Index

List of Tables

List of Figures

Acronyms

DNS Domain Name System

DNS Domain Name System

Abstract

Blockchain has acquired popularity all over the world in a short period due to its distributed data management solution. Blockchain has provided security and data integrity with the intervention of the third party. One of the prominent use of blockchain technology is as a cryptocurrency. People are using cryptocurrency for transferring money, but it has also attracted hacker from all over the world. Attackers are targeting blockchain projects because of high investments. Since its early period of blockchain, there has been a series of attacks on the blockchain frame. In order to make understanding easy, the report contains a description of types of the network. In order to take a step towards solving this issue, the primary purpose of this report is to give detail about blockchain technology, how it is vulnerable to various kind of attack from the adversary. Public and private blockchain are detailed with their pros and cons. Apart from that, some non-technical risks are also discussed. This report also gives insights about some attacks on blockchain projects.

Keywords: *Blockchain Technology - Attacks - Risk - Prevention*

Chapter 1

Introduction

Blockchain facilitates to transfer value without the need for an intermediate party. Examples of such values are information, contracts, assets, identity. This technology gives cryptographically secure and decentralized mechanism that removes the need for management from a single entity. Blockchain technology is building block for the cryptocurrencies such as Bitcoin and Ethereum. It is efficiently shared, trusted, and secure ledger of various transactions.

The traditional approach for payment methods and storage purposes are in a centralized manner. Trusted third party is required for electronic banking transaction. The intervention of the third entity makes transaction slower and expensive, and even high cost is needed to make an irreversible transaction. To tackle this issue, a system required, which has unique features such as publicly available, free from the inference of the third party, irreversibility and secure. In October 2008, Satoshi Nakamoto published for peer-to-peer distributed technology which can fulfil all these requirements preciously. It uses cryptographic proof rather than a trusted third party, which enable two or more entities to participate directly. It enables to make transactions publicly available to read, which also hides the identity of a specific user. This advanced technology is secure as far as a single entity or organization does not control more than 50% of network [1]. Immutability of ledger can be useful for saving data for a more extended period without risk of tamper. According to some experts, this technology has the potential to change the future of many industries.

Blockchain has received popular all over the world in a short period. Researches are going on to use the benefits of blockchain in various field. However, like other technologies, blockchain is also vulnerable to threats and attacks from the adversary. As a result of that, researches for making blockchain immune to the attacks also started.

1.1 Motivation

Myriads of advantages have made blockchain one of omnipresent technology in recent time. However, the number of threats and attacks on this technology are increased. It has also attracted hackers to steal value and data, and because of that, many hacker's ground and attacker are finding new ways to find loopholes in the implementation of blockchain. In the past, they have even succeeded in many attempts, and users and organization have lost sensitive information and value worth of tremendous money.

Famous cryptocurrency Verge has been a victim of cyber attacks for two times. The first attack was during April 2018, at that time attackers stolen digital coin worth of more than $1.1 million. In May 2018, verge faced the same problem and lost around $1.75 million [2]. Just Dice was one of the most popular gambling platforms during the year 2013. Authorities announced that some stupid mistakes cost them for $1,21,000 approximately 1,300 BTC at that time [3]. During November 2012, trojan horse virus was installed on user PCs, which resulted in the loss of 3,457 Bitcoins. Another blockchain technology, MyBitcoin lost almost $2 million on 8^{th} August 2011 [4].

Apart from that, a blockchain start-up, The Backdoor, hacked its own wallet to save own users from possible attacks from attackers. Experts say that these attacks could have avoided with proper planning and preventive measure. Considering above mentioned losses and what happened with The Backdoor, it becomes vital to analyze potential attacks on blockchain framework. Analysis and adaption of preventive measure of such attacks and risk are also paramount.

1.2 Objective

To give a lucid explanation of centralized, decentralized and distributed system, so that it becomes easy to understand important of blockchain and reason behind its popularity. This report also aims to explain the working and important features of blockchain. Types of blockchain, such as public blockchain and private blockchain, are also detailed.

A core objective of this report is to analyze various attacks, risk, issues and their prevention measure for the distributed ledger technology called Blockchain. It also aims to provide insights into examples, in which blockchain technology has been a victim of the malicious intention of attackers.

1.3 Applications

Cryptocurrency

Omnipresent digital currency mechanism facilitated by Blockchain works automatically, it also facilitates a real-time, time-efficient transaction which might be next to impossible in traditional database system [5, 6]. Use of cryptocurrency removes the requirement of the third party, which makes the whole system fast and reliable. It also enables banks to progress payment speedily and more preciously while reducing resource requirements. Address of each node is also a cryptographic hash, which can hide the identity of a particular node. Various feathers provided by Blockchain makes it next-generation business process development.

Supply Chain Use

Suppliers can use blockchain for tracking products from the origin of the raw materials to the final products. Which will not only enables suppliers and manufacturers to verify the authenticity of the product, but also it will increase the trust of consumers for product and brand.

Health Care

Health care service providers can make the best use of blockchain, for securely saving data of their patients, types of equipment. Whenever a patient's record is generated, it can be digitally saved on the blockchain, which also provides proof and trust to the patients that record would not be altered in the nearby future. Furthermore, encoding can be used before saving record directly on the blockchain, which will intend to provide a level of security to any specific user.

For Voting System

Use of blockchain in the voting system has the potential to remove the lurking risk of fraud in the voting process. During November 2018 in West Virginia, such voting system was tested even [7]. In which, each vote can be considered as a block, making them infeasible to be altered. It can also bring transparency in the voting system, with that it can also provide the facility of the instant result.

1.4 Report Outline

In chapter 2, the background of the problem is described, which includes types of system, working and features of blockchain with possible diagram. Types of blockchain, such as private and public, are also explored. Chapter 3 gives insights for possible attacks on blockchain and its preventive measure. Some non-technical risks are also explored.

Chapter 2

Background and Literature Survey

2.1 Types of System

Every system can be divided into three categories. First, centralized. Second, Decentralized and third is Distributed. Differences in the system can affect every whoever is using it [8]. Simultaneous use of these three categories is not possible. Hence, organizations and institutions need to choose out of available option. While deciding, which system to use, pros and cons of each system should be considered. With history's perspective, a centralized system is more prominent. But the centralized system has its disadvantages which can be overcome by a decentralized or distributed system. Below detail explanation of each system is given with its potential advantages and disadvantages.

2.1.1 Centralized Framework

Centralized system is more easy to define, implement and more intuitive. The centralized system uses typical client/server architecture, where an unlimited number of client-side nodes can communicate with one server-side node. Every client nodes are connect to server node, so server node can be considered as central node, and central node is responsible for working as storage from where every client can access their information. Wikipedia, IBM are centralized systems. In which, user can search for a specific query, and that query will be resolved by server lying at possibly any corner of the world.

Advantages

1. Quick, easy deployment and quick development
2. Easy maintenance of system as whole
3. Feasible to control data from central entity
4. Cost effective
5. Quick update

Disadvantages

1. Network connectivity is a key factor - Chances of system failure is higher, due to dependency on single server
2. Longer access time for nodes residing at far points
3. Difficult Server Maintenance because of only one server

2.1.2 Decentralized Framework

In this type of system, multiple central entities are available rather than single central entities, and these central entities are also connected to each other. Every central entity also stores an own copy of data. Presence of centralized still makes still vulnerable to an accident as a centralized one. However, the architecture of the decentralized system adds robustness, because even if the central entity fails, the rest of the central entities still continue to work. It means, it allows the system administrator to repair one central node, while the system itself continues its work, with limitation on performance and data availability to some extent.

Advantages

1. Access time is faster than centralized system
2. High fault tolerance
3. More flexible and diverse system
4. Scalability is higher than centralized

5. Easy evolution

Disadvantages

1. Security and privacy risk
2. Higher maintenance cost

2.1.3 Distributed Framework

The distributed system removes the need for a central entity, which ultimately rejects centralization. Each and user have equal access. However, access rights can be altered as when required. Blockchain and the internet are a well-known example of a distributed system. It is free from independent failure. Apart from that, it also allows the user to define ownership of data. Resources are distributed among users that lead to improved efficiency of the network. Because of the benefits it provides, the distributed framework is changing industry drastically.

Advantages

1. Transparency
2. Scalable
3. Easy evolution
4. Extremely high fault tolerance

Disadvantages

1. Difficult to implement
2. Higher maintenance cost

2.2 Blockchain Technology

Blockchain is a chain of digital blocks containing various data and information. Once a block is connected to the chain, it can never be changed again, and it will be publicly available to read. For connecting the new block to the chain, blockchain uses the hash value of the previous block and new block. Digital blocks contain information of hash of the previous block, time and information which is to be added, etc. That is quite groundbreaking due to its avails facility for keeping track of medical records, full supply records and transaction records, etc. Some important terminologies are explained below.

Nonce

Blockchain allows the only specific type of hash values. For example, the first ten digits should be zero only. It is not always the case that the hash value will have ten-digit in starting. In order to, meet up this requirement while finding available signature data in the string needs to be changed continuously. Moreover, hash functions are designed in such a way that only a trivial change in a string can lead to the complete different hash value. So, a small special piece of data is added in the string to get an acceptable hash value. That piece of data is known as a nonce.

Mining Process and Miners

The process of finding nonce is called mining. The entity which continuously works to find such nonces are known as miners. Methods that miners use can also be related to trial and error method. Miners use their computation power for finding an acceptable signature. Acceptable signature is expected output from any miner. Large computational power increases the possibility of finding out proper nonce in lesser time. In the case of publicly available blockchain, any user can work as a miner by using blockchain specific application. Process, in which, miners compete to get signature and get a reward for success is also known as Proof-of-Work [1]. The second method for choosing miner is called Proof-of-Stack. In Proof-of-Stack selection of miner depends on the cryptocurrency miner posses, rather than computational power which is used in Proof-of-Work [9]. Other popular consensus algorithms are Practical Byzantine fault tolerance (PBFT), Proof-of-Reputation [9].

How Block is Added to ledger?

According to Fig 2.1, whenever new data is to be added in blockchain, it is added into the imaginary pool of unverified data. Miners who have to participate in the mining process can access those data from the pool. Once miners get enough information that can create one block, they fetch data from the pool and start mining procedure as explained in section 2.2. As soon as

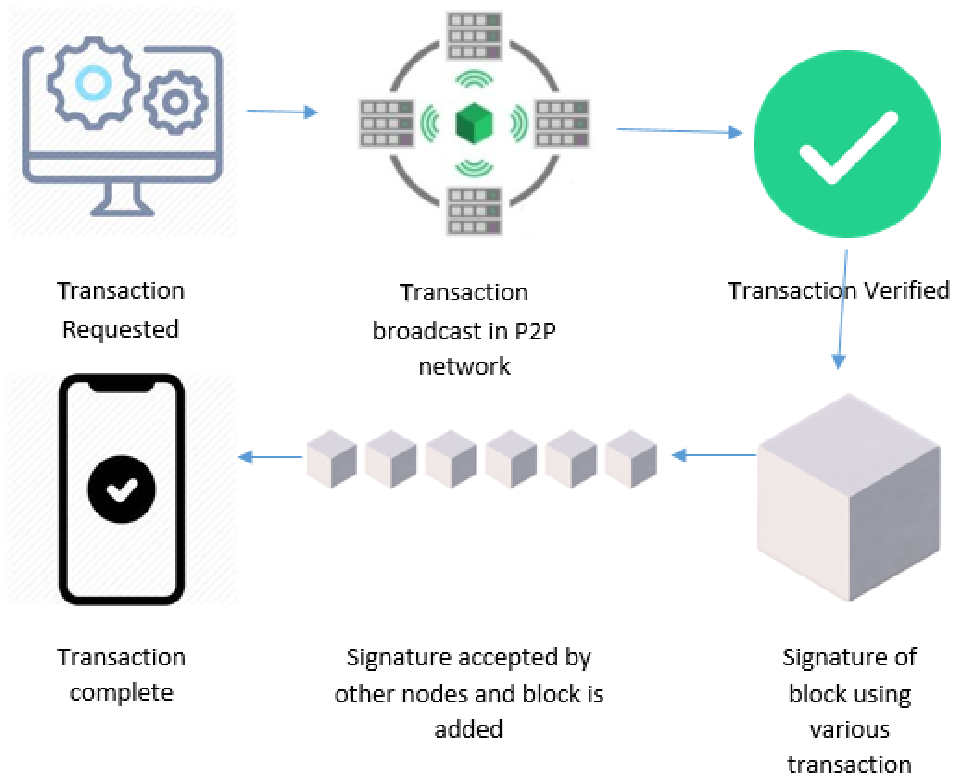
Transaction Requested
Transaction broadcast in P2P network
Transaction Verified
Signature of block using various transaction
Signature accepted by other nodes and block is added
Transaction complete

Figure 2.1: Working of blockchain

miner find an acceptable signature, it broadcast that signature in the system. Agreement from the predefined percentage of a node is required. Once that many nodes agree for a new block, a new block is added to the ledger. Afterwards, the block becomes immutable.

2.3 Features of Blockchain Technology

2.3.1 Robustness

Myriads of computers all around the world keep own copy of the ledger, and availability of duplicate copies makes Blockchain robust to the failure of single (or a few) node [1]. Unavailability or instability of node doesn't stop the whole system from working, because ledger still exists in other nodes. Alteration of data at one node is infeasible; it requires agreement or change in data on at least 50% of the node.

2.3.2 Censorship-Resistance

Absence of a single entity which manipulates a blockchain that is paramount feature of decentralized network. In a centralized approach, one authority has access to whole database, and it can change database as and when required [1]. For an example, while doing bank transaction, third party is always involved. On other hand, blockchain abolish interference of centralized authority, which facilitates to do transaction directly between two parties.

2.3.3 Transparency

Each and every change in ledge also goes through every participants. Updates in database are reflected in every node, so that new information is available in trivial time. It means each node has knowledge about the data residing at other node. Data is also consistent with every node, it provides transparency to the system [1].

2.3.4 Irreversibility

Every transaction of ledger in blockchain, defines next transaction. In other word, every transaction contains hash value of previous transaction. It means that every block of chain is connected. So, for changing one block of ledger, all the previous transaction requires changes, that is infeasible task for today's computer. That characteristic makes blockchain irreversible and secure against potential threat.

2.3.5 Disaster Recovery

Synchronized storage of data at various node improves fault-tolerance and reliability of blockchain. Every node has a access to create data and store ledger of blockchain, but it comes the cost redundancy [6, 10]. Moreover, attack on individual node can't cause destruction to the whole system [11].

2.4 Types of Blockchain

On the basis of who can assess and control blockchain, this technology has two types of mechanism. First is permissionless blockchain is open for public use, whereas second one is permissioned blockchain which allows only limited number of users. Description and example of both type is explained below.

2.4.1 Permissionless Blockchain

Permissionless Blockchain is also known as public Blockchain. Whole idea differs from the previous type. Any computer, with adequate technological requirements mandated by network,can participate as a minor. As name suggests, no other personal identity or machine authorization required to play a role of minor. It allows anyone to read and participate in system. When it is used as a part of cryptocurrency, at that time, having cryptocurrency is enough allow any user to transact digital money. This model is almost resembles basic idea of blockchain technology given by Satoshi Nakamoto [1]. On other hand, scalability and privacy issues are the drawbacks of public blockchain. To conclude, any entity can participate for transaction, and that can result into the privacy breach. Bitcoin and Ethereum are examples of permissionless blochain technology.

2.4.2 Permissioned Blockchain

Blockchain was original developed as publicly available and free system, but permissioned blockchain is exactly contrasting. Permission from owner is required to take part in blockchain. It gives control in owner's hand, it also means that one entity can manipulate whole system. That right of possession allows authorities to do whatever want to do with system, and also enables to impose various access rights to other users. For an example, owner can restrict some node from reading information. Even validation procedure is done by only selected entities. That makes this model faster and scalable than public blockchain. As an epitome, USA based supermarket company Walmart is designing permissioned blockchain to track fruits and vegetables. On the top of it, some information regarding products will be publicly available. Moreover, private blockchain is becoming popular in industries such as supermarkets, agriculture and transportation etc.

Chapter 3

Cybersecurity Attacks, Risk and Prevention

3.1 Types of Attacks and Prevention Measure

Attackers have stolen \$1 billion from cryptocurrency exchanges and various other platform [12]. It becomes vital to analyse such potential attacks which have affected users and validation nodes all over the world. Different methodology can be used for damaging blockchain, and various preventive measures are required to thwart effect of malicious attack [13].

3.1.1 Phishing

Phishing is defined as malicious attempt to extracting information from users [14]. It includes sensitive information such as bank details, username, password, etc. In short, phishing is stealing confidential data by masquerading attackers as a trusted party. Phishing breaks confidentiality of information [15]. Email spoofing and messaging are prominent ways to expose any computer to this attack. For implementation of phishing, attackers mostly disguise themselves as a representative of reputed firm. In addition to that, attackers makes their own website or application by a name trivially different from the original one. By the use of email or message, address of this platform is sent to potential victim. For an example, institute called Block.one which developed EOS.IO blockchain during the 2018, has been the victim of phishing attack [14]. Phishing group sent email with the intention of stealing wallet key. Unfortunately, attack was successful.

Clone phishing is a type of attack in which duplicate webpage with also most resembling, or webpage with approximately same is made [15, 16]. Targeted phishing one of the prominent type of attack. It includes aiming at owners of wallets, key person of companies, and owner of cryptocurrency [17, 15]. Duplicate cryptocurrency purses uses forgery purse, in which applications related to cryptocurrency is published on well-known application providing platform. Then that malicious demands for the private key and purse password [15].

Electrum Bitcoin

Electrum bitcoin wallet has been victim of phishing attack. From December 2018 to April 2019, Electrum bitcoin wallet user lost almost $4 million which is as equal as around 771 BTC for the month of April of 2019 [18]. Research done by Malwarebytes Labs, attackers successfully tricked wallet owners to download fraudulent version of wallet.

How to Protect System From Phishing ?

Modern methods for protecting blockchain from phishing attack is related can be derived by the use of machine learning and artificial intelligence [13, 15]. To discover phishing sites, large number of algorithms are being discovered.

1. One of the solution is find alternative of DNS, as an epitome, ENS (the Ethereum name Service) [15].

2. For the avoidance of attack on social networking sites, clone solution is to track activity on corporate pages and community pages [15].

3. Surveillance of site traffic, avoiding risky transaction and investments come under the ways to protecting system phishing.

4. Verification of each sender's and receiver's address each time

5. It is advisable not to open suspicious link and not to download unknown attachments

6. Authentication of SSL certificate before using any service

7. Adapting two step verification process

8. Avoidance of public Wi-Fi

3.1.2 51% attack

Satoshi Nakamoto mentioned possible security attack on the blockchain by dishonest note [1]. For adding a block of unconfirmed transactions in blockchain ledger, mining node needs to solve complex problems which requires high computation power. Still by controlling more than half of the blockchain framework, attacker do harm to the framework. If more than 50% of network's mining power agree on wrong information, then incorrect information is considered as truth, and it becomes eligible to be added into a ledger. In other word, one entity control more than the half of system, then only that entity is sufficient to decide whether to allow transaction or not. Moreover, entity will have power to halt other transaction being added to the system. In nutshell, one entity can monopolise whole blockchain framework. Though 51% attack can give control to the one entity, alteration of early written block is still infeasible task. Reason behind this is attacker would need to change whole chain of block which is joined via hash function. If 51% attack is considered as a controlling framework without taking consideration of fraction of network which is under control, then 51% attack is also possible for less than 50% of mining power. But chances of getting success decreases. That security flaw also lies in cryptocurrencies such as Ethereal, Bitcoin Gold, Monacoin, Verge, and even gone through such attack ,and almost $20 million where stolen because of this type of attack during the during the period of 2016-17 [12, 19].

Ghash.IO

Ghash.IO operated during the year 2013-2016. By mining bitcoin worth of $200 million during its first year, Ghash.IO show cased its tremendous mining power [20]. Because of this excessive hashrate, Ghash.IO was in controversy during year 2014. It's mining power crossed the 50% hashrate of whole bitcoin, but then after Ghash.IO declared that it will exceed than 40.00% [20].

Krypton Framework

Ethereum Krypton blockchain also suffered from 51% attack. Attackers took two approach to damage system. First was overpowering the framework with at least 50% of hashing power, because of that they were able to roll back transaction and spend coins twice. Attackers also launched DDoS attack on Krypton's biggest mining pool, ensuring that the network was weak the time of attack. Though amount which was stolen was around $4,000 only, attack on Krypton Framework can't be ignored [21]. This attack also comes under the category of double-spending and DDoS.

Bitcoin Gold

According to the experts, total $18 million was stolen by combination of both double-spending attack and 51% attack [22]. Attackers used Bitcoin gold for the exchange of other coin, then they withdrew. Then again they used coin from wallet, means double-spending.

Protection of Blockchain Framework From 51% Attack

To counter this attack, one way is to change the number of confirmations required to confirm transaction [23]. Bitcoin and Krypton implemented this way in the past to get rid from 51% attack.

1. Use of **delayed Proof-of-Work (dPoW)** which is updated consensus algorithm [24]. In delayed Proof-of-Work, "delayed function" penalizes miner who might be preparing for such an attack. According to co-Founder of Horizen Rob Viglione, a delay function poses excessive cost, a 10x cost, which can make prohibitively expensive.

3.1.3 DNS Redirection

In order to steal sensitive information username, id and password. Most notorious way to do so is via DNS redirection. DNS redirection is also known as DNS hijacking. As shown in Fig 3.1, this attack is performed by sending wrong IP address to the user's computer, when computer tries to resolve URL. Because of manipulated IP address, user will be forced to visit website other than expected. That website might resembles as the authentic one, due to that it is very likely that user will enter sensitive information such as username, password, bank details, etc. DNS redirection is one type of technical phishing [15].

BlackWallet.co

On 13^{th} January of 2018, BlackWallet.co suffered from DNS Redirection attack. Adversaries redirected, the DNS entry of the BlackWallet.co domain, to a server they operated [25]. As a result of that users were logging in malicious server, then attackers used that credentials to steal

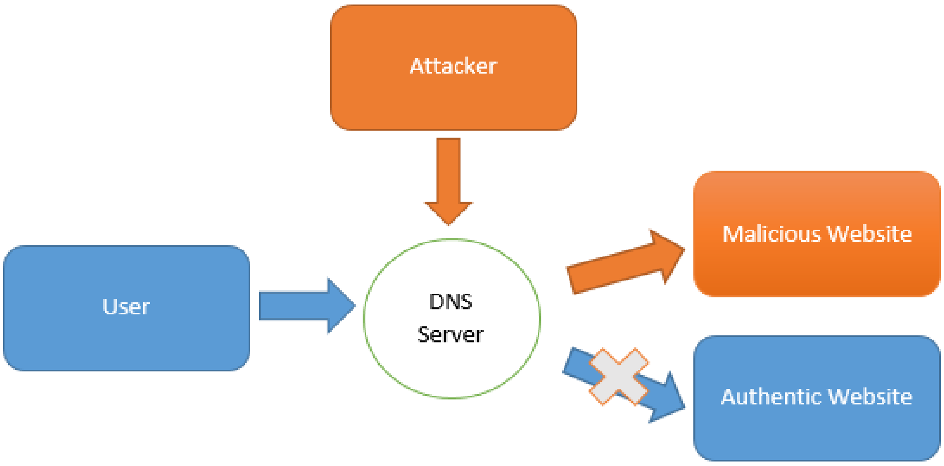

Figure 3.1: DNS attack

money from authentic wallet. Users lost around 6,70,000 Lumens which is one of the top ten cryptocurrency, contemporary worth of $0.4 million.

Caution Against DNS Attack

It is very difficult for normal user to interpret and confirm whether organization's DNS is hijacked or not, but as a active user, everyone can keep eyes on changes in website, application and unnecessary pop-up.

1. Whenever user access any website, user can verify certificate. It is preferable that not to continue just because URL is correct.

2. Organizations should post security related alert message on website to make users aware about potential threat to the system.

3.1.4 DoS Attack

Traditional domain name resolution method uses hierarchical resolution process and central server plays important role. That makes system most vulnerable to attack such DoS. In DoS (Denial of Service), adversary tries make network, framework or system unavailable for indefinitely with the intention of disruption in system [26]. In most of the cases, this attack is done by doing excessive number of requests to the sytem, which can prevent query or request from authentic users [27]. Well-known example of this attack is sending request to web server, which might result into the congestion in network and repudiation of request from some user. Such attack has a potential to damage blockchain framework also. For an example, a scenario in which nodes with malicious intention is part of network also. Now, malicious node can create unnecessary traffic in system. But it is very rare and difficult task in blockchain because of blockchain's dynamic topology [28]. In some cases, attackers use more than one node to send request in order do distributed attack, which is also known as DDoS [9].

Step Against DoS Attack

Possibility of DoS can't be removed completely. However, there are some possible ways which can be used to curb DoS attack. Security of blockchain lies in the hashfunction with which blocks are related. One way to make blockchain secure is to reduce the size of block, but as size of block decreases number of transaction contained by single block also decreases. For security purpose, reducing the size of block is preferable. More number of block also increases transaction fees, that can be used to prevent DoS attack at some extent. Because while generating undesirable traffic on network, malicious nodes need to pay fees for each transaction. Size of block is parameters of the blockchain framework, by changing other parameters of the blockchain DoS attack can be controlled. Actually that method is trial and error method, researches are going on to find optimal result [28]. Penalizing nodes that sends lots of duplicate, expired, incorrect signature, so those nodes would get banned. Ultimately, DoS attack is inevitable, but certainly ,by proper care chances of success can be reduced at large extent.

3.1.5 Sybil Attacks

Sybil attack is kind of attack in which one person or entities tries to control whole network by pretending to many users at same time, this can be done by creating multiple account, nodes or computers [28]. In simple language, it can be compared to making multiple social media accounts. For the crytocurrency, relevant example for this attack is to make multiple nodes of blockchain network. One way to exploit sybil attack is that attacker can always refuse to broadcast and transaction from any one the node, as a result of that it may isolate node from network. In fact, large-scale sybil attacks, where attackers tries control most of the network is known as 51% attack. 51% is explained in section 3.1.2.

3.1.6 Eclipse Attack

For an example, if given node is dependent on x number of node for its own view of distributed ledger. However, if adversary any how can manage to make the node to choose those x number of nodes from his/her malicious nodes alone, then he can eclipse the correct view of distributed ledger. In other words, attackers will control all the nodes to which given specific node is connect in given network, then attacker will successfully shows wrong ledger to the node, which will waste computation power of that peer.

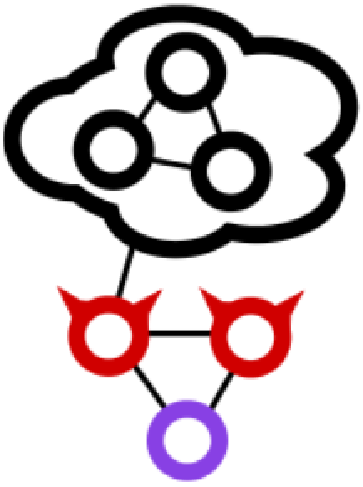

Figure 3.2: Eclipse attack

Fig 3.2, depicts the possible scenario for eclipse attack. In figure block nodes shows legitimate blockchain network. Purple color shows targeted node, and red color denotes nodes which are controlled by attackers. From the Fig 3.2, it is obvious that attacker has isolated victim node, and it may lead to display manipulated ledger to the victim node.

3.1.7 Selfish Mining Attack

Blockchain's consensus algorithm allows only longest chain to be the trusted and correct ledger. It might reject correct ledger, if at all, it would be shorter than a corrupted one. This feature lead to the vulnerability in blockchain framework. Attacker might create its own fraudulent ledger, once it get longer than the correct, at least by one or two block, attacker will publish it, all over the network. Because of design of consensus algorithm, other node will accept that corrupted ledger as a authentic one. Just before publishing ledger on network, if attacker will do any transaction, then risk of double-spending is also there.

3.2 Security Risk

Popularity and execution of any technology in industry relies on the effective risk management. Risk management becomes vital when Technology is core of the company. Blockchain is not an exception from them. Blockchain should be implemented correctly and effectively, so that it fulfills organization intention of data security, privacy, confidentiality and time efficient solutions.

3.2.1 Standard Risks

Organizations are vulnerable to the some standard risk even while using blockchain Technology. Such issues should be addressed for the efficient and successful use of blockchain [29]. Below details about such typical risks are mentioned.

Planning Risk

Resources, used for the implementation of blockchain, can be hindrance for the product and services being delivered from the platform of blockchain. In addition to that, organization should be careful while deciding which entities can participate in blockchain network. Because number of participation can create impact on the efficiency and security of blockchain.

Reputational

Most of the fintech applications of other technology are not the core of organization, whereas blockchain is heart for expansion and survival of institute. Failure of blockchain might leads to shut down of whole industry, and bad consumer experience.

Information Security Risk

Firstly, as explained in 3.1, blockchain is vulnerable to various cyberattacks such as 51% attack, phishing, DNS hijacking, etc. 51% attack is mostly dangerous for permissioned system. Secondly, user details such log in credentials, password is susceptible for attackers, who intent to take over user's account for malicious purpose.

Technical Limitations

Main idea of blockchain lies in storing redundant data at more one node. For the continuous updation is mandatory, but for that complex network among participants. It requires large scale network with huge computation power [11].

Regulatory

In present, there is no regulatory compulsion for blockchain. But in the future, regulatory risk related is possible, such as whether to include international transaction or not, privacy and data protection concern for international transaction.

Operational and IT

Current rule, regulations, procedure, law and policies needs to be changed to adapt new business methodology. In addition to that, there remains technological concern for catch up the demand of scalability and speed.

3.2.2 Value Transfer Risks

Elimination of third party exposes communicating nodes to new risks, earlier these risks were controlled by trusted third party. In other word, there remains risk while transferring value from one node to another node. These value can be information, assets, and identity.

Consensus Protocol

The transfer of value between node occurs by agreement from other nodes which use consensus protocol, and Proof-of-Stack and Proof-of-Work are consensus algorithms. Proof-of-Stack is consensus algorithm with the advantage of energy efficiency and security over Proof-of-Work [9]. Deficient consensus protocol can lead to the fatal result. For an example, in the case of Proof-of-Stack, there is a chances of problem called Nothing at Stack [30].

Data Confidentiality

In distributed ledger technology, to fulfill the demand of system, data or information needs to be shared all over the network. Doing so result into the loss of confidentiality from basic requirements CIA (Confidentiality, Integrity and Availability). Monitory the metadata can revel a lot about the type of activity and volume associated with the activity of any public address.

Key Management

Though mechanism of blockchain makes it next to impossible to alter the block, chances of theft is private key is always there. Once private is exposed to the adversary, he/she can extract money using public key. So, when it comes blockchain's private key, precious and proper management of key becomes mandatory.

Chapter 4

Conclusion

Table 4.1 shows which types of attacks can harm which component of blockchain framework. Presence of bullet shows the high possibility. For an example, DNS hijacking can effect Users, because as explained in section 3.1.3, user can be redirected to fallacious website.

Table 4.1: Relations Between Various Attacks and Component of Blockchain Framework

	Blockchain	**Miners**	**Mining Pools**	**Exchange**	**User**
DNS hijacking		●	●	●	●
DoS	●	●	●		
51% Attack	●	●			
Phishing		●	●	●	●
Eclipse Attack		●			●
Selfish Mining Attack	●	●	●		

References

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” *Cryptography Mailing list at https://metzdowd.com*, 03 2009.

[2] “Verge Falls Victim to 51% Attack, Again - CoinCentral.” `https://coincentral.com/verge-falls-victim-to-51-attack-again/`. [Online; accessed 13-October-2019].

[3] “Bitcoin Scams and Cryptocurrency Hacks List - BitcoinExchangeGuide.com.”

[4] “Remembering the 2011 MyBitcoin Hack Now Worth $1.8 Billion,” Aug. 2019.

[5] H. Wang, Y. Wang, Z. Cao, Z. Li, and G. Xiong, “An overview of blockchain security analysis,” in *Cyber Security* (X. Yun, W. Wen, B. Lang, H. Yan, L. Ding, J. Li, and Y. Zhou, eds.), (Singapore), pp. 55–72, Springer Singapore, 2019.

[6] G. Paul, P. Sarkar, and S. Mukherjee, “Towards a more democratic mining in bitcoins,” in *Information Systems Security* (A. Prakash and R. Shyamasundar, eds.), (Cham), pp. 185–203, Springer International Publishing, 2014.

[7] “Why security experts hate that “blockchain voting” will be used in the midterm elections - MIT Technology Review.” `https://www.technologyreview.com/s/611850/why-security-experts-hate-that-blockchain-voting-will-be-used-in-the-midterm-ele` [Online; accessed 13-October-2019].

[8] “Comparison - Centralized, Decentralized and Distributed Systems.” `https://www.geeksforgeeks.org/comparison-centralized-decentralized-and-distributed-systems/`, Dec. 2018. [Online; accessed 13-October-2019].

[9] M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang, and A. Mohaisen, “Exploring the Attack Surface of Blockchain: A Systematic Overview,” *arXiv:1904.03487 [cs]*, Apr. 2019. arXiv: 1904.03487.

[10] L. Wang and Y. Liu, “Exploring miner evolution in bitcoin network,” pp. 290–302, 03 2015.

[11] F. Dai, Y. Shi, N. Meng, L. Wei, and Z. Ye, “From bitcoin to cybersecurity: A comparative study of blockchain application and security issues,” in *2017 4th International Conference on Systems and Informatics (ICSAI)*, pp. 975–979, Nov 2017.

[12] A. Chandhok, “Top five blockchain security issues in 2019.” `https://ledgerops.com/blog/2019/03/28/top-five-blockchain-security-issues-in-2019`, 2019.

[13] "LedgerOps - 2018 Blockchain Threat Report.pdf(Shared)- Adobe Document Cloud." https://documentcloud.adobe.com/link/track?uri=urn:aaid:scds:US:eae0e5e7-d798-4854-b3fa-4dae1686eb3f, 2018. [Online; accessed 9-October-2019].

[14] Wikipedia contributors, "Phishing — Wikipedia, the free encyclopedia." https://en.wikipedia.org/w/index.php?title=Phishing&oldid=918612483, 2019. [Online; accessed 11-October-2019].

[15] A. A. Andryukhin, "Phishing Attacks and Preventions in Blockchain Based Projects," in *2019 International Conference on Engineering Technologies and Computer Science (EnT)*, pp. 15–19, Mar. 2019.

[16] "Phishing for cryptocurrencies: How Bitcoins are stolen." https://www.kaspersky.com/blog/crypto-phishing/20765/. [Online; accessed 8-October-2019].

[17] E. Pearson, C. L. Bethel, A. F. Jarosz, and M. E. Berman, ""to click or not to click is the question": Fraudulent url identification accuracy in a community sample," in *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pp. 659–664, Oct 2017.

[18] Y. B. Perez, "Behind the scenes: Electrum hackers steal $4m with Bitcoin phishing attacks." https://thenextweb.com/hardfork/2019/04/16/behind-the-scenes-electrum-hackers-steal-4m-with-bitcoin-phishing-attacks/, Apr. 2019. [Online; accessed 12-October-2019].

[19] "Learn Cryptography - 51% Attack." https://learncryptography.com/cryptocurrency/51-attack, abstract = Learn Cryptography is a resource to understand how and why the cryptographic systems they use everyday work to secure their communications and protect their privacy. [Online; accessed 8-October-2019].

[20] Wikipedia contributors, "Ghash.io — Wikipedia, the free encyclopedia." https://en.wikipedia.org/w/index.php?title=Ghash.io&oldid=901128807, 2019. [Online; accessed 12-October-2019].

[21] "Small Ethereum Clones Getting Attacked by Mysterious '51 Crew'." https://news.bitcoin.com/ethereum-clones-susceptible-51-attacks/, Sept. 2016.

[22] FMF, "A 51% Attack Happened- How Did it Happen to Bitcoin Gold?." https://medium.com/formosa-financial/a-51-attack-happened-how-did-it-happen-to-bitcoin-gold-da131a8080a6, July 2018. [Online; accessed 12-October-2019].

[23] "What is a 51% Attack? (Blockchain)." https://thecoinoffering.com/learn/what-is-a-51-attack-blockchain/, Aug. 2018. [Online; accessed 13-October-2019].

[24] "A Solution to Crypto's 51% Attack? Fine Miners Before It Happens," Oct. 2018.

[25] "Blackwallet hacked, hackers stole $400,000 from users' accounts through DNS hijackingSecurity Affairs." https://securityaffairs.co/wordpress/67753/cyber-crime/blackwallet-hacked-dns-hijacking.html. [Online; accessed 13-October-2019].

[26] Z. Chao-yang, "DOS Attack Analysis and Study of New Measures to Prevent," in *2011 International Conference on Intelligence Science and Information Engineering*, (Wuhan, China), pp. 426–429, IEEE, Aug. 2011.

[27] R. S. Singh, A. Prasad, R. M. Moven, and H. K. Deva Sarma, "Denial of service attack in wireless data network: A survey," in *2017 Devices for Integrated Circuit (DevIC)*, (Kalyani, India), pp. 354–359, IEEE, Mar. 2017.

[28] E. Zaghloul, "Beginners Guide on Blockchain Security Attacks Part 1 — Network." `https://medium.com/zkcapital/beginners-guide-on-blockchain-security-attacks-part-1-network-ca4e74435723`, July 2018. [Online; accessed 12-October-2019].

[29] P. Santhana, "Blockchain Security Risks for Financial Organizations | Deloitte US." `https://www2.deloitte.com/us/en/pages/risk/articles/blockchain-security-risks.html`, 2017. [Online; accessed 12-October-2019].

[30] Wikipedia contributors, "Proof of stake — Wikipedia, the free encyclopedia." `https://en.wikipedia.org/w/index.php?title=Proof_of_stake&oldid=918026749`, 2019. [Online; accessed 12-October-2019].

Acknowledgement

I take this opportunity to express my deep sense of gratitude and indebtedness to my seminar guide, Dr. Sankita J Patel , my seminar coordinator Mr. R. P. Gohil and H.O.D, Dr. M. A. Zaveri from Computer Engineering Department, SVNIT Surat for their valuable guidance, useful feedback and co-operation with kind and encouraging attitude towards this seminar.