Is Blockchain Vulnerable to Malicious Attacks?

Dr. Gurusami Kolandan,

Research Scholar, Chanakya National Law University, Patna, Bihar

Abstract: *Blockchain is the latest outcome of the advancement of information technology. It gains significance in the financial and security markets in terms of minimising risk and maximising profit. Since huge amounts of money and data are involved in the securities market, it is necessary to ensure the data is safe and secure. SEBI, the securities market regulator, is actively contemplating the application of blockchain in the securities market. In this paper, the author discusses how secure the blockchain is, by explaining, in brief, the security features and how they protect the user from malicious attacks. Blockchains are not foolproof technologies. It is also vulnerable to malicious attacks. Blockchain-driven applications have recently been the target of many malicious attacks that caused huge financial losses to their users. Despite its shortcomings, the key features of blockchain technology, namely ensuring security in transactions due to its principles of cryptography, decentralization, and consensus, have gained importance around the globe. Many countries are planning to issue blockchain-based digital currencies, evidencing their vital role.*

Keywords: Attack, Blockchain, Computer, Crypto, Hack, Malicious, Security.

1. Introduction

Blockchain is a data structure with inherent security properties that are primarily used in currency transactions, which necessitates a methodology of storing data that is difficult to alter, hack, update, and defraud. Digital currencies facilitate a more efficient currency management system, and they are also more cost-effective than paper currency. The growing popularity of cryptocurrencies, as well as their inherent security features, drew many countries to issue the Central Bank Digital Currency (CBDC). The Government of India is contemplating the issuance of CBDC to reap its benefits.

The principles of cryptography, decentralization, and consensus are the cornerstones of the blockchain. It is also known as "Distributed Ledger Technologies (DLT) because the data is structured into blocks that can hold a set amount of data. Each block contains the cryptographic hash of the previous block, which connects the two. Thus, a chain is formed by the linked blocks. Once the data or information filled in the block reaches its capacity, it is chained to the previous full block, creating a chain of data. To record new information, an empty block is then added to the end of the chain. Transactions are validated within the

block to ensure that each transaction is true using a consensus mechanism. Since a single user cannot alter the record of transactions, the chances of a single point of failure are remote. It facilitates decentralization through the participation of members across a distributed network.

2. Significance

The specialty of blockchains is the absence of a central authority, which allows users to control their transactions. The presence of intermediaries is obvious in many businesses, especially in the securities market. Blockchain technology eliminates the need for intermediaries and paperwork. It takes less time to complete the transaction than traditional technologies in the absence of a more complex validation process. It facilitates peer-to-peer transactions, which ensure that none of the parties take undue advantage. It makes transactions faster, besides reducing the chances of errors and fraud and thereby reducing operational costs. Its ability to do settlement and reporting enhances operational efficiency. It reduces the time for information exchanges, improving the efficiency of communication. It also creates a more transparent environment by making it difficult to commit fraud in transactions. Because public blockchains are a transparent technology, they are extremely beneficial for the interaction of various business processes. The accuracy of the blockchain is ensured by the approval of transactions by a network of computers and the elimination of humans in the verification process. The efficiency of transactions can be achieved through a decentralised system.

3. Application

Blockchain is a new technology and has been widely used in cryptocurrencies for the past three decades. The significance of the blockchain has been realized in the middle of this decade due to the popularity of cryptocurrencies, which increased its applications in other sectors as well. Digital currencies, viz., Ethereum and Ripple facilitate easy buying and selling. They are gradually replacing paper currencies throughout the world. The same technology can be extended to similar applications, especially securities transfer through the tokenization of existing stocks into digital stocks that act similarly to digital currency. The major challenge in the implementation of digital stock is the requirement of decentralised stock exchanges, whereas the current securities markets are centralized, and the authenticity, security, and validity of the transactions are ensured by the centralized authority. The other challenges of the securities market are longer settlement cycles, inefficient process cycles, high transaction costs, and the indispensable role of market intermediaries. The blockchain addresses these issues effectively. The decentralized market permits peer-to-peer transfers of stocks, which facilitates the direct buying and selling of securities between buyers and sellers. It eliminates the presence of a centralised authority and third parties or intermediaries for trading. It plays a key role in clearing and settlement, the automation of post-trade processes, and tracking, blocking, and reporting illegal attempts on the network. It also acts as an online automated surveillance system for each transaction. It reduces the settlement time and transaction costs. It ensures secure transactions and lowers compliance expenses. It accelerates securities transfer processing and improves contract administration. Blockchain technology has a big role to play in the securities market, financial markets, financial services, etc. in the future.

The process of cross-border payments is complicated due to the involvement of multiple banks and multiple currencies, and it takes a long time to process the payments due to the

presence of many intermediaries across the border. Blockchain facilitates more cost-effective, end-to-end remittances within a short period without intermediaries. It also removes the hurdles associated with multiple banks and multiple currencies.

One of the major hurdles encountered by supply chain management is the traceability of the movement of goods. Blockchain's immutable ledger facilitates the real-time tracking of goods,

Blockchain is widely applied in cyber security because it removes the risk of a single point of failure and provides end-to-end encryption and privacy. It ensures a transparent and secure way of recording transactions in a decentralized system. Cryptographic algorithms ensure the verification and encryption of the data stored on the network, making it possible.

The healthcare industry encounters issues of data collection, maintenance, access, and corruption. Blockchain addresses these issues by providing instant access to data through a decentralised system. Also, it ensures the confidentiality of patient information by restricting access.

The government can better ensure, data integrity, enhance data security, reduce redundancy, and streamline its processes through the application of blockchain technology. It facilitates objectivity and uniformity through automated contracts and third-party oversight of transactions. It not only increases transparency but also ensures transactional and participant accountability. It enhances the efficiency of land registration. The major concerns in the election process are security, the integrity of voter registration and turnout, and poll accessibility. Voting platforms based on blockchain, address these concerns efficiently by ensuring tamper-proof records.

4. How does the blockchain ensure security in a transaction?

Blockchain, being an emerging technology, offers trust and enhanced security in its applications. Its structure and advanced level of encryption protect each transaction. The anonymity and security features make it difficult to alter, manipulate, and delete. Being a decentralised ledger system, it increases the level of security by duplicating and distributing data across the whole network. Data stored in conventional computer servers are more vulnerable to malicious attacks than data stored in the blockchain-enabled network of computers. To protect against unauthorised activity, it creates an unalterable record of transactions in blocks with end-to-end encryption. It also permits access to information for all designated nodes to record, share, and view encrypted transactional data on their blockchain. Hence, it paved the way for every participant to verify the correctness of the information by using zero-knowledge proof, through which one participant proves the correctness of data to another without disclosing data details. The security is enhanced due to the authenticity of the transaction, which is verified and confirmed by participants. However, a participant in a network will be provided with a private key to work as a personal digital signature. The unauthorised alteration of records invalidates the digital signature. If a hacker hacks one block in a network, he can only alter that block, which cannot align with other blocks. When everyone in the block crosses over, the hacked block will be the odd man out. To succeed in hacking the entire blockchain, he has to simultaneously hack, control, and alter at least 51% of the blocks in the blockchain to become the majority of blocks in that blockchain. Because they have to change all hacked

blocks to make them the majority blocks, such a hacking process is very expensive, time-consuming, and resource-intensive. However, the hacker cannot conceal the block modification. The other members of the network notice these hacked blocks and hard fork off to a new version of the chain that has not been hacked, attempting the hacker's wasteful one due to controlling valueless assets.

Immutability and consensus form the basis of the security of a blockchain network.

Immutability is the ability of the blockchain to prevent alterations in confirmed transactions. It ensures the integrity of data and confirms the validity of each new block of data. It is the specialty of the blockchain that ensures that the recorded transactions cannot be changed, altered, or deleted. The records kept in the blockchain are permanent in nature due to the date and time stamping of all transactions, and that facilitates tracking information over time, securely ensuring reliable audit information. The data is valuable, and its protection is inherent like any IT system. For better protection, blockchain enables one to have control over digital data.

Consensus acts as the brain of the blockchain, deciding the addition of blocks by pitting nodes against each other. Consensus models in a blockchain verify the legitimacy of a transaction. It is the ability of the nodes in a blockchain network to agree upon the validity of transactions and the true state of the network. To reach consensus, consensus algorithms are used, and their ability to arrive at consensus depends on the abilities of their algorithms because they ensure the following rules and the current state of the network are agreed upon by all parties involved. Its protocols include proof of work, proof of stake, proof of authority, etc.

Immutability and consensus provide a framework for data security in blockchain networks. The immutability of consensus is known as the longest-chain rule. If two conflicting versions of the same block appear, the block that is followed by the longest chain of blocks is treated as a legitimate one and abandons all its forks. The peers in the majority blockchain usually support the longest chain. The attack of the hackers will be defeated through this mechanism.

Cryptography is a mathematical and computational methodology for encoding and decoding data. It is another feature of the blockchain that contributes to the security of a transaction. It is mainly used to protect digital data and privacy by permitting only authorized access to data. It secures transactions between two nodes in a blockchain by preventing third parties from accessing data from private messages during a communication process. It is the best way to protect data from unauthorized access. When it is used in combination with hashing, the security of the blockchain will be stronger.

Encryption plays a substantial role in attaining data security in a blockchain, and cryptographic hashing functions are an important part of it. A hash function or algorithm, being a process, acts as a unique identifier for data blocks that receive an input of data of any size and return an output (hash) that contains a predictable and fixed size (or length). Irrespective of the number of times the hash function is executed, the final hash will be the same if the input does not change. The data of a block determines the block hash; therefore, every change demands a change to the block hash, and to form a chain of connected blocks, each block's hash is calculated with the previous block's hash. These hash identifiers are critical for the immutability and security of a blockchain. Since each

block includes the previous block's unique hash, it serves as a link in the blockchain, and any change in a block retroactively means a new hash has to be calculated for the block and also for every subsequent block. If there is any contradiction with the existing one, the other nodes reject the changes automatically and make the blockchain immutable. The hash function is also involved in the validation of the transactions of the consensus algorithms. Similarly, the Proof of Work (PoW) algorithm on the Bitcoin blockchain uses a hash function (SHA-256).

Timestamping is an important process in a blockchain for recording data to prove its existence at a specific date and time. If the user, before stamping, signs the document, he can prove that the document was in his possession at the time of the stamping and, without exposing its contents, can prove the files' origin, date, authenticity, and integrity. Since stamping is decentralized, to prove the certification of the document in the future, no third party or centralised internet service is required because he can prove the document's stamping through the posting of the document's hash on the publicly available blockchain.

On a peer-to-peer computer, the process of verifying and adding transaction records to a blockchain is known as "mining." It also confirms the authenticity of a transaction before including it in the blockchain through a network of computers. Miners perform the blockchain mining process through special blockchain mining software that enables them to communicate with others securely and verify the transactions to make sure that they are valid and in line with the blockchain code. Their "proof of work" (POW) is algorithmic evidence supporting or denying each transaction. Miners work together to secure a transaction network.

Crypto-economics plays a key role in ensuring the security of blockchain networks by describing nodes' behaviour on distributed blockchain networks, giving networks more incentives to perform honestly, and detaching dishonest nodes from the blockchain network.

The security features are carefully designed into the blockchain to protect it from malicious attacks.

5. The blockchain and its vulnerability to malicious attacks

The rationale behind the development of blockchain is to enhance security, efficiency, and trust. However, blockchain networks are not immune to malicious attacks and fraud because they have inherent security features like transparency, public verification, etc., which help hi-tech criminals breach the security mechanism. According to Orkut (2019) [1], blockchain technology has long been touted for its security. Under certain conditions, it can be quite vulnerable. Wang (2020) [2] argues that opportunities for malicious activity can arise within the various blockchain consensus models: Collusion, consensus, divergence, and dominance.

The strong security features of blockchain attracted not only many users but also cybercriminals. The nature of asymmetric cryptography ensures security by preventing anyone other than the private key owner from accessing funds held in a cryptocurrency wallet, putting the funds in a safe place as long as the private key is kept secure. Bitfinex, the world's largest cryptocurrency exchange, had its private keys stolen, resulting in the loss of US$ 73 million in customer bitcoins.

Hackers target centralised repositories, which are vulnerable to exploitation even if there is a single point of failure. Bithumb, one of the largest Ethereum and Bitcoin cryptocurrency exchanges, recently had its employee computers hacked, resulting in the theft of $870,000 in bitcoin as well as the data of 30,000 users.

6. Malicious attacks

Malicious attacks on the blockchain can be made in any of the following manners:

6.1 Email attack

Hackers generally employ the techniques of phishing attacks and routine attacks through mass emails to drain the wallets of users.

6.1.1 Phishing attack:

Blockchains are vulnerable to phishing attacks. The hackers, mainly with the help of Master Mana Botnet, a bargain Trojan malware, send bulk phishing emails to users with attachments or links containing malicious code to create back doors to empty the wallets of the users.

6.1.2 Routing attack:

The routing attack is made against the Internet Service Provider's (ISP) uptime through Border Gateway Protocol (BGP) that spreads the information in the network. Since BGP is vulnerable to misconfiguration and attack, a Malicious ISP or an attacker intercepts the data sent to an ISP and split the network into partitions with few IP prefixes, to carry out partition attacks by rejecting the genuine one. The Delay attack is carried out by delaying the propagation of information by a block in a blockchain network. The objectives of these attacks are to reduce the revenue of the minor and to make the network susceptible to double spending.

6.2 Peer-to-peer network-based attacks

6.2.1 Eclipse attack:

A decentralised network using the peer-to-peer protocol does not permit a node to simultaneously connect to other nodes on the network. Hence, an eclipse attack on a decentralised network isolates a target node and prevents the target from having the right information about the activities of the network and current ledger. The purpose of targeting a specific node is to control all of that node's neighbouring connections. An attacker taking control of all user's outgoing connections could then conduct a double-spend attack against the user or manipulate that node's mining efforts in a manner conducive to attacking the blockchain as a whole. Generally, eclipse attacks are performed on high-profile blockchain nodes—miners or merchants.

6.2.2 Sybil attack:

The Sybil attack is also a peer-to-peer network attack, targeting a certain number of nodes, contrary to the Eclipse attack, which targets the entire network. It floods the network with a large number of nodes with pseudonymous identities and tries to influence the network. The attacker creates the illusion that all nodes in the network are operated by unrelated individuals when, in fact, these nodes are operated by a single attacker-cum operator in the back and, if possible, creates a fork in the ledger, allowing the attacker to perform double spending and other attacks. The adoption of proof-of-work algorithms has made it incredibly expensive for single hackers to carry out Sybil attacks, as each transaction carries a separate fee. To date, no successful Sybil attacks on a major cryptocurrency have occurred.

6.3 Consensus Mechanism and Mining-based Attacks

6.3.1 Selfish mining attack:

Selfish mining is an attempt by a malicious miner to increase their share of the reward by not broadcasting mined blocks to the network for some time and then releasing several blocks at once, to make other miners lose their blocks.

6.3.2 Finney attack:

A Finney attack is a fraudulent double-spend attack. The prerequisites for these attacks are the participation of a minor, once a block has been mined, and the occurrence of a specific sequence of events. Despite the precautions taken by the merchant this risk cannot be avoided because it depends on the acceptance of the unconfirmed transactions by him or even waiting for a while to ensure the payment made to him is agreed upon by everyone in the network. Since these attacks are challenging, they cannot be made unless there is a significant gain to the attacker.

6.3.3 Mining malware

It is a kind of malware that uses the computing power of unsuspecting victims' computers to mine cryptocurrencies for hackers. Over a million computers were infected by this malware, which helped attackers mine more than 26 million tokens of various cryptocurrencies.

6.3.4 51% attack:

A blockchain's built-in security features make a 51 percent attack extremely difficult. Private blockchains are not vulnerable to 51% of attacks. However, a public blockchain is vulnerable to a 51 percent attack when a miner or a group of miners can control 51 percent or more of the mining power of the blockchain network, which helps them dominate the verification and approval of transactions and gain control. Hackers can manipulate or carry out fraudulent transactions through the dominant nodes. No 51 percent attack made until 2017. However, during May and June 2018, Monacoin, Bitcoin Gold, Zencash, Verge, and Litecoin Cash, blockchain-based cryptocurrencies, were targeted by a 51 percent attack and lost about $20 million in total; they also stole about $100,000 through a series of attacks on the Vertcoin currency. The hackers did not even leave the top 20 currencies;

Ethereum Classic lost more than $1 million. 51 percent of attacks will continue to grow in frequency and severity [3].

6.3.5 Timejack attack:

The blocks in a blockchain are based on the internal median time reported by peer nodes, which allows attackers to manipulate the time of a block by adding fictitious friends to friend lists and then complete the attack on the targeted block. The manipulated block will not accept blocks from the actual network as the timestamp of the blocks will not be the same as its timestamp, which helps the attackers to do double spending or malicious transactions with the manipulated block because these transactions can't be submitted to the actual blockchain network.

6.3.6 Race attack:

This attack is similar to the Finney attack but varies slightly. The attacker intends to double spend and does not need to pre-mine the block with his transaction, but he submits an unconfirmed transaction to a merchant and simultaneously performs another transaction that he made to the network, giving the merchant the impression that his transaction is the first. It is never submitted to the blockchain network by the attacker.

6.4 Smart contract-based attacks

Smart contracts are completely automated contracts without third-party intervention. The completed transactions, once written into the blockchain, become immutable to ensure returns based on their agreed-upon performance. Smart contracts are highly secured contracts, but they are also vulnerable to various attacks. The security of smart contracts is not part of a blockchain but depends on the strength of their codes. The strength of the code determines the malicious attack. The hackers can easily infiltrate the smart contract and steal, alter, or divert it if codes are poorly written and viz.

6.4.1 Reentrancy attacks:

A reentrancy attack can be made by creating a function that makes an external call to another untrusted contract before it resolves any effects. ERC-20 Tokens are tokens solely designed and used on the Ethereum platform, following a list of standards so that they can be shared, exchanged for other tokens, or transferred to a crypto wallet. An attacker can steal all the ether stored in the contract by recursively making calls to it. value() method in an ERC20$9 token if the user does not update the balance before sending ether. A careless user may lose his entire balance in the contract if he forgets to update his balance [4].

6.4.2 Denial-of-Service (DoS) attack:

It is a cyberattack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting the services of a host connected to the Internet. It enables a malicious actor to keep funds and authorities to himself. The vulnerable contract prevents refunds to the old leader of the contract and makes the attacker the new leader. Moreover, it cancels all the bid() requests sent by other bidders and keeps the attacker as the leader of the auction [5].

6.4.3 Overflow attacks:

An overflow in a smart contract happens when the value of the type variable (256) is exceeded. In a smart contract for online betting, if someone sends a large amount of ether, exceeding (2,256), the value of the bet would be set to 0. Although the exchange of an ether value greater than 2,256 is unrealistic, it remains a programming vulnerability in smart contracts written in solidity [6].

6.4.4 Short-address attacks:

Ethereum is an open software platform based on blockchain technology that enables developers to write smart contracts and build and deploy decentralized applications. Also, the Ethereum Virtual Machine (EVM) running on the Ethereum network enables anyone to run any application, providing a better opportunity for attackers to initiate short-address attacks. Ether token is used to pay transaction fees, miner rewards, and other services on the network. The short address attack uses bugs in Ethereum's virtual machine to issue extra ERC20 tokens on limited purchases through the creation of an Ethereum wallet ending with a 0 digit, by removing the last 0. In vulnerable smart contract codes, forcible balance transfers to the contract can occur without a fallback function, which can be used to exhaust the gas limit and disallow the final transaction [7].

6.4.5 Decentralized Autonomous Organization (DAO) attack:

DAO, being the transfer mechanism, would transfer the ether to the external address before updating its internal state and noting that the balance had already been transferred. This gave the attackers a recipe for withdrawing more ether than they were eligible for from the contract via re-entrancy. The DAO hack took advantage of Ethereum's fallback function to perform re-entrancy. Every Ethereum smart contract byte code contains a default fallback function, which has the following default implementation: This default fallback function can contain arbitrary code if the developer overrides the default implementation. If it is overridden as payable, the smart contract can accept ether. The function is executed whenever ether is transferred to the contract. As the attack against "The DAO" demonstrated, contracts that are vulnerable to re-entrancy attacks can be drained of all ether.The only publicly documented re-entrancy attack was against "The DAO" contract [8].

6.5 Wallet-based Attack:

A wallet is a file that contains a collection of private keys associated with peers in the system and communicates with the corresponding blockchain. It is safely guarded by the host. Through a malware attack on the host, the attackers can steal the wallet. NiceHash, a cryptocurrency company, was attacked in December 2017, and bitcoins worth US$63 million were stolen from its wallet [9]. The attackers are successfully attacking third-party services, enabling the storage of wallets as well.

6.5.1 Parity multi-sig wallet attack:

The Parity Multisig Wallet is a smart contract built to run on the Ethereum blockchain that operates with a multi-signature address and requires more than one private key to sign and authorise a crypto transaction before the Ether associated with it is approved to be

transferred. This is to improve usability and eliminate the risks associated with a single vulnerable point that can compromise the entire wallet. It is split into two contracts, viz., a wallet library contract and an actual wallet contract consuming the library, to reduce the transaction cost. Anyone can perform the deposit function by depositing money into the wallet. However, a withdrawal function that allows for the withdrawal of funds was placed in the central library. The wallet contract forwards all unmatched function calls to the library, which facilitates all public functions from the library to be callable by anyone, including wallets, which can change contract owners, making them vulnerable to attack. To carry out the attack, the attacker has to become an owner by adding his account to the library contract. When all wallets were implemented after a particular date, he became a joint owner. Then he triggered a kill function, looting the wallets.

7. Conclusion

Blockchain technology is a fast-growing technology of this decade, but it has been subjected to numerous malicious attacks as a result of the improper implementation, sacrificing security elements, and so on, all of which cost users dearly in its early stages. However, these attacks immensely contribute to its betterment. It is undergoing continuous improvement to enhance its security and improve its application in many sectors. Cryptocurrencies, smart contracts, automated tracking, policy applications, and other business applications are better than their previous versions, evidencing the trust reposed in them by the business world by adopting this technology in almost all sectors. Its visibility and use will be enhanced due to the adoption of this technology in the fast-growing Internet of Things. The trust, immutability, transparency, and value addition induced Unilever, Walmart, Visa, etc., to adopt this technology. ICICI Bank and Yes Bank have started adopting this technology. Kotak Mahindra Bank and Axis Bank expressed their interest and initiated trial transactions. Other players are exploring the possibility of adopting a strategy to add more value to their businesses. The government of India is contemplating setting up a national blockchain framework to prepare a centralised ecosystem that will cover 44 sectors, including e-governance. In addition to this, the Government of India is planning to digitise its currency, which will be legal tender money in the future, evidencing its significance. The application of blockchain technology in the securities market signifies a positive response, and in the future, digital stocks will rule the securities market in a decentralised market. Blockchain technology will soon dominate almost all sectors in the world.

Reference:

[1] M.Orcutt, “Once hailed as unhackable, blockchains are now getting hacked”, (**2019),** February Available from:https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/), accessed on October 15, 2022.

[2] L.Wang, “Fraud and Emerging Tech: Blockchain”, (**2020**), February, Available from: https://www.thecaq.org/fraud-and-emerging-tech-blockchain/ accessed on October 15, 2022.

[3] See Note No. [4].

[4] S. Muhammad, S. Jeffrey, N.Laurent, K. Charles, S.Sachin, N.DaeHun, and M.Aziz, “Exploring the Attack Surface of Blockchain: A Systematic Overview”, (**2019**), April 6: Available from:arXiv:1904.03487v1 [cs.CR]. accessed on October 12, 2022.

[5] Ibid.

[6] Ibid.

[7] Ibid.

[8] R.Price, “Digital currency Ethereum is cratering amid claims of a $50 million hack, Business insider India”, (**2016**), Available from: https://www.businessinsider.in/tech/digital-currency-ethereum-is-cratering-amid-claims-of-a-50-million-hack/articleshow/52795138.cms(accessed on October 15, 2022.

[9] B.Peterson, “Thieves stole potentially millions of dollars in bitcoin in a hacking attack on a cryptocurrency company," **(2017),** December [Online]. Available from: https://www.businessinsider.in/thieves-stole-potentially-millions-of-dollars-in-bitcoin-in-a-hacking-attack-on-a-cryptocurrency-company/articleshow/61955402.cms,accessed on October 12, 2022.