risks related to this technology. Blockchain has been exposed continuously to security issues and considerable losses have been caused due to cyber-attacks on it. In this paper, we adopt a case study-based approach discussing the use cases of blockchain threats, its impact, and solutions and also review the security enhancement solutions. The data for this study has been collected from various secondary collections and a mitigation matrix has been created to show the types of cases. Even though there are a few studies done on the protection and privacy of blockchain, there is an absence of proper examination on the security of the blockchain. This research will help managers to adopt a new approach to understand and adapt to emerging risks related to blockchain and develop the necessary risk mitigation strategy for an organization.

1. Introduction

Blockchain was conceptualized first in 2008, by an individual or a group of individuals named Satoshi Nakamoto. This technology was first used in Bitcoin (Nakamoto, 2007). Satoshi Nakamoto invented blockchain in the year

2008 and released its code as open source in 2009. Due to the acceptance of bitcoin as a currency by websites and startups, the value of bitcoin continued to rise, but the value of bitcoin is unstable (Joshi et al., 2018). However, blockchain the key technology behind bitcoin is gaining popularity, it has found new applications in various sectors such as stock trading, data management, identity management, file storage, supply chain auditing, crowdfunding, and others (Rosic, 2016).

Blockchain is an decentralized immutable ledger that means the stored data cannot be deleted or tampered with and it does not have one centralized server (Taylor et al., 2019). The remarkable part of this technology is that the participants do not need to trust each other to interact as the network is open and the nodes automatically record and verify the transactions without any central authority or third-party interventions such as banks, governments, financial institutions, and other organizations (Griffin & Shams, 2019). By implementing a consensus protocol, the agreement goal is reached which dictates the rule with the help of which users should play and abide (Seang & Torre, 2018). The use of blockchain provides transparency as it is open and accessible to all. Blockchain allows the construction of smart property, smart contracts, and decentralized currency. Due to such advantages and applications of blockchain, it is regarded as one of the most significant inventions since the internet itself (Nguyen et al., 2019).

As blockchain is one of the most important technologies and is being used widely in various fields the users are very concerned about its security. Further digital currencies are being stolen, the attack on security exchanges are on the rise, and various other incidents have taken place in recent years (Wang et al., 2019). As the application of blockchain increases the threats related to the security of blockchain also increases (Li & Chen, 2017).

In this paper, some of the basic concepts of blockchain, along with the consensus functions are discussed. The paper discusses the present security of blockchain with the help of some recent security cases on the blockchain. The paper then proposes some solutions to mitigate these threats and improve the security of the blockchain. In the end, the paper explores few future directions and then ends the research with a conclusion.

2. Literature review:

2.1 Overview of Blockchain Technologies

The three main important pillars of blockchain technology with the help of which blockchain has helped to gain popularity are (Rosic, 2016):

1. Decentralization
2. Transparency
3. Immutability

Decentralization:

Coordination among individual activities was not possible before the invention of blockchain. There had to be a centralized entity that could interact between the entities and act as a third party which stored all the data and to get the necessary information you had to interact with this centralized system. There

are some drawbacks of using a centralized system such as it makes an easy target for hackers as all the data is stored in one centralized system or if the centralized system goes down or needs a new upgrade the whole system had to shut down and no one else could access the data in it. These drawbacks were overcome using blockchain technology.

As blockchain uses a decentralized system, the data is not kept in a solitary unit, instead, it is distributed over a vast network and everyone on the network has access to that information (Rosic, 2016). Due to the use of this decentralized system, it becomes very difficult for the hackers to hack into the system and even if multiple people try to shut down the system blockchain will still be able to run (Khandelwal, 2019).

Transparency:

Blockchain is distributed over a vast network where everyone can see the information in it. A person's identity is represented only by their public address and their original identity is hidden with the help of complex cryptographic functions; this ensures privacy for the user. This kind of transparency is the first of its kind in any financial system as you are able to see all the transactions done by the person's public address, the real identity of the person is secure. Transparency also forces an entity to be honest as all the transactions done are publicly available (Rosic, 2016).

Blockchain can be trusted because for each node the data records done by the blockchain are transparent, it is also transparent during the update of the data (Lin & Liao, 2017). Based on the company's ability to manage equity, assets, and debt the valuation can be placed and investors can be provided with a transparent view of the company's performance. With the help of blockchain, a new era of financial transparency can be started. (Silver, 2020).

Immutability:

Immutability is the property of the blockchain to remain unaltered or unchanged over a period of time. The data in the blockchain network is very hard to change once it is stored (Rosic, 2016). Additionally, due to the distributed consensus mechanism, it can achieve consensus even in a trustless environment (Nguyen et al., 2019). Cryptographic hash functions are the main reason for the blockchain to get this property (Rosic, 2016). For auditing data, this function is highly beneficial. By this property, the recipient of the data is confident about the data being unaltered and authentic. Also, the data provider can verify that the data is not altered, secured, and efficient.

For databases used in financial transactions, this element of immutability is very useful as the records are present there forever and no changes can be made in the record unless somebody takes control of 51% or more nodes simultaneously in the system, which is highly unlikely cause to do this one require extremely high computational power. The chain being on a distributed platform such attempts can be detected by other nodes and this would get investigated (Joshi et al., 2018).

2.2 Consensus Function

Blockchain uses a decentralized consensus mechanism to check the consistency and reliability of transactions and data. The consensus mechanism is an important part of a blockchain network which in a trustless environment ensures that each node approves on network condition. Other than this property consensus mechanism also takes care of other operations such as incentivizing the participants and addition of the transactions (Li & Chen, 2017).

In a blockchain network, the nodes can behave maliciously, be faulty, perform arbitrarily, or contain misinformation due to latency in connection, an example of such instance is the Byzantine failures. It is called a Byzantine failure because of its similarity to Byzantine generals' problem. Byzantine General problem took place when some of the generals commanding a certain percent of the Byzantine army circled around a city. During this time some generals favored the decision of retreating while some preferred the option of invasion. So, if only a part of the army attacked the city the attack would be unsuccessful. This was a major problem to reach a consensus on retreat or attack in such kind of environment. A similar problem is also faced in blockchain as there is no centralized authority present and the network is distributed (Joshi et al., 2018).

2.2.1 Proof of Work (POW):

Earlier blockchain networks were built on the POW mechanism. This protocol is used as a standard to stop incidents such as a denial of service or any other incidents like this which may waste the processing time of the computer (Joshi et al., 2018). For a new block to be accepted cryptographic proof of work is required. For example, bitcoin relies on a SHA256 algorithm for calculating proof of work and verifying transactions, in which for the block to be accepted the output of the hash should be in a select range (Nguyen et al., 2019).

In the blockchain, a random node or user is selected by nominating someone to record the transaction and this may lead to vulnerability attacks. A lot of computational calculations are required to verify the random node or user if a user requests to issue a new block. Nodes calculating the value of the hash in proof of work mechanism are called miners. The block header's hash value containing a nonce in a network is calculated by every node. This value is often altered by the miners to generate distinct hash values. With the help of this protocol, the calculated values are entailed to be equivalent to or lesser than a specified value. As soon as the target value is achieved by the nodes, it broadcasts the block on the network and then the other nodes approve accuracy of the hash. Now if the block is approved, the other nodes add this block to their own blockchain. This process of calculating hash value is called mining (Joshi et al., 2018).

POW mechanism is vulnerable to 51% attack. In this type of attack if a solitary node controls network computational power of more than 51% they can alter the data or by adding conflicting blocks prevent other transactions or in a cryptocurrency network use their coins multiple times. Networks that are new with inadequate computational power are exposed to this attack whereas for a

large blockchain network this attack may not be that serious as a lot of computational power is required. (Nguyen et al., 2019).

2.2.2 Proof of Stake (POS):

POS is a consensus protocol where the users can mine or authenticate new transactions on the basis of amount the user holds. Unlike POW, excessive processing power is not needed by the POS mechanism. Instead, the rights depend on the volume of resources held by the user on the network. According to this protocol people are much less probable to attack the network if more currency is involved. The more amount of money involved by the user the higher the chance of selection. A miner should maintain the least amount of cryptocurrency needed to be an authenticator and blockchain tracks set of miners in this protocol.

A specific form of transaction is sent by the miner that locks as a deposit in the cryptocurrency. The validated participants than undertake the method of validating and creating fresh blocks (Joshi et al., 2018). For a successful attack on the network, the attacker needs to own a majority of bitcoin which is much more expensive and the incentive provided by the proof of stake mechanisms is lesser than the amount the user has at stake. Due to this reason, the attacker will suffer seriously by his own attack (Lin & Liao, 2017).

Owing to delay in the network in practice this is much more complicated to implement which might make the validators receive offset chain information (Seang & Torre, 2018). According to Vitalik Buterin, co-founder of Ethereum, proof of stake consensus mechanism is going to make Ethereum safer compared to Bitcoin as the attack on this network will be much more expensive (Otieno, 2019).

3. Risks related to blockchain and use cases: results and discussions:

3.1 Case 1 - Selfish Mining Attack

Description:

The miners in selfish mining without broadcasting to the network keep the mined block and create separate branch that gets announced only after sufficient demands are fulfilled. In this attack, while the private chain is mined by the selfish miners the honest miners waste plenty of time and resources (Joshi et al., 2018). By intentionally keeping their block private the miners in selfish mining attempt to increase their reward. The selfish miners to acquire a chain longer than the public block resume to mine private blocks of their own instead of releasing them to the public. A race among the private chain of selfish miners and the public chain of honest miners are caused due to such activities. Selfish miners to claim block rewards release their blocks during the time public blockchain starts arriving to their private chains size. Also, the greater mining power of selfish miners helps them to win the block race (Saad, Spaulding, et al., 2019).

As a part of the blockchain, the selfish miners chain is admitted whereas the honest miners are forced to waste processing power making them useless. Bocks made by the honest miners are made useless by the selfish miners

because just before the honest miners, the selfish miners will be revealing their new blocks (Solat & Potop-butucaru, 2017). Due to factors like this, selfish miners incentivize honest miners to join the branch and gains a competitive advantage. Due to the combination of mining power in favor of the attacker, the decentralization nature of the blockchain is undermined by this attack (Li & Chen, 2017).

Impact:

Without being detected to compromise the blockchain applications the attackers might occupy adequate hash power from online servers to add 51% attack along with selfish mining (Saad, Njilla, et al., 2019). In the year 2018, from May to June, five of the Blockchain-based cryptocurrencies that are Bitcoin Gold, Litecoin Cash, Verge, Monacoin, and Zencash suffered a loss of USD 5 million because they were targeted by a 51% attack. The attackers acquired greater than 51% network's hashing power in each cryptocurrency that then was used for stopping other miners from computing blocks or rearrange transactions. Due to this, the attackers obtained power over blockchain carrying out double spending (Saad, Spaulding, et al., 2019).

Probable Solution:

A new protocol named FruitChain was proposed by Pass and Shi which extends the bitcoin proof-of-work with compensation mechanism along with similar liveliness and consistency attributes with estimated proof of Nash equilibrium.

There is another protocol named Ouroboros for proof-of-stake blockchain protocol in which a reward mechanism is incorporated in the proof-of-stake protocol which shows that the Nash equilibrium is approximated by the honest miners. Therefore, authentic transactions will become permanent and approved and attacks such as selfish mining can be neutralized (Zhang et al., 2019).

3.2 Case 2 - Reentrancy Attack

Description:

The reentrancy attack is a type of logical race problem, the main aim of the reentrancy attack is to destroy the atomicity of the transaction and to hijack the flow of contract control (Wang et al., 2019). In the reentrancy attack, by making calls repeatedly the adversary can obtain the ether which is in the contract before sending the ether if the balance of user is not refreshed. If a user is careless and forgets to update his balance, he might end up losing his whole contract balance (Saad, Spaulding, et al., 2019).

During the calling of a smart contract, after the call is completed there is a change in the contract account's existing state. The intermediate state can be used by the attacker to conduct calls recursively to the smart contract and if Ether is involved in the contract then it might result in illegal Ether stealing (Li & Chen, 2017).

Impact:

A project known as "The DAO" was established by a company known as Slock by crowdfunding. It collected 12.7 million Ether which was valued at USD 150 million as crowdfunding got an overwhelming response.
The DAO was attacked by a hacker who recognized a weakness in code where without examining the settlement of the current transaction a recursive withdraw function could be executed. The attacker than by requesting a withdrawal and contributing a small amount started the attack with a recursive function. With the help of this, the attacker was able to gain almost USD 70 million out of the crowdfund (Marketing, 2019).

Probable Solution:

An opportunity is provided by the new programming language to study common attacks and existing languages of smart contracts that are programmed in these languages. Some common pitfalls and exploits by design can be prevented by using a smart programming language that covers this characteristic.
As of now a language-based approach on a process calculi is preferred that prevents some of the common exploits by design including the reentrancy attack that almost destroyed the DAO. This type of attack is prevented, as among diverse processes no state is shared and a process, if it is still running, cannot be called again unlike a function, and therefore, no unplanned change takes place. Work like this evaluates if such a language can be combined effectively in a smart contract virtual machines and the attacks can be prevented on the language level (Tuncer et al., 2017).

3.3 Case 3 – Border Gateway Protocol Hijacking Attack

Description:

BGP routing protocol manages the way IP packet is sent towards their respective target. Attackers either manipulate or leverage BGP routing to interrupt the blockchain network traffic. To delay the network messages the BGP hijacking generally need to command the network operators that can be misused (Li & Chen, 2017). A collection of IP prefixes to which the data is routed is represented by an autonomous system.
In BGP route hijacking, an attacker autonomous system announces the prefix that belongs to a victim, and owing to this factor the traffic is re-routed through or to the attacker autonomous system. An attacker can also send faulty or malicious traffic to a victim. The victim is left incapable of processing valid BGP traffic and exhausts its resources to handle the traffic (Ali & Kupcu, 2020). The Internet Service Providers (ISPs) which is responsible for handling traffic routing, controls one or more autonomous systems that control the flow of the traffic (Ali & Kupcu, 2020). Owing to the huge centralization of some mining pools there will be a considerable effect if this type of attack. The attackers can effectively delay the speed of block broadcast or divide the Bitcoin network (Li & Chen, 2017).

Impact:

During the last couple of years, many BGP attacks have took place against the autonomous systems that host cryptocurrency exchanges or mining pools. A malicious ISP in Canada in the year 2014, interrupted mining pools traffic by announcing BGP prefixes belonging to key ISPs such as LeaseWeb, Amazon, Alibaba, and Digital Ocean. Owing to this the attacker was able to gain USD 83,000. In April 2018, MyEtherWallet.com which is mainly utilized in trading Ethereum token was attacked by a series of BGP attacks. Around USD 152,000 was stolen by the attackers from the web application (Saad, Spaulding, et al., 2019).

Probable Solution:

A new BGPCoin system is introduced with a blockchain-based dependable source infrastructure and resource assignment attestation that is based on a smart contract as a solution for BGP security. It is a dependable blockchain-based solution that gives consistent repudiations and resource distributions, and are responsible for starting an advertisement source. On the tamper-resistant blockchain-based Ethereum by using a smart contract to supervise and perform resource assignment. BGPCoin yields noteworthy advantages in the safe origin advertisement and the dependable infrastructure for object repository compared to other solutions. BGPCoin poses a credible and achievable BGP security solution on the state of security of smart contract programming and Ethereum blockchain (Xing et al., 2017).

3.4 Case 4 - DDoS

Description:

Distributed Denial-of-Service (DDoS) is a networking attack which targets mining pools, currency exchanges, e-wallets, and other services in blockchain (Conti et al., 2018). In this attack, the targeted server is flooded with superfluous requests to prevent other users from normal services and overload the system. This can then prevent the blockchain users from receiving normal services (Park & Park, 2017).

From several different sources that are distributed over the internet the incoming traffic flooding attack to a victim is originated. By taking advantage of some individual's computer security weaknesses and vulnerability a hacker may utilize the entity's computer to attack other computers (Zhang et al., 2019). Launching a DDoS attack has minimal to no adverse effect on the functions of network owing to consensus mechanism and decentralized nature of blockchain, so the DDoS attacker to disturb the DDoS network has to launch a powerful DDoS attack (Conti et al., 2018). Bitcoin is among the top industries that are susceptible to DDoS attacks and this shows the security challenges faced by blockchain industry (Wang et al., 2019).

Impact:

In June 2017, Bitfinex a cryptocurrency exchange was led to temporary suspension due to a distribution denial-of-service (DDoS) attack. Various exchanges of cryptocurrencies such as Ethereum and Bitcoin have been

regularly experiencing a DNS or DDoS attack which is restraining the service available to the users (Saad, Spaulding, et al., 2019).

Probable Solution:

A Proof-of-Activity protocol was proposed as a solution to DDoS attack in which the user that stores the first transaction places the crypt value that is stored in each block header. These users are assumed, to be honest, and are known as stakeholders. If more stakeholders are connected with the chain only then more transactions are stored and storing crypt value is arbitrary. More miners are attracted to a chain that is more in length and is more trustworthy between other peers. Since all the networks are governed by stakeholders in the network an attacker cannot place a malicious transaction or block (Conti et al., 2018).

In fee-based design, a mempool accepts an incoming transaction only if the mining fee and relay fee both are paid. By allowing transactions that aims to be mined in the blockchain is the key idea behind this to counter the DDoS attackers. Therefore, this technique reduces the mempool size by putting a cap on the filter's spam transactions and incoming transactions (Saad et al., 2018).

3.5 Case 5 - Wallet Attack

Description:

The wallet theft attack takes place along with some consequences on application as the credentials like the keys that are connected to peers in the system are kept in a digital wallet. A wallet is stored un-encrypted by default in a Bitcoin network that allows attackers to know the nature of transactions issued by it. The attackers can steal the wallet with a malware attack even when a wallet is guarded safely. The wallets can be leaked to an attacker as there are many third-party services enabling storage of wallets which can be compromised (Saad, Spaulding, et al., 2019).

This attack mostly occurs due to failure to do sufficient permission checks or fail to make explicit functions visible due to which an attacker can modify or access a particular function (Wang et al., 2019). For regular automated payments, wallet contracts are additional logic that can be built on the user wallet (Marketing, 2019).

Impact:

An attacker hacked the parity client wallet which resulted in holding up of 500,000 Ether. To reduce the transaction or gas fees, a centralized library contract was used by the Parity multi-sig wallet functionality. But there was a vulnerability in this function as there remained few important functions open that the attacker exploited. After this the attacker became a joint owner for all the wallets that were implemented after a particular date by adding himself as an owner of the account. He then froze all the currencies in the wallet by triggering a kill function. As of that day, a total of USD 155 million were forever locked by the attacker in cryptographically inaccessible wallets (Marketing, 2019). A new updated version of the library contract and security

alert was then released by the official Parity blog and Twitter (Wang et al., 2019).

Probable Solution:

To **secure** wallets secure and advanced ways are used to store the user keys such as brain wallets and paper wallets. In the brain wallet as the name suggests the keys are stored in the form of a small paraphrase in the minds of clients. The correct private key can be generated if the passphrase is memorized correctly. The keys are written on a document in a paper wallet and then the keys are stored at some physical location which can be compared to the cash money storage system.

A cold wallet can also be used for the protection of wallets. The excess amount by the user is stored in a cold wallet which is another account. In this method, two computers are used in which the second computer is disconnected from the internet and a new private key is generated by using a wallet software. The extra amount can be added to the new wallet with the help of private key. The wallet safety can be achieved as the hackers cannot get keys because of the computer not being connected to the internet (Conti et al., 2018).

3.6 Case 6 - Eclipse Attack

Description:

In an eclipse attack, a group of malicious nodes by using IP addresses isolates its neighboring nodes which compromises their incoming and outgoing traffic in blockchain, a node cluster can be formed when a node can connect every other node in the network. Every peer in a node cluster is aware of the IP addresses of other peers. The attacker can change the blockchain view and isolate the honest nodes in a cluster with the help of sufficient nodes. The attacker can then feed them with false information about transactions and blockchains by controlling their incoming and outgoing traffic (Saad, Spaulding, et al., 2019). The attacker blocks or diverts towards itself the IP addresses which are used by the user to connect.

To deceive the victims from the network the attacker can hold multiple IP addresses (Conti et al., 2018). By occupying and holding the victim's slots the node is reserved in a remote network. The eclipse attack is specially designed to isolate the nodes by blocking the newest blockchain data from invading the eclipse node (Wang et al., 2019). After separating, the attacker can also cost the victim unneeded computing power on blockchains outdated views. Than the attacker can conduct its malicious acts by leveraging the computing power of the victim (Li & Chen, 2017). Other attacks like the selfish mining and double spending can be launched by the attackers on the network by deploying helpers (Conti et al., 2018).

Impact:

Ethan Heilman presented the first eclipse attack on blockchain's peer-to-peer protocol known as Bitcoin and also demonstrated the eclipse attack (Heilman et al., 2015). By controlling its victim's access to information, the attacker can

then filter victim's blockchain view or for more sophisticated attacks use the victim's computational power. Kademlia protocol was designed for logarithmic content discovery and Ethereum inherits most of the complicated artifacts of the Kademlia protocol and this results in the creation of serious vulnerabilities. By controlling only two machines with single IP address each this type of attack can be launched by an attacker (Marcus et al., 2018).

Probable Solution:

The simplest method of mitigating an eclipse attack is by blocking the incoming connections and by making only outgoing connections to specific nodes. Whitelists are used to choose specific outgoing connections. To enhance important security features is one of the major features of using a whitelist. Known miners or well-connected peers are mostly the ones whitelisted (Heilman et al., 2015).

4. Discussion and findings:

Blockchain has witnessed growing popularity in the last few years owing to its decentralized nature, transparency, and immutability. But as its applications increase the threats to the blockchain network also increases so it is important to understand blockchain vulnerabilities for emerging applications. There is a risk of the data being hacked even though the transactions are being encrypted and anonymous.

POW requires high energy efficiency and also in POW the miners compete for block rewards which leads to block race. This race condition causes attacks like double spending, selfish mining, and others. Ethereum uses a POS protocol to overcome these vulnerabilities but the use of POS is unjust as it favors the rich owing to its auction process for the mining of blocks. In smart contracts, the flexibility in their programming makes it more vulnerable as the user's balance can be stolen causing a reentrancy attack, attacks like this cannot be caused on other cryptocurrencies that do not offer programming flexibility such as Bitcoin.

Currently, there are many security problems in blockchain, but as it happens to any new technology there is a need to have a continuous problem-solving approach to enhance the technology. Blockchain is still in the developing phase and it will provide new opportunities in the future, but the attacks on its surface will also rise. It is important to find effective solutions for future use and security of the blockchain and more research is needed to be done on the security of this technology.

Table 1: Risk Mitigation Model

Area	Description	Impact	Probable Solution
Selfish Mining Attack	For gaining unneeded rewards or wasting resources of honest miners	Deteriorate resources of honest miners and reduce income of the pool	Fruit Chain and Ouroboros can be used by incorporating a reward mechanism to neutralize the attack.
Reentrancy Attack	To destroy the atomicity of the transaction and to hijack the flow of contract control	Illegal stealing of Ether.	Smart Programming Language can be designed to prevent some common pitfalls and exploits.
BGP Hijacking Attack	To interrupt miners' connections to a mining pool server	To steal cryptocurrencies	BGPCoin is a dependable blockchain-based internet resource management solution.
Exchange DDoS	A combined attack to exhaust network resources	The services for honest miners are denied, segregate or ban the miners	Proof of Activity (POA) protocol or Fee-based design is used to mitigate DDoS attacks.
Wallet Attack	Attackers destroy or steal users private key	Cryptocurrencies in the wallet are lost	Brain Wallet, Paper Wallets, or Cold Wallet is used to secure the wallet.
Eclipse Attack	Attacker isolates the victim in the network from the other peers	For conducting malicious attacks, the attackers take control the victim's computing power	Use of whitelists or disabling of incoming connections is done to mitigate this type of attack.

5. Conclusion:

Blockchain works on a decentralized network and uses the peer network and its computing resources. To improve the blockchain security consensus protocols such as POW and POS are used. The main core of blockchain is supportive and secure owing to which major applications that need trust and security will shift towards this technology. Blockchain has attracted huge interests due to its increasing use in industry and academic research. As applications based on blockchain grows, amount of security threats on blockchain system also rises. The security of the blockchain is constantly improving and still, threats related to blockchain are being reported and there are active studies on security.

The objective of this paper is to focus and understand the major threats related to blockchain, concentrating on various cases and propose a mitigation model to limit these risks. In this paper, several use cases regarding blockchain attacks are mentioned with the impact these attacks have on an organization and probable solution for resolving the same. In this paper, various attacks on blockchain technology are explored and the research on ongoing defense activities is highlighted. With the current state of blockchain security, various attacks can still be launched on the blockchain network. To mitigate this type of attacks and stir new research directions, in this paper some countermeasure has been highlighted which can enhance the security and use of blockchain. In

the blockchain, there is a difficulty in implementing new innovative applications and there are still some limitations regarding its use, but still, the blockchain is going to be a technology that will soon be widely used in various industries.

References

Ali, F. S., & Kupcu, A. (2020). Improving PKI, BGP, and DNS Using Blockchain: A Systematic Review. http://arxiv.org/abs/2001.00747

Conti, M., Sandeep, K. E., Lal, C., & Ruj, S. (2018). A survey on security and privacy issues of bitcoin. IEEE Communications Surveys and Tutorials, 20(4), 3416–3452. https://doi.org/10.1109/COMST.2018.2842460

Griffin, J. M., & Shams, A. (2019). Is Bitcoin Really Un-Tethered? SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3195066

Heilman, E., Kendler, A., Sun, Y., Edmundson, A., Vanbever, L., Zürich, E. T. H., Li, O., Rexford, J., Chiang, M., Mittal, P., Edmundson, A., Vanbever, L., & Rexford, J. (2015). Eclipse Attacks on Bitcoin's Peer-to-Peer Network. USENIX Security.

Joshi, A. P., Han, M., & Wang, Y. (2018). A SURVEY ON SECURITY AND PRIVACY ISSUES OF BLOCKCHAIN TECHNOLOGY. 1(2), 121–147. https://doi.org/10.3934/mfc.2018007

Khandelwal, A. (2019, November 29). Seven pillars of blockchain. https://www.investindia.gov.in/team-india-blogs/seven-pillars-blockchain

Li, X., & Chen, T. (2017). A Survey on the Security of Blockchain Systems. January 2020. https://doi.org/10.1016/j.future.2017.08.020

Lin, I. C., & Liao, T. C. (2017). A survey of blockchain security issues and challenges. International Journal of Network Security, 19(5), 653–659. https://doi.org/10.6633/IJNS.201709.19(5).01

Marcus, Y., Heilman, E., & Goldberg, S. (2018). Low-Resource Eclipse Attacks on Ethereum's Peer-to-Peer Network. IACR Cryptology EPrint Archive, 2018(January), 236.

Marketing, A. (2019, January 22). 10 Blockchain and New Age Security Attacks You Should Know | Aruba Blogs. https://blogs.arubanetworks.com/solutions/10-blockchain-and-new-age-security-attacks-you-should-know/

Nakamoto, S. (2007). Bitcoin : A Peer-to-Peer Electronic Cash System. 1–9.

Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T., & Dutkiewicz, E. (2019). Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities. IEEE Access, 7, 85727–85745. https://doi.org/10.1109/ACCESS.2019.2925010

Otieno, N. (2019, October 15). Vitalik Buterin Believes Proof-of-Stake Algorithm Will Make Ethereum More Secure Than Bitcoin | Blockchain News. https://blockchain.news/news/vitalik-buterin-believes-proof-of-stake-algorithm-will-make-ethereum-more-secure-than-bitcoin/

Park, J. H., & Park, J. H. (2017). Blockchain Security in Cloud Computing : Use Cases , Challenges , and Solutions. 1–13. https://doi.org/10.3390/sym9080164

Rosic, A. (2016). What is Blockchain Technology? A Step-by-Step Guide For Beginners. https://blockgeeks.com/guides/what-is-blockchain-technology/

Saad, M., Njilla, L., Kamhoua, C., & Mohaisen, A. (2019). Countering Selfish Mining in Blockchains. 2019 International Conference on Computing, Networking and Communications, ICNC 2019, 360–364. https://doi.org/10.1109/ICCNC.2019.8685577

Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D., & Mohaisen, A. (2019). Exploring the Attack Surface of Blockchain: A Systematic Overview. 1–30. http://arxiv.org/abs/1904.03487

Saad, M., Thai, M. T., & Mohaisen, A. (2018). POSTER: Deterring DDoS attacks on blockchain-based cryptocurrencies through mempool optimization. ASIACCS 2018 - Proceedings of the 2018 ACM Asia Conference on Computer and Communications Security, 809–811. https://doi.org/10.1145/3196494.3201584

Seang, S., & Torre, D. (2018). Proof of Work and Proof of Stake consensus protocols: a blockchain application for local complementary currencies. 1–21. https://gdre-scpo-aix.sciencesconf.org/195470/document

Silver, C. (2020, February 14). Council Post: How The Transparency Of Blockchain Drives Value. https://www.forbes.com/sites/forbestechcouncil/2020/02/14/how-the-transparency-of-blockchain-drives-value/#5a86b19831a6

Solat, S., & Potop-butucaru, M. (2017). ZeroBlock : Timestamp-Free Prevention of Block-Withholding Attack in Bitcoin.

Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K. K. R. (2019). A systematic literature review of blockchain cyber security. Digital Communications and Networks, June 2018. https://doi.org/10.1016/j.dcan.2019.01.005

Tuncer, D., Koch, R., Wg, I., Conference, I., & Hutchison, D. (2017). Security of Networks and Services in an All-Connected World. http://www.springer.com/series/7411

Wang, H., Wang, Y., Cao, Z., Li, Z., & Xiong, G. (2019). An Overview of Blockchain Security (Vol. 2). Springer Singapore. https://doi.org/10.1007/978-981-13-6621-5

Xing, Q., Wang, B., & Wang, X. (2017). BGPCoin. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security - CCS '17, 1, 2591–2593. https://doi.org/10.1145/3133956.3138828

Zhang, R., Xue, R., & Liu, L. (2019). Security and privacy on blockchain. ACM Computing Surveys, 52(3). https://doi.org/10.1145/3316481