Block Chain Security: Attacks & Issues

Suhel Sayfuddin Khan , Mohd. Arbaaz Riyaaz Ahmed Khan

Project Guide: **Prof. Nitin**

ASM'S INSTITUTE OF MANAGEMENT ANDCOMPUTER STUDIES

ABSTRACT

Blockchain is a technology which allows the decentralization of data.The data stored in a manner that there is no single central control to modify the data. Bitcoin is the first successful Blockchain application implemented with the concept known as cryptocurrency.Blockchain allows a transaction flow without the interference of any bank or government. Now in the last couple of years, the adoption of Blockchain has increased across multiple industry for different use cases and deployments.

However, Blockchain security is still the weakest part of it & needs a better improvement. Therefore, the purpose of this study is to make a review of the Blockchain security issues using the past published literature.

This Research conducts a review based on articles and research papers to find possible problem solving actions that gives an overall view of existing security threats and their respective impacts on Blockchain. This research starts with an overview on Blockchain Security and brief discussion on fellow attacks and issues.

KEYWORDS

Blockchain technology, Security, Attacks,Prevention.

INTRODUCTION

Blockchain is a list of records called blocks; which store data publicly and in chronological order. The information in BLockchain is encrypted using cryptography to ensure that the privacy of the user is maintained and data cannot be modified.Information on a Blockchain network is not administrated by a centralized authority, unlike modern financial institutions.As long as you have access to the network, you have access to the data within the Blockchain. As a participant in the Blockchain network, you will have the same copy of the ledger, which all other participants have in the following Blockchain.

Even if one node on one particular participant machine gets corrupted, the other participants will be notified immediately, and they can amend it as soon as possible.

Because blockchain is in demand (and because it's generally used in transactional settings) and with this increase in popularity, a number of blockchain security issues have raised that it has become an fascinating target for hackers and other cyber criminals.

In spite of this, there exists following issues and challenges with respect to security.

the attack space includes a range of Wallet attacks (i.e., client-side security), Network attacks (such as phishing attack, Vulnerable Smart Contract) and mining attacks (such as 50%, block withholding, and bribery).

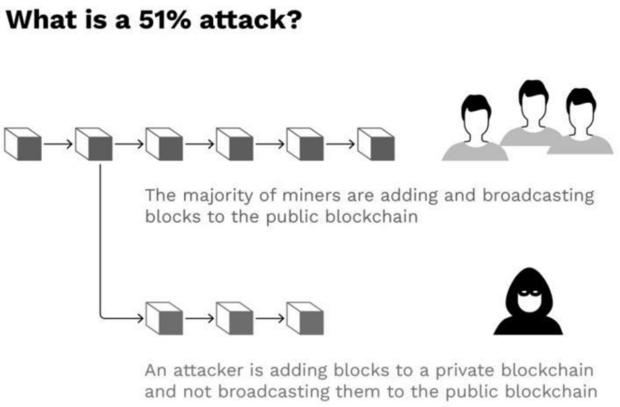
ANALYSIS

➢ Issues in Blockchain Securiuty (Attacks) :

✓ 51% Attacks

51% attack is an attack on a blockchain. Blockchain is a type of digital database in ledger form. Information is collected together in groups or blocks and this information is linked together to create a chain of data.In cryptocurrency trading, blockchain technology is used to note approved transfers of digital currencies and With Ethereum(a crypto currency coin) for example, "miners" can attempt to add blocks to the chain by solving mathematical problems with the help of a mining machine. These machines are fundamentally a network of computers.If miners manage in adding a block to the chain, they receive Ethereum in return.The speed at which all the mining machines within the network operate is the Ethereum hashrate.

A good hashrate can help gauge the health of the network.


What is a 51% attack?
The majority of miners are adding and broadcasting blocks to the public blockchain
An attacker is adding blocks to a private blockchain and not broadcasting them to the public blockchain

Steps how 51% attack make a start:

1. The entity or person that is interested in attacking the network would need to attain enough hash power to successfully mine blocks on a copy of the network's chain in secret.

2. This secret chain keeps going in parallel to theoriginal

A 51% attack occurs when one or more miners takes control of more than 50% of a network's mining power, computing power or hashrate.

If a 51 percent attack is successful, the miners have an essentially control over the network andcertain transactions that occur within it.

✓ Selfish Mining Attack

A selfish mining attack, also known as a block withholding attack.It describes a malicious attempt to discredit blockchain network integrity. Selfish mining attacks occur when an miner in a mining pool attempts to withhold a successfully validated block from being broadcast to the rest of the mining pool network.After the selfish miner withholds their successfully mined block from the rest of the mining pool group, they continue to mine the next block.Resulting in this the selfish miner having demonstrated more proof-of-work compared to other miners in the group.This allows the selfish miner to claim the block rewards also financial rewards while the rest of the network adopts their block solutions. There are two types of block selfish mining attacks:

1. first one is known as the Finney Attack which aims for financial gain when a double spend occurs.
2. And another one is to cause financial harm to a pool operator.

A selfish miner will maintain their own private chain, and publicly reveal it with a opportunity in order to obtain greater rewards that would normally be granted based on their actual contributions or Hashrate to the mining pool. It is possible for more than one miners in a mining pool to engage in selfish mining behavior during the mining process.

✓ **Phishing Attack**

Phishing is the fallacious attempt to obtain sensitive information such as usernames, passwords, and credit card details;
Phishing is often used for malicious reasons, by disguising as a truth full entity in an electronic communication.
Phishing is further categories as:

A. Social Engineering Schemes-
Fake ICO
Pyramids, Ponzi
Bloating
Clones
Social networking
Aimed phishing

B. Technical schemes-
DNS based
Hijacking
Malware Key
loggers

Best Practices

a) Prevention of 51% Attack

□ **50% Limit on a single miner**

The blockchain should ensure that not even a single miner or group of miners, controls less than or equal to 50% of the hashing power.
It would be difficult for a single miner or a group to attack the network by outbuilding the longest verified blockchain.
To perform the attack,an attacker has to own powerful hardware and requires massive energy. Also, an attacker shoud be lucky since the mining process will be random.

□ **Using Proof of Stake**

In a small blockchain network a single miner has majority to overcome the Blockchain. All the blockchain network that uses pow have to upgrade their equipment or devices regularly because of the policy of pow.

Failure to do so, may lead to them not receiving the block rewards, and they will fall behind other miners in the network.
To avoid the risk of a 51% attack, the blockchain can use Proof of Stake (PoS), whichis a more secure consensus than PoW.
In most cases, the PoS incentives are controlled by most affluent users unlikely to perform the attack.
However, blockchains have moved from this structure, and they prefer more decentralized alternatives such as Delegated-Proof-of-Stake(DPoS).

To avoid the risk of a 51% attack, the blockchain can use Proof of Stake (PoS), whichis a more secure consensus than PoW.
In most cases, the PoS incentives are controlled by most affluent users unlikely to perform the attack.
However, blockchains have moved from this structure, and they prefer more decentralized alternatives such as Delegated-Proof-of-Stake(DPoS).

□ **Strong network community**

When using the PoS or DPoS, a user with a minimal stake level in a network is voted a block validator.The validators are voted in by thecommunity.

In case of collusion to compromise the network, they are thrown out of the network bythe community.

This approach prevents the occurrence of a 51% attack.It is also effective in avoiding double-spending as the rules for the malicious validators are coded into the blockchain.

b) Selfish Mining Attack

Two possible best practices have been

suggested to intercept selfish mining attacks from occurring on blockchain networks.

The first practice is to randomly assign miners to branches of the blockchain when a fork occurs.

Another practice is to set threshold limits for mining pools on the network that would intercept selfish miners from gaining an important advantages over other miners operating on the network.

c) Phishing Attack

(1) Use bookmarks instead of links.
(2) The use of browsers with anti-phishing extension,the installation of anti-phishing soft the prohibition of clicking through links and downloading questionable attachments (3)Doing the authentication of the SSL certificate before using the services.
(4)Inform about phishing, launch off-line copies of crypto-wallets, use of two-factor authentication, complex passwords (minimum 14 symbols),refusal of public Wi-Fi, use of secure gateway.

d) Eclipse attack

If an attacker has access to adequet IP addresses then Nodes can be eclipsed.
The simplest way to avoid this is for a node to restrict internal connections and be calculated aboutany connections made with other nodes.

However this, can make it more difficult for new nodes to join a blockchain network.Beacause of the public and open-source nature of most blockchains, it is effortless for attackers to access their structural foundation in search of vulnerabilities to utilize.

Since structural changes are quite difficult to accept and apply midway through a blockchain network's lifecycle, the best method to ignore a cryptocurrency eclipse attack is to design the blockchain network's node configuration to counter eclipse attacks from the beginning.

- ✓ Random node selection:
- ✓ Deterministic node selection:
- ✓ Increased node connections:
- ✓ New node restrictions:

Conclusion

The blockchain technology is changing the IT industry. Blockchain can bring together Industries, Governments, and many Nations. Blockchain technology is widely acknowledged and highly evaluated due to its decentralized nature and peer-to- peer characteristics.

The main purpose of this research paper is to gather information on attacks on blockchain. Moreover, this paper discussed the various security issues, vulnerabilities, and attacks that slowdown the increased adoption of blockchain technology while exploring these challenges in a variety of aspects.

We also suggested some best practices.These practices may not be the best solution for the problem but can be used in such situations.

REFERENCE

i. 9Ibm (https://www.ibm.com/topics/blockchain-security),

ii. Ananda krishna, Blockchain security issues-a complete guide. 12 Feb 2022

iii. Rahul Venugopal, what is blockchain: features and Use case, 16 feb 2022

iv. Marie Jeanne Tuyisenge, "BLOCKCHAIN TECHNOLOGY SECURITY CONCERNS:LITERATURE REVIEW" june 2021.

v. Stackexchange (https://bitcoin.stackexchange.com/questions)

vi. Idrees, S.M.; Nowostawski, M.; Jameel, R.; Mourya, A.K. Security Aspects of Blockchain Technology Intended for Industrial Applications. Electronics 2021, 10,951

vii. Recent Trends in Blockchain for Information Systems ecurity and Privacy, Edited by Amit Kumar Tyagi and Ajith Abraham published 2022.

viii. Understanding a 51% Attack on the Blockchain by Ephraim Njoroge December15, 2021

ix. Marcel Deer; DEC 11, 2021 https://cointelegraph.com/explained/what- is-an-eclipse-attack#:~:text=In%20an%20eclipse%20attack%2C%20a,or%20to%20cause%20general%20disruption.

x. https://www.bitpanda.com/academy/en/lessons/what-is-a-51-attack-and-how-is-it-prevented.

xi. https://golden.com/wiki/Selfish_mining_attack-39PMNNA#

xii. /www.isprasopen.ru/2018/docs/Andryukhin.pdf

xiii. https://cointelegraph.com/explained/wh at-is-an-eclipse-attack#:~:text=In%20an%20eclipse%20attack%2C%20a,or%20to%20cause%20general%20disruption

xiv. https://www.section.io/engineering-education/understanding-the-51-attack-on-blockchain/

xv. https://golden.com/wiki/Selfish_mining_attack-39PMNNA#:~:text=A%20selfish%20mining%20attack%2C%20also,of%20the%20mining%20pool%20network

xvi. https://www.gemini.com/cryptopedia/eclipse-attacks-defense-bitcoin#section-how- to-prevent-a-cryptocurrency-eclipse-attack

xvii.