Borneo International Journal eISSN 2636-9826; Vol. 6 (1); 2023; 20-32
Published by *Majmuah Enterprise*
www.majmuah.com

Blockchain Threats: A Look into the Most Common Forms of Cryptocurrency Attacks

MUZDALINI BINTI MALIK and MOHAMAD FADLI BIN ZOLKIPLI
School of Computing, Universiti Utara Malaysia (UUM), 06010 Sintok, Kedah, MALAYSIA
Email: muzdalini@gmail.com, m.fadli.zolkipli@uum.edu.my| Tel: +60135840083, +60177247779 |

Received: February 19, 2023
Accepted: February 22, 2023
Online Published: March 01, 2023

Abstract

Blockchain technology provides a secure and reliable method for transactions and has become increasingly prevalent since the advent of cryptocurrencies. However, the use of cryptocurrencies has also led to a rise in blockchain-related threats and attacks. This paper aims to provide a comprehensive overview of the most common forms of cryptocurrency attacks and focusing their impact on assets, business and organization, and threat to the security and stability of the blockchain. This paper is to highlight the several types of attacks including 51% attacks, phishing frauds, malware and ransomware attacks, social engineering attacks, and more. This paper also analyzes the current and future efforts to mitigate these threats, including best practices to prevent from blockchain attacks and serves as a valuable resource for individuals and organizations looking to better understand about type of cryptocurrency attack and protect against the growing threat of cryptocurrency attacks.

Keywords: blockchain; cryptocurrency; attacks; threats

1. Introduction

Blockchain is a peer-to-peer network-based decentralised digital ledger of transactions (Hassan et al., 2020). The system employs cryptographic techniques to ensure that once a transaction is logged, it cannot be edited or erased. The data is structured into blocks, and each block is connected to the one before it, forming a chain of blocks that comprises the blockchain (Dryall, 2018). The principle of decentralisation and an efficient digital eco-system has led to the usage of Blockchain Technology in a variety of industries, including finance, commerce, and government services (Husna Zakaria et al., 2018). Blockchain technology becoming increasingly popular, and it is the primary technology used in cryptocurrencies.

Cryptocurrency is not controlled by any firm or institution, but rather by how it is generated and where it is mined (Naje et al., 2021). Such that, they are maintained by a network of people and computers on the blockchain. This enables safe and transparent transactions without the use of middlemen and reduces the possibility of fraud or intervention from centralised institutions. Some of the most well-known cryptocurrencies include Bitcoin, Ethereum, and Litecoin. Although cryptocurrency employs secure technologies, such as blockchain technology, it still faces threats, and studies reveal that there are numerous forms of cryptocurrency assaults. Due to their decentralised structure and use of complicated mathematical procedures, cryptocurrency and blockchain systems are vulnerable to different types of attacks.

The potential threats and security of Blockchain and cryptocurrencies have been the subject of active research in several different domains. Referring to some of the comments that have been made, there is a report from McAfee in which they also emphasize cryptocurrency exchanges as a very attractive target for attackers (Froehlich et al., 2021). In this paper, we introduce blockchain technology and its use in cryptocurrencies, as well as potential threats and attacks on blockchain and cryptocurrency. The remainder of this paper is arranged as follows: Section 2, overview on technology blockchain, blockchain threats and cryptocurrency attacks that are used in this strand of the research. Section 3, explore eight types of hacking attacks that occur against cryptocurrencies. Section 4 presents the Impact of Cryptocurrency Hacking Attacks. Section 5 discusses the prevention and mitigation of cryptocurrency hacking attacks to reduce and slow down or prevent the cryptocurrency hacking process. Further, Section 6. Finally, we conclude the paper in discussing attacks that are currently popular, effective ways to defend from attackers. Section 7, that presents our conclusion.

2. Overview of Blockchain and Cryptocurrency

Blockchain Technology

According to the (Naje et al., 2021), the Blockchain technology was proposed for the first time in the late 1980s and early 1990s. A sequence of signed data was used in 1991 to digitally sign papers in such a method that it was evident that neither of them had been combined. Blockchain is a public ledger that tracks internet transactions. It employs the decentralisation and cryptographic hashing concepts to create a transparent, transparent, and immutable digital asset. As a result, core technology is used in cryptocurrencies to assure cryptocurrency integrity by encrypting, verifying, and permanently preserving transactions. Researchers were drawn to Blockchain due to its potential qualities such as distributed ledger, immutability, decentralised systems, consensus, transparency greater security, speedier settlement, anonymity, cost-effectiveness, and non-third-party authentication. **Table 1** shows the key features and its description about the various advantages and the features of the blockchain technology (Anita & Vijayalakshmi, 2019).

Table 1: Blockchain Key Features and Its Description (Anita & Vijayalakshmi, 2019).

Key features	Description
Immutability	Nobody has the ability to alter Blockchain's distributed ledger.
Transparency	Each public address's transactions are transparent and secure to all Blockchain users.
Distributed ledger	A computerised system or database for keeping and recording transactions in different locations.
Consensus	A fault-tolerant technique and method of establishing consensus across all Blockchain members.
Anonymity	Blockchain transactions are untraceable, providing a better level of privacy.
Distributed ledger	Computer programs allow the transaction without third parties.

Hash functions, yet another cryptographic primitive, are used to chain blocks. An arbitrary-length message is converted by a hash function into a fixed-length hash output referred as a digital fingerprint or message digest. The hash function has the fascinating virtue of being collision-resistant, which means that no two separate messages will yield the same hash output. This attribute serves as the foundation for block chaining. The hash of the previous block header is included in the new block header when chaining a new block to the blockchain. Researcher explained how blocks are chained together to form a blockchain. **Figure 1** shows the chaining of blocks (Agbo et al., 2019).

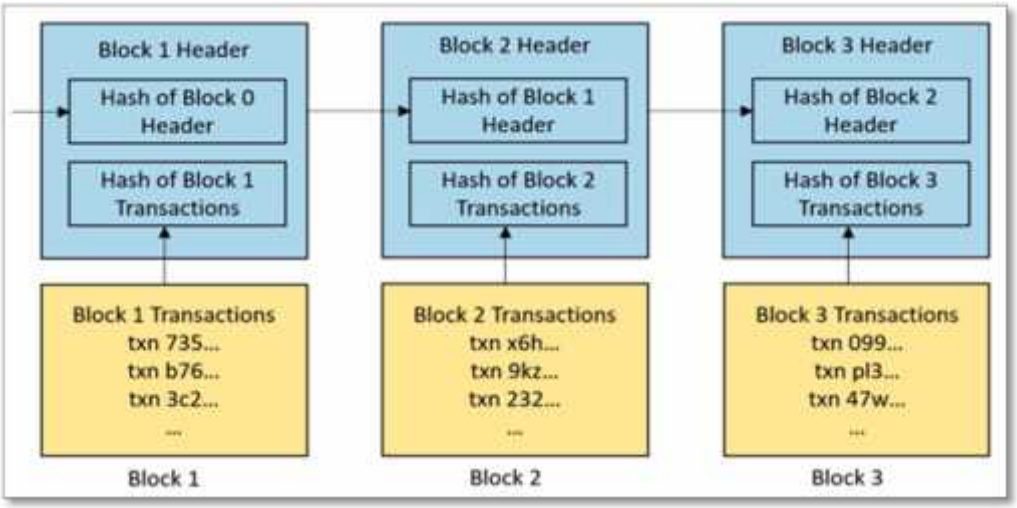

Figure 1: The Chaining of Blocks (Agbo et al., 2019).

Although Blockchain technology is seen as a safe technology and difficult to attack but there are still security problems in the Blockchain network. The study of blockchain incidents has been given in the form of an information system idea, using the theft of bitcoins from a cryptocurrency wallet as an example (Ishchukova et al., 2022).

Borneo International Journal eISSN 2636-9826; Vol. 6 (1); 2023; 20-32
Published by *Majmuah Enterprise*
www.majmuah.com

Blockchain Threats

While blockchain technology is secure and transparent, it is not immune to threats. Hacking, scalability, interoperability, regulation, privacy, and energy consumption are some of the key risks to blockchain technology. Using hacking If the network is not secure enough, blockchains can be subject to hacking. Hackers can attempt to manipulate the network by altering the data in blocks, obtaining private keys, or mounting a 51% attack to gain control of the network**.**

P2P Network that exists in the successful cryptocurrency like bitcoin network may pose a serious threat to itself. Research (Yang et al., 2022) has also shown that the attack can also take over the target node's network connection, and it only needs to remove part of the victim node's TCP handshake packet during the attack capable of occupying the victim node's network connection for an extended period. The BHE attack is distinct in that it can impact the victim node's peering possibilities by changing the victim node's internal peer database (trial table and new table) and preventing the victim node from establishing a stable connection. It enables the attacker to take over all the target node's network connections and appear as its normal network middleman.

Cryptocurrency

The researcher (Ghosh et al., 2020), focus and explain structure of blockchain and the working of the ongoing transactions in the cryptocurrency network. This paper explains the structure on the bitcoin network. **Figure 2** shows how sender A sends some bitcoins to receiver B. Both need to install Bitcoin. He also needs the sender's private key and the recipient's Bitcoin address. Every entity in the blockchain network can send digital assets to the sender's Bitcoin address. To establish that the money being sent belongs to the sender, a cryptographic key is used to implement a digital signature on the transaction. A signal is broadcast to every miner on the bitcoin network as early as the sender renders his transaction public on the network. This is done to inform the miners of the new transaction's receipt. Upon that, the miners validate digital signatures and determine whether the sender is sending funds within the stated limits.

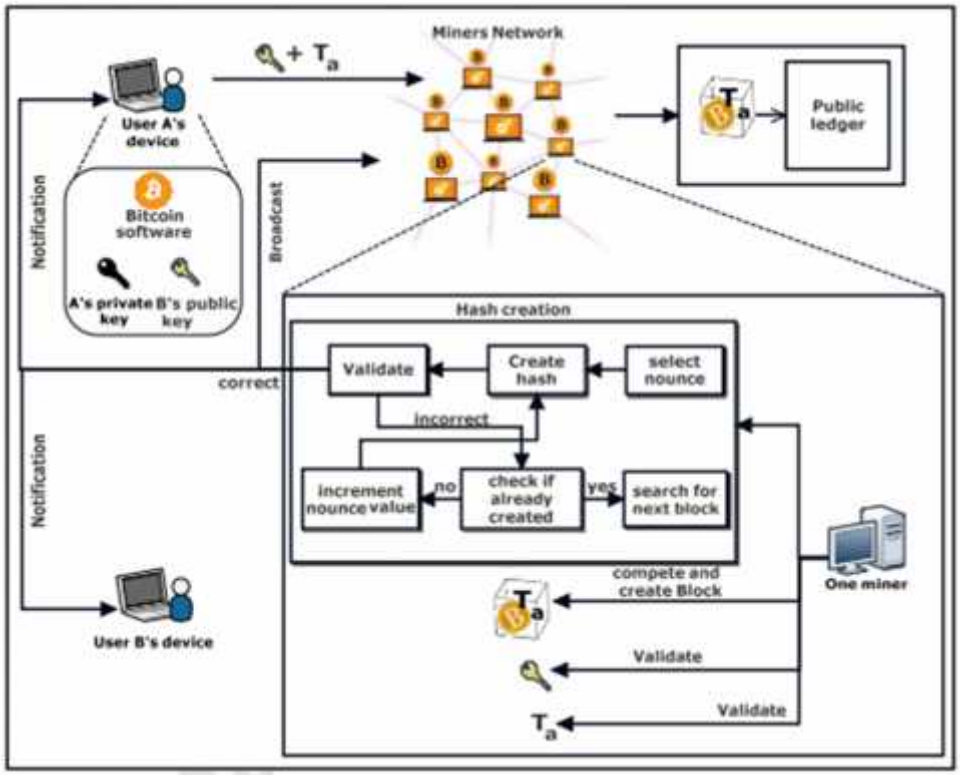

Figure 2 : Transaction Lifecycle on The Bitcoin Network (Ghosh et al., 2020).

Cryptocurrency assaults are several types of cybercrime that try to steal or compromise digital currencies and the platforms that store them. As the popularity and value of cryptocurrencies have grown, these attacks have become more regular and financially destructive. Aiming for financial gain, malevolent threat actors (including scammers and

hackers) have been highly motivated to hack and swindle to get possession of bitcoin wallets and carry out transactions. This is due to the high reliance on technology, the increasing usage by dealers and businesses, and the inherent anonymity connected with transactions and wallet owners. (Almukaynizi et al., 2018). The most often examined cryptocurrencies in the literature are Ethereum, Monero and Bit- coin. Millions of dollars have been taken from thousands of victims as a result of these hacks. Furthermore, crypto jacking attacks take use of millions of linked devices. However, ransomware denial of service and productivity losses create much bigger costs, which are estimated in the billions of dollars (Badawi & Jourdan, 2020).

3. Types of Cryptocurrency Hacking Attacks

Blockchain Attack Vectors

The blockchain isn't as secure as we believe it is. Even though security is built into every blockchain technology, even the most robust blockchains are vulnerable to current hackers. Blockchains have already been utilised by cybercriminals to carry out damaging actions. If the WannaCry and Petya ransomware attacks had not been funded in bitcoin, they would not have been as pervasive. It appears that hackers are now making a living by exploiting blockchain security flaws.

White hat hackers uncovered 43 flaws in various blockchain and cryptocurrency systems in less than 30 days in March 2019. They found weaknesses in well-known platforms like as EOS, Coinbase, and Tezos. (*Researchers Found over 40 Bugs in Blockchain Platforms in 30 Days*, n.d.). According to the (Anna, 2022). Cybercriminals demonstrate their intelligence by targeting such large networks as Bitcoin and Ethereum. **Table 2** shows five most common blockchain attack vectors and some list of attacks below these attack vectors that we summarize from the article:

Table 2: Blockchain Attack Vectors and Its Description

No	Blockchain Attack Vectors	Types of Attacks
1.	Blockchain network attacks: Blockchain network assaults are a sort of cryptocurrency attack that targets the blockchain network itself. It is a node that creates and executes transactions while providing other services. These attacks have the potential to interrupt network operations and result in considerable financial losses for users.	i. Distributed denial of service (DDOS) ii. Sybil attacks iii. Transaction malleability attacks Timejacking iv. Routing attacks v. Long range attacks on proof of stake networks vi. Eclipse attacks
2.	User wallet attacks: Hackers seek to obtain wallet credentials by employing both traditional methods such as phishing and dictionary attacks, as well as more sophisticated methods such as detecting weaknesses in cryptographic algorithms. The following is an overview of the most common methods of attacking user wallets.	i. Phishing ii. Flawed key generation iii. Attacks on cold wallets iv. Vulnerable signatures v. Dictionary attacks vi. Attacks on hot wallets
3.	Smart contract attacks: The key blockchain security concerns associated with smart contracts are bugs in source code, a network's virtual machine, the runtime environment for smart contracts, and the blockchain itself. Let's go over each of these attack paths individually.	i. Vulnerabilities in contract source code ii. Vulnerabilities in virtual machines

4.	Transaction verification mechanism attacks: Transaction verification is a fundamental component of blockchain technology that assures the network's authenticity and integrity. The transaction verification system, also known as the consensus mechanism, is subject to attacks that might interrupt network operations and cause users to incur financial losses.	iii. iv. v. vi. vii.	Finney attacks Race attacks Vector76 Alternative history attacks 51% or majority attacks
5.	Mining pool attacks: Mining pool attacks are another type of cryptocurrency attack that targets the process of mining, the computational process by which transactions are verified and added to the blockchain. Mining pools are groups of miners who combine their computing power to increase the likelihood of successfully mining a block and receiving the associated reward. Mining pools are a suitable place to start. Malicious miners use common web application flaws in the blockchain consensus technique to obtain internal and external control of mining pools.	i. ii.	Selfish mining Fork after withholding

Phishing and Social Engineering Attacks

Phishing and social engineering assaults are both frequent methods of targeting bitcoin users. These assaults are intended to dupe victims into disclosing critical information or finances, and they can have disastrous effects for the victims. The attacker will build a phoney website or email that looks to be from a reputable cryptocurrency exchange, wallet, or service in a phishing assault (Campbell & Moghaddam, 2018). The victim is then prompted to provide their login information, seed phrase, or private key, which the attacker can then use to steal their money.

Social engineering assaults use psychological manipulation to deceive the target into disclosing sensitive information or money. For example, the attacker may act as a customer service representative and request the victim's private key in order to address a fictitious issue with their account. It is essential to be watchful and careful when utilising bitcoin services to prevent being a victim of these assaults. This involves authenticating websites and emails, employing strong passwords and two-factor authentication, and never disclosing sensitive information, such as private keys or seed phrases, to anybody (Weber et al., 2020). To lessen the danger of a successful assault, it is also advised to utilise renowned and secure bitcoin exchanges, wallets, and services.

51% Attacks

A 51% assault on a blockchain network occurs when an attacker or a group of attackers controls more than 50% of the network's processing capacity, allowing them to manipulate the network by controlling the majority of nodes. With this power, the attacker may reverse transactions, double spend, and block new transactions from being verified, allowing them to effectively take over and control the network (Sayeed & Marco-Gisbert, 2019). This sort of assault is extremely dangerous to the security and integrity of a blockchain network. According to (Saad et al., 2020), Five blockchain-based cryptocurrencies, Bitcoin Gold, Monacoin Zencash, Litecoin Cash, and Verge, were the targets of a 51% attack between May and June 2018, resulting in a $5 million USD loss. In order to reorder transactions and prohibit other miners from producing blocks, attackers in each cryptocurrency were allowed to get more than 51% of the network's hash rate. As a result, they were able to seize control of the Blockchain and double-spend on critical transactions.

Ransomware

Ransomware is a sort of cyber assault in which the attacker encrypts the victim's data and demands a ransom payment to obtain the decryption key (Froehlich et al., 2021) . There has been an upsurge in the usage of cryptocurrencies, such as Bitcoin, as a way of payment for ransomware attacks in recent years. Ransomware is a sort of malware that prevents the victim from accessing the machine it infects until the ransom is paid. A typical ransomware infection, as described by (Conti et al., 2018), contains the following events:

i. Infection: Ransomware, like other types of malwares, spreads via a number of attack vectors. Email marketing containing malicious links or attachments to the malicious payload, as well as exploit packs, are examples of these vectors. Interestingly, modern ransomware has the ability to self-promoter. WannaCry and NotPetya, for example, infect local workstations on the same network by exploiting flaws in network protocols.

ii. Encryption: After an infiltration, ransomware covertly encrypts files on the affected machine. Ransomware specifically targets data that are important to the user, such as photographs, movies, and papers. Ransomware encrypts files using an asymmetric encryption technique, a symmetric encryption algorithm, or a combination of the two. The encryption key is generated on-site or received from a remote Command and Control server (C&C). Backup data is frequently encrypted or erased to prevent recovery. Yet, the data required to run the system remains unaltered, at least until the ransom payment deadline.

iii. Extortion: After encrypting the data, ransomware shows a ransom warning on the screen. The ransom note of modern ransomware includes a threat message, ransom quantity specified in fiat currency such as US dollars or cryptocurrency such as bitcoin, a countdown timer that shows the time remaining until the deadline, and a payment address.

iv. Decryption: Following successful transaction, the ransomware will either automatically begin the decryption process or urge the victim to download and run a decryption programme.

Reverse Proxy Phishing

Reverse proxy phishing is a sort of phishing assault in which attackers create a fake website that seems real and uses it to deceive victims into entering their login credentials, personal information, or sensitive financial information such as cryptocurrency wallet credentials. When directed towards bitcoin exchanges or other sites where users store and manage their digital assets, these assaults may be very destructive. The stolen credentials can then be used by the attackers to take the victim's cryptocurrencies. Users must be cautious and take precautions to secure their online accounts, such as setting two-factor authentication and avoiding questionable emails or links.

An example of reverse proxy phishing can be seen by researcher (Barr-Smith & Wright, 2020) who uses the reverse proxy phishing method in their study. The html similarity library is used in this study to quantify the resemblance between original sites and any obvious clone. Unfortunately, it is ineffective in differentiating many more sophisticated phishing sites, as only those employing reverse proxies make slight changes to the Bitcoin address. The sites under examination use reverse proxies and other similar techniques to dynamically replicate the site's user experience while capturing the full user qualification and production code. This operator to fool users, more advanced forgeries might even substitute bitcoin deposit addresses with invalid addresses.

Cryptojacking

Cryptojacking malware frequently infects devices using traditional phishing tactics. It may also embed itself in websites and then execute in the web browser of a victim when they visit that site. Cryptojacking is a sort of cybercrime that includes the unlawful use of other people's equipment to mine for cryptocurrencies, such as cell phones, computers, or servers. Profit is the motive, but it is supposed to remain disguised from the victim.

Cryptojacking is a whole distinct type of assault based on cryptocurrency Cryptojacking injection is a paradigm shift in web-based crypto-mining attacks since it eliminates the need for a vital third-party, such as a weak web server. It makes use of the capacity of web browsers to run code. The code's purpose is to "mine" cryptocurrency. The now-defunct website coinhive.com, for example, released browser-based cryptomining programmes capable of mining Monero cryptocurrency bits. The original idea was for a user to compensate a website provider by giving a portion of their browser's CPU cycles while surfing the site. This was viewed as a viable alternative to advertising for monetizing "free access" resources (Badawi & Jourdan, 2020).

Dusting

Dusting is a sort of cryptocurrency assault in which a little quantity of bitcoin is transferred to an address with the intent of confusing or deceiving the receiver or disrupting the regular operation of a blockchain network. The word "dusting" refers to the fact that these little transactions frequently result in a small amount of "dust," or minute fractions of bitcoin that are too small to be spent or traded economically. Dusting attacks are designed to link a specific bitcoin address to a person or organisation, thereby jeopardising their privacy and identity. Dusting attacks may also be used to

disrupt a blockchain network's regular operation by overloading its transaction processing capacity with a high number of tiny transactions.

Double-Spend Attack

A double-spend assault in cryptocurrency refers to an effort by a hostile actor to spend the same digital money more than once. This can happen in a decentralised system where many servers hold identical copies of a public transaction ledger, but transactions arrive at each server at separate times. However, double spending can occur when a coin is taken from an improperly protected and guarded wallet. An anonymous hacker attacked the Bitcoin Gold cryptocurrency and amassed almost $18 million in stolen assets. The victims in this scenario were exchangers rather than end consumers.

DDoS Attacks

One of the most common assaults against internet services is distributed denial-of-service (DDoS) (Saad et al., 2020). Despite the fact that it is a peer-to-peer system, blockchain technology is vulnerable to DDoS attacks. Similar attacks have been launched on blockchain-based apps such as Bitcoin and Ethereum on a regular basis (Saad et al., 2019).

A Distributed Denial-of-Service (DDoS) attack is another type of cryptocurrency attack that can disrupt the normal operation of blockchain networks. In a DDoS attack, a large number of requests are sent to a network or server, overwhelming it with traffic and rendering it inaccessible to legitimate users. DDoS attacks can be launched against cryptocurrency exchanges, mining pools, and other blockchain-related services.

4. Impact of Cryptocurrency Hacking Attacks

Loss of assets

The unlawful use of a victim's processing power to mine bitcoin is referred to as cryptojacking. It can have a substantial impact on asset loss in a variety of ways:

i. Energy costs: Crypto jacking can drastically raise energy consumption because the compromised device runs mining software. This can lead to increased electricity expenditures and a shorter device lifespan.

ii. Performance: Crypto jacking can substantially slow down an infected device, creating performance issues and perhaps resulting in system crashes

iii. Security: Crypto jacking can expose the victim's device and network to other security threats. The malware used to perform crypto jacking may contain other malicious payloads that can further compromise the victim's security.

iv. Privacy: Crypto jacking can collect and transmit sensitive information from the infected device, potentially compromising the victim's privacy.

According to (König et al., 2020), Web-based cryptojacking infects websites with malicious JavaScript code that provides mining tokens to all visitors without their knowledge. They then compute and give the hashes back. This has a significant impact on the performance of the hosts and servers targeted by this attack, increasing CPU use and battery drain.

Impact on businesses and organizations

According to quantile regression, hacking attacks have a mainly large impact on bitcoin volatility's upper conditional distribution. The hacking of cryptocurrency-related businesses, such as cryptocurrency exchanges, causes heightened volatility. These findings imply that when pricing bitcoin investments, hacking is a distinct risk factor. The right tail of the variability distribution has a considerable effect, meaning that bitcoin exchange hacking has the opportunity to result in extremely volatile periods (Lyócsa et al., 2020).

According to a study conducted by (Abhishta et al., 2019), most cryptocurrency exchanges can recover from a DDOS attack within a day. Nonetheless, hourly data has been observed to allow trading to be totally halted owing to a DDOS attack. It demonstrates how a persistent DDOS attack can have a significant impact on exchange results.

Threat to the security and stability of the Blockchain

The blockchain's security and stability can be threatened in a variety of ways. These include:

i. Phishing attacks: are frauds designed to steal a user's credentials. Fraudsters utilise phoney URLs to send emails that look to be from a reputable source and ask for the user's credentials.

ii. Risks connected with software and operational weaknesses: Blockchain technology's security is subject to these concerns, which have plagued computers for the past 50 years.

iii. Distributed ledger technology (DLT) vulnerabilities: Blockchains are resistant to attacks, but not immune to them. DLT is vulnerable to several concerns that centralised databases are not, even though blockchains are significantly more secure than traditional database structures.

iv. Immutability, anonymity, and distributed control: These characteristics make blockchain a revolutionary technology, but they are also its greatest weaknesses.

v. 51% assaults: Miners are critical in verifying blockchain transactions, but a 51% attack is the most feared threat in the blockchain ecosystem.

vi. Private key management: Private keys are used to validate transactions and serve as IDs and security credentials for blockchain users. They are, however, subject to theft or loss since they are produced and maintained by users rather than third parties.

vii. Weaknesses in the blockchain's security system: Despite its distributed property and integrity, blockchain may still be attacked, and the blockchain's security mechanism can disclose its vulnerabilities.

viii. Risk management and compliance when data meshes with other sources: Blockchain provides a trustworthy environment for storing information, but enterprises and entities must guarantee that data stays consistent and compliant when meshing with other sources.

ix. Security attacks and their prevention: Although blockchains are safe since each user has a copy of the data, security attacks and their prevention remain a crucial part of creating sophisticated blockchain systems.

5. Prevention and Mitigation of Cryptocurrency Hacking Attacks

Phishing and Social Engineering Attack

Phishing and social engineering are two forms of cyber assaults that commonly target bitcoin users. By appearing as a reputable entity, these assaults are intended to deceive users into disclosing sensitive information such as passwords and private keys. To avoid and minimise these sorts of assaults, the following steps can be taken:

i. User Education and Awareness: Educating users on the hazards of phishing and social engineering assaults can assist to lessen the probability of these attacks succeeding. This might involve providing information on typical attack strategies such as bogus login sites and emails, as well as encouraging users to be wary of any demands for personal information.

ii. Two-Factor Authentication (2FA): By asking users to provide a second layer of authentication, such as a one-time code texted to their phone, in addition to their password, 2FA can assist to avoid phishing and social engineering attacks. This makes it more difficult for attackers to get access to a user's account, even if the user's password has been stolen.

iii. Use Recognized Sites: Encouraging consumers to only access bitcoin services and information from reputable sources will assist to limit the danger of phishing and social engineering attacks. Official websites, recognised exchanges, and well-known wallets are examples of this.

iv. Using a Secure Browser: Using a secure browser with built-in protection against phishing and social engineering attempts will help lower the danger of these sorts of assaults. This can involve using an anti-phishing browser, such as Google Chrome, or a browser that encrypts data, such as Tor.

v. Regular Monitor: Regular monitoring of user accounts can assist in detecting any strange behaviour, such as illegal access or changes to personal information, which may suggest a phishing or social engineering attempt.

51% Attacks

A 51% attack is a situation where a malicious actor or group of actors control over than 50% of a cryptocurrency network's computational capabilities, thereby allowing them to control the network and manipulate it in their favour. This can result in double-spending, censorship, and other malicious activities.

To prevent and mitigate 51% attacks in the cryptocurrency industry, various measures have been suggested and implemented. Some of the most effective measures include:

i. Decentralization: Increasing the number of participants in a network and making it more geographically dispersed helps to prevent 51% attacks. The more nodes a network has, the harder it becomes for a malicious actor to control more than 50% of the network.

ii. Proof of Stake (PoS) Consensus: PoS consensus algorithms replace the Proof of Work (PoW) algorithm used by Bitcoin, which is more vulnerable to 51% attacks. PoS algorithms require participants to hold a certain amount of cryptocurrency, making it more expensive for an attacker to control the network.

iii. Regular Forks: Regular forks can help to prevent 51% attacks by making the network more resilient to attacks. Forks make it more difficult for an attacker to gain control over the system since they must control more than 50% of the processing power after each fork.

iv. Layered Security Measures: Implementing multiple layers of security can help to mitigate the effects of a 51% attack. This can include using firewalls, intrusion detection systems, and encryption.

v. Regular Monitoring: Regular monitoring of the network helps to detect any signs of a 51% attack and take action to prevent it. This can include monitoring the network for unusual transactions and computing power fluctuations.

Ransomware

Ransomware attacks are especially dangerous for cryptocurrency users because they frequently target sensitive information, such as private keys and passwords, and can result in the irreversible loss of access to these resources. According to (Alshaikh et al., 2020), The signature technique is based on recognising distinct ransomware patterns, such as a certain sequence of bytes in the ransomware source code, the order of call functions, and the content of the ransom demand message. These sequences are saved in a database, and anti-malware software searches for them in executable files while scanning. The concept of behaviour-based detection is the observation of the features of how malware acts. As a result, It is founded on research into common ransomware behaviours such as file access, file system activity, and network activity. The following steps can be done to avoid and limit the risks of ransomware attacks:

i. Regular Backups: Backing up essential data on a regular basis and putting it in a secure location will assist to prevent data loss in the case of a ransomware attack. Backing up data to external hard drives or cloud storage services is one example.

ii. Anti-Virus Software: Installing and upgrading anti-virus software on a regular basis will assist identify and prevent ransomware attacks. Malicious software can be identified and prevented from infecting a device by anti-virus software.

iii. Updates to all software and operating systems on a regular basis can assist to guarantee that any known security vulnerabilities are fixed. Ransomware attacks frequently exploit these flaws, thus it is critical to maintain all software up to date.

iv. User Education and Awareness: Educating users about the perils of ransomware attacks as well as the necessity of safe computing habits can assist to lower the risk of these attacks. This might include encouraging customers to be wary of strange communications, to avoid downloading software from untrustworthy sources, and to keep their anti-virus software up to date.

v. Implementing a firewall can assist to prevent unwanted access to a device as well as preventing harmful software from infecting a device.

vi. Avoid Paying the Ransom: It is vital not to pay the ransom in the incidence of a ransomware attack. This can encourage the attacker to continue their harmful operations and may also result in the attacker losing access to the encrypted data permanently.

Reverse Proxy Phishing

Reverse proxy phishing attacks on cryptocurrency can be particularly damaging as they can result in the loss of sensitive information, such as private keys and passwords. To reduce and avoid the hazards of reverse proxy phishing attacks., the following measures can be taken:

i. Implementation of Two-Factor Authentication: Using two-factor authentication (2FA) can assist to enhance the security of bitcoin accounts. When accessing an account, this might entail utilising a mobile device to acquire a one-time code.

ii. Strong Passwords: Creating and employing strong passwords can aid in the prevention of reverse proxy phishing attempts. Passwords should be a blend of upper and lowercase characters, numbers, and symbols that are difficult to guess.

iii. Avoid using public Wi-Fi: Public Wi-Fi networks are frequently insecure, allowing criminals to steal important information. It is suggested that when accessing cryptocurrency accounts, you use a secure, private network.

iv. Using a Virtual Private Network (VPN): A VPN can assist in encrypting internet traffic and preventing intruders from intercepting sensitive information. This is possible.

v. Use of Anti-Phishing Tools: Installing anti-phishing tools, such as browser extensions, can help to detect and prevent reverse proxy phishing attacks. These tools can identify suspicious websites and warn users before they provide sensitive information.

Dusting

Prevention and mitigation of cryptocurrency dusting attacks can be achieved through various means, including:

i. Keeping software up to date: Installing updates for cryptocurrency wallets and other software as soon as they become available can help prevent dusting attacks as these updates often contain security fixes.

ii. Utilizing hardware wallets: A hardware wallet provides added security as it stores the private keys offline and is immune to malware attacks.

iii. Regularly monitoring transactions: Regularly checking transactions can help identify and report any suspicious transactions, allowing users to take appropriate action to prevent potential damage.

iv. Using multi-signature technology: Multi-signature technology requires multiple parties to sign off on transactions, providing an added layer of security.

v. Education and awareness: Raising awareness and educating users about the dangers of dusting attacks is crucial in preventing them.

Double-Spend Attacks

Various methods may be used to prevent and mitigate bitcoin double-spend attacks, including:

i. Putting blockchain consensus algorithms into action: Consensus algorithms, like as Proof of Work (PoW), and Proof of Stake (PoS0), guarantee that the blockchain network agrees on the legitimacy of transactions, making a double-spend assault more difficult.

ii. Using reputable third-party services: Exchanges, for example, can provide a safe environment for transactions, lowering the danger of double-spend attacks.

iii. Using multi-signature technology: Multi-signature technology requires several parties to sign off on transactions, adding an extra layer of protection against double-spend attacks.

iv. Monitoring transactions on a regular basis: Checking transactions on a regular basis can help consumers discover and report any suspicious activities, allowing them to take proper action to avoid any damage.

DDoS Attacks

Various methods may be used to prevent and mitigate bitcoin DDoS assaults, including:

i. Putting network security measures in place: DDoS assaults can be mitigated by implementing intrusion detection, firewalls, prevention systems, and other network security measures (*Protecting Financial Institutions from DDoS Attacks | Resource Library*, n.d.).

ii. Using content delivery networks (CDN): CDNs distribute material to several servers, decreasing the possibility of a single failure point which might be a DDoS attack target.

iii. Using load balancing techniques: Load balancing techniques like round-robin and least connections can distribute incoming requests evenly over numerous servers, lowering the danger of a single server being swamped by a DDoS assault.

iv. Increasing network capacity: Increasing network capacity, such as by adding additional servers, can assist absorb DDoS assaults and decrease their impact.

v. DDoS protection services, such as cloud-based DDoS protection, can aid in the prevention of DDoS assaults by filtering out unwanted traffic.

6. Discussion

Blockchain technology has been a game-changer for secure transactions, but it has also led to a surge in blockchain-related threats and attacks. The usage of blockchain technology has grown substantially in recent years, resulting in a rise in cryptocurrency attacks. Because of the value of cryptocurrencies has increased, so have the value of attacks against them. The rising usage of decentralised financial systems as a method to access a greater range of financial goods and services is one of the primary causes driving to the increase of blockchain-based assaults. These systems are especially vulnerable to attack because they rely on a huge number of smart contracts that may be abused by malicious actors.

Section 3 shows the Phishing attacks are the type of cryptocurrency assault that uses social engineering approaches to deceive victims into exposing their private keys or sensitive information. Another popular type of assault is the 51% attack, in which an attacker gets control of more than 50% of the computational power of a blockchain network, allowing them to manipulate the system for their own advantage. Ransomware attacks, which encrypt a user's data and demand money in return for the decryption key, are another developing threat. These assaults can be very catastrophic, resulting in the loss of valuable information and the interruption of corporate activities. DDOS attacks with sending many requests are sent to a network or server, preventing genuine users from accessing it.

All these attacks are seen to impact assets, businesses and organizations and threaten the security and stability of the blockchain. For example, at section 4 prove a DDOS attack allows trading to be completely stopped by a DDOS attack. Although it can be rebuilt it takes time and disadvantageous. To mitigate these risks, users need to know how to prevent each of the attacks as discussed in section 5. It is also important for organizations to invest in robust security measures to protect their networks and users from these types of attacks.

7. Conclusion

In this paper, we describe Blockchain technology and identify common types of cryptocurrency hacking attacks. Although Blockchain technology is seen to have complete main features, but the results of several studies show that it is vulnerable to threats and there have been several attacks on this technology. We may argue that hacking attacks have now become a source of concern for every individual and corporation. The first line of defence in winning a war is understanding how the adversary operates, followed by the skills and tools required to assist prevent the attack. As a result, we want to broaden our investigation in the future to include the strategies and tools used by hackers to reduce the danger and resist cryptocurrency assaults.

Acknowledgments

The authors would like to thank to all School of Computing members who involved in this study. This study was conducted for the purpose of Ethical Hacking & Penetration Testing Research Project. This work was supported by University Utara Malaysia.

References

Abhishta, A., Joosten, R., Dragomiretskiy, S., & Nieuwenhuis, L. J. M. (2019). Impact of Successful DDoS Attacks on a Major Crypto-Currency Exchange. *Proceedings - 27th Euromicro International Conference on Parallel, Distributed and Network-Based Processing, PDP 2019*, *March*, 379–384. https://doi.org/10.1109/EMPDP.2019.8671642

Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain technology in healthcare: A systematic review. *Healthcare (Switzerland)*, *7*(2). https://doi.org/10.3390/healthcare7020056

Almukaynizi, M., Paliath, V., Shah, M., Shah, M., & Shakarian, P. (2018). Finding cryptocurrency attack indicators using temporal logic and darkweb data. *2018 IEEE International Conference on Intelligence and Security Informatics, ISI 2018*, 91–93. https://doi.org/10.1109/ISI.2018.8587361

Alshaikh, H., Ramadan, N., & Ahmed, H. (2020). Ransomware Prevention and Mitigation Techniques. *International Journal of Computer Applications*, *177*(40), 31–39. https://doi.org/10.5120/ijca2020919899

Anita, N., & Vijayalakshmi, M. (2019). Blockchain Security Attack: A Brief Survey. *2019 10th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2019*, 1–6. https://doi.org/10.1109/ICCCNT45670.2019.8944615

Anna. (2022). *Blockchain Attack Vectors: Vulnerabilities of the Most Secure Technology*. https://www.apriorit.com/dev-blog/578-blockchain-attack-vectors

Badawi, E., & Jourdan, G. V. (2020). Cryptocurrencies emerging threats and defensive mechanisms: A systematic literature review. *IEEE Access*, *8*, 200021–200037. https://doi.org/10.1109/ACCESS.2020.3034816

Barr-Smith, F., & Wright, J. (2020). Phishing with A Darknet: Imitation of Onion Services. *ECrime Researchers Summit, ECrime*, *2021-Novem*. https://doi.org/10.1109/eCrime51433.2020.9493262

Campbell, S., & Moghaddam, F. M. (2018). Social Engineering and Its Discontents. *The Psychology of Radical Social Change*, *October*, 103–121. https://doi.org/10.1017/9781108377461.007

Conti, M., Gangwal, A., & Ruj, S. (2018). On the economic significance of ransomware campaigns: A Bitcoin transactions perspective. *Computers and Security*, *79*, 162–189. https://doi.org/10.1016/j.cose.2018.08.008

Dryall, S. (2018). Cryptocurrencies and Blockchain. *The WealthTech Book*, *July*, 158–161. https://doi.org/10.1002/9781119444510.ch38

Froehlich, M., Hulm, P., & Alt, F. (2021). Under Pressure. A User-Centered Threat Model for Cryptocurrency Owners. *ACM International Conference Proceeding Series*, 39–50. https://doi.org/10.1145/3510487.3510494

Ghosh, A., Gupta, S., Dua, A., & Kumar, N. (2020). Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects. *Journal of Network and Computer Applications*, *163*, 102635. https://doi.org/10.1016/j.jnca.2020.102635

Hassan, A., Zaki Mas, M., Md Shah, W., Faisal Abdul-Latip, S., Ahmad, R., Ariffin, A., & Yunos, Z. (2020). A Systematic Literature Review on the Security and Privacy of the Blockchain and Cryptocurrency. *Journal of Cyber Security*, *2*(1), 1–17.

Husna Zakaria, N., Kunhibava, S., & Bakar Munir, A. (2018). Prospects and Challenges: Blockchain Space in Malaysia. *MLJ Cx Malayan Law Journal Articles*, *3*, 1–15. https://umexpert.um.edu.my/file/publication/00011934_162541_74356.pdf

Ishchukova, E., Romanenko, K., & Salmanov, V. (2022). Model of Information System for Application of Blockchain Technologies. *Journal of Physics: Conference Series*, *2218*(1). https://doi.org/10.1088/1742-6596/2218/1/012036

König, L., Unger, S., Kieseberg, P., & Tjoa, S. (2020). The risks of the blockchain a review on current vulnerabilities and attacks. *Journal of Internet Services and Information Security*, *10*(3), 110–127. https://doi.org/10.22667/JISIS.2020.08.31.110

Lyócsa, Š., Molnár, P., Plíhal, T., & Širaňová, M. (2020). Impact of macroeconomic news, regulation and hacking exchange markets on the volatility of bitcoin. *Journal of Economic Dynamics and Control*, *119*. https://doi.org/10.1016/j.jedc.2020.103980

Naje, S., Sami, A., & Younis, Y. A. (2021). Blockchain and Cryptocurrencies in Libya: A Study. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3492547.3492594

Protecting Financial Institutions from DDoS Attacks | Resource Library. (n.d.). Retrieved February 10, 2023, from https://www.imperva.com/resources/resource-library/white-papers/protecting-financial-institutions-ddos-attacks/

Researchers found over 40 bugs in blockchain platforms in 30 days. (n.d.). Retrieved February 17, 2023, from https://thenextweb.com/news/blockchain-cryptocurrency-vulnerability-bug

Saad, M., Njilla, L., Kamhoua, C., Kim, J., Nyang, D., & Mohaisen, A. (2019). Mempool optimization for Defending Against DDoS Attacks in PoW-based Blockchain Systems. *ICBC 2019 - IEEE International Conference on Blockchain and Cryptocurrency*, 285–292. https://doi.org/10.1109/BLOC.2019.8751476

Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D. H., & Mohaisen, D. (2020). Exploring the Attack Surface of Blockchain: A Comprehensive Survey. *IEEE Communications Surveys and Tutorials*, *22*(3), 1977–2008. https://doi.org/10.1109/COMST.2020.2975999

Sayeed, S., & Marco-Gisbert, H. (2019). Assessing blockchain consensus and security mechanisms against the 51% attack. *Applied Sciences (Switzerland)*, *9*(9). https://doi.org/10.3390/app9091788

Weber, K., Schütz, A. E., Fertig, T., & Müller, N. H. (2020). Exploiting the human factor: Social engineering attacks on cryptocurrency users. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *12206 LNCS*(July), 650–668. https://doi.org/10.1007/978-3-030-50506-6_45

Yang, J., Sun, G., Xiao, R., & He, H. (2022). Detectable, Traceable, and Manageable Blockchain Technologies BHE: An Attack Scheme against Bitcoin P2P Network. *Wireless Communications and Mobile Computing*, *2022*. https://doi.org/10.1155/2022/2795004