MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 60-81

A METHODICAL ANALYSIS OF THE BLOCKCHAIN TECHNOLOGY AND ITS CONCERNS ABOUT SAFETY

Ramanpreet Singh[1], Sukhwinder Singh Sran[2], Meenakshi Bansal[3]

[1]Yadavindra Department of Engineering, Punjabi University Guru Kashi Campus, Talwandi Sabo
ramanindagation@gmail.com
[2]Department of Computer Science and Engineering, Punjabi University, Patiala
sukhwinder.ucoe@gmail.com
[3]Yadavindra Department of Engineering, Punjabi University Guru Kashi Campus, Talwandi Sabo
ermeenu10@gmail.com

ABSTRACT

Blockchain being an emerging technology has drawn the attention to extend its applications in healthcare, financial institutions, energy sections supply chain management etc. Researchers have made significant progress in the field of blockchain technology, most notably with the development of a consensus algorithm. Extensive analysis of blockchain technology provides an essential component: the consensus algorithm. The fundamental idea of a consensus algorithm is that it can provide a reliable method for adding additional nodes to a blockchain network. The purpose of this study is to offer a thorough analysis of blockchain technologies, categorizes consensus methods, and delves into the problems with their security. Several vulnerability metrics are also offered for investigating the severity of attacks.

KEYWORDS

Blockchain, Consensus algorithms, Sybil attack, Double-spending, Vulnerability metrics.

1. INTRODUCTION

Day by day technology is growing vastly; the challenge to keep the system safe is more considerable. As we know due to cyber attacks, no system is secured. So chances of network damages, and data tamper can happen at any time. Therefore, blockchain can play vital role for dealing with different kinds of attacks and can protect network and system to damage. Blockchain technology uses consensus procedures to create a public ledger where cryptographic transactions can't be altered. As we know, blockchain is trustable to resist fraud and hacking[1]. Maintaining consensus is a major challenge in conventional systems due to their reliance on a small number of centralized servers. In blockchain technology, each node also functions as a server and host. In order for the consensus protocols to be fully implemented, it is necessary to disseminate the relevant data to all nodes[2]. Decentralized cryptocurrency was initially coined in blockchain by Satoshi Nakamoto[3]. People start to pay attention to blockchain technology after the introduction of the bitcoin cryptocurrency. Blockchain relied heavily on three technologies: cryptography, peer-to-peer networking, and a distributed system. The immutability of the blockchain means that the transaction records of digital currencies are safe from tampering. Several industries, including logistics, IoT, healthcare, insurance, elections, finance, and more, are utilizing blockchain technology.DLT stands for "distributed ledger technology," and it's essentially a shared, decentralized database that many people may access.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 60-81

1.1. Overview

Blockchain, a distributed ledger, may be used to record transactions and verify transactions involving digital assets in a P2P network. The network's nodes are all interconnected in some fashion and they all have a replicated copy of the ledger. We'll use a wedding as an illustration of how a blockchain works in its most basic form. Marriage rituals have been practiced for many hundreds of years. While the specifics of a wedding ceremony will vary from culture to culture and region to region, it is common practice to have witnesses present at any legal ceremony involving a binding contract between two parties.

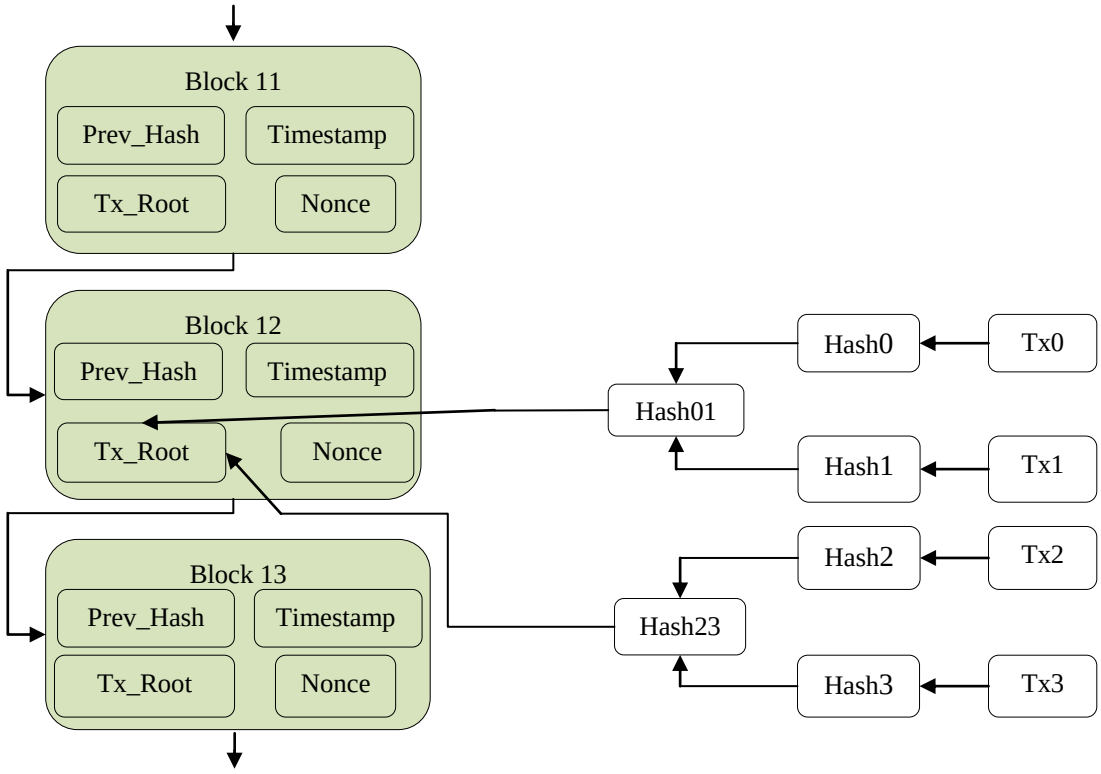

Figure 1.Blockchain validation process

Using the strength of a distributed ledger to retain reliable records of the "agreement/transaction" within an invited group, Blockchain technology is reminiscent to a wedding in many ways. By having copies of the agreement or transaction held by different parties, its authenticity can be verified. The term "blockchain" refers to the succession of blocks that are linked together in a linear fashion, hence the name. Figure 1 depicts the validation process that occurs within each block, which comprises multiple transactions. The block includes a number of fields in the block header in addition to the list of transactions that make up the block itself. The brief overview of the elements of a block is given below:

• **Version:** This parameter keeps track of the protocol version used by the node presenting the block to the chain.
• **Tx_Root:** This field, commonly known as the merkle root, includes the hash value of all of the confirmed transactions in the block. Each transaction is hashed into a hash value, as shown in Figure 2, and then each pair of hash values is combined and sent into a second hash algorithm. The merkle root can be found by repeating this process until there is only one remaining element.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 60-81

• **Prev_Hash:** This is the block's parent reference, which connects it to the block before it in the sequence. The contents of the previous block will be hashed, and the result will be stored in the current block's Prev Hash field. The number is generated by bitcoin's 256-bit hashing algorithm.
• **Timestamp:** The time when the block was discovered.
• **Bits:** This field shows the difficulty level of the PoW.
• **Nonce:** PoW relies on this field to show how much work a node put in to earn the privilege of adding its block to the blockchain.

1.2. Classifications of blockchain

There are four distinct blockchain technologies. They each find use in different situations.

1.2.1. Public blockchain

While using a public blockchain, there is no single controlling entity. Permissionless blockchain are decentralized ledgers that anyone can join. In this blockchain, all nodes have equal permission to view the entire blockchain, add new data blocks, and verify existing data blocks. Cryptocurrency transactions and mining are conducted via these blockchain. Bitcoin, Ethereum, and other cryptocurrencies are all public blockchain examples[4].

1.2.2. Private blockchain

You may also hear the term "managed blockchain" used to refer to private blockchain. These are governed blockchain solutions that require user authorization to access. The authority at the centre decides who gets to be a node. All nodes in this blockchain do not have the same set of permissions for operations. Since the private blockchain are only partially decentralized, access to them by the general public is restricted (e.g. hyperledger and ripple etc). The benefits of public and private blockchain's inspired the creation of the consortium blockchain and hybrid blockchain. The validation of new data is slower on public blockchain, whereas fraud is easier to commit on private blockchain[4].

1.2.3. Consortium blockchain

Consortium blockchain is that which is governed by a collection of different entities working together. This is called permissioned blockchain in nature. This blockchain has the advantage of more decentralization than private blockchain. Amore decentralization provides higher levels of security. In order for consortiums to be formed, collaborative work on the part of multiple organizations is required. This creates logistical complications as well as the possibility of antitrust violations [4].

1.2.4. Hybrid blockchain

Hybrid blockchain is managed by a central authority, but it relies on public blockchain for the validation of some transactions, which requires them to conduct some permission less processes and provide some supervision. Hybrid blockchain, such as IBM Food Trust, has several advantages, one of which is increased efficiency across the whole food supply chain [4].

1.3. Contributions

Blockchain is a system that facilitates the use of a distributed ledger. The system as a whole is quite secure, despite the shared ledger. Bitcoin is digital money that operates on the blockchain

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 60-81

ledger system. Blockchain is more valuable than the U.S. dollar or any other monetary system. This is a motivating factor in the ongoing theft attacks against the blockchain. The real value of this study is in its explanation of the security flaws and threats inherent to blockchain systems. Threat actors can take advantage of these openings in order to damage your important resources. When it comes to identity verification, P2P systems don't need a central trusted party chain, and it's simple to produce identities on P2P networks that treat everyone fairly. To begin, the attacker generates a large number of sybil nodes and establishes connections with the legitimate nodes, which then disrupt the true connections between the legitimate nodes on the P2P network. When the attacker obtains a sizable fraction of the network's total influence, he has effectively taken command of the P2P system. In the end, the attacker employs sybil nodes and an attack mechanism to set off many threats that undermine a P2P network's credibility.

Digital currencies are vulnerable to double-spending, a scenario in which an attacker makes two purchases with the same currency in order to earn double the value. To illustrate, the attacker may manipulate the transaction state and double-spend the same transaction. The honesty of the ledger is compromised by the potential for double expenditure. Double-spending can be caused by a number of different types of attacks, such as sybil-based double-spending, 51% attacks, etc. What follows is the outline for the rest of the paper: The several types of consensus algorithms are discussed in Section 2. Section 3 discusses the blockchain applications. The blockchain's security flaws are outlined in Section 4. The other typical blockchain problems are discussed in Section 5. Section 6 presents the investigation and findings of blockchain. Measures of susceptibility are discussed in Section 7. This paper concludes with a discussion of potential areas for further study in Section 8.

2. CLASSIFICATION OF CONSENSUS ALGORITHM

Since blockchain technology is itself decentralized, it may function without the oversight of any one particular institution. To reach agreement on the chronology of transactions on a blockchain, a consensus method must be used. The consensus protocols are implemented by nodes in blockchain network to provide reliability and consistency of data in addition secure transaction [5]. Consensus algorithms are also known as consensus mechanism and consensus protocols.

- A way for the blockchain nodes to agree on something.
- The updates to the distributed ledger must be universally accepted by all nodes.

Consensus, in its simplest form, is an agreement on the chronological order of confirmed transactions. The weak protocol encompasses a wide variety of consensus procedures[6].

2.1. Proof based consensus

In a proof-based consensus method, the node that provides the most convincing evidence of its legitimacy is the one that gets to link another block to the existing chain and reap the financial benefits. A couple of the most common proof-based consensus algorithms are proof-of-work (PoW) and proof-of-stake (PoS), however there are many other variants that have been developed.

2.1.1. Proof of work

Satoshi Nakamoto introduces the world to bitcoin in a white paper. In his 2008 study[3], he made use of the proof-of-work idea popularized by Cynthia Dwork and Moni Naor in 1993[7]. The most well-known cryptocurrency consensus protocol is proof-of-work (PoW). Markus Jakobsson and Ari Juels coined the phrase "proof of work" in 1999[8].

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 60-81

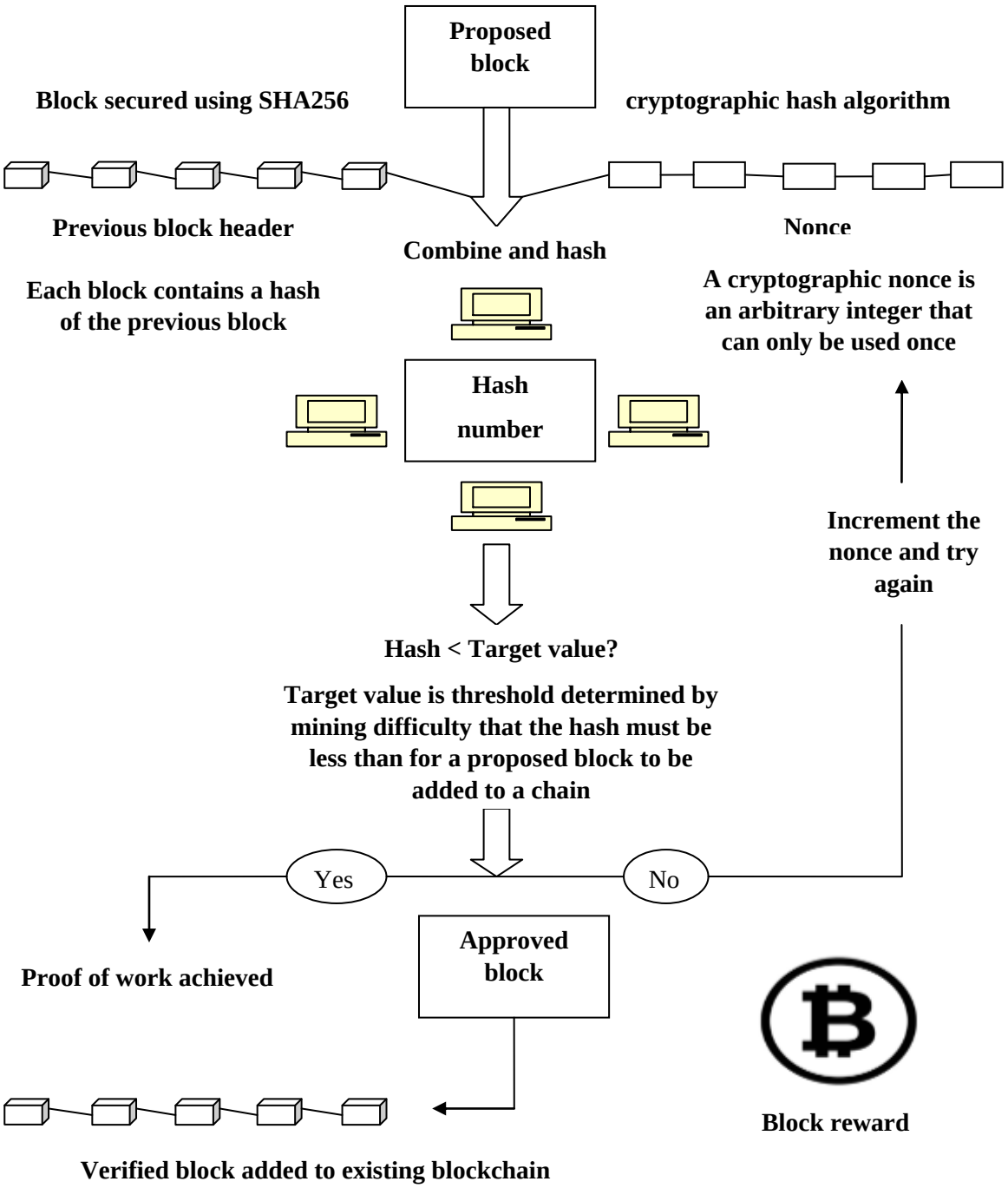

Figure 2. Illustration of the proof of work algorithm [9]

As the saying goes, "Simple to verify, but hard to find," and that's the guiding philosophy here. Figure 2 depicts the proof-of-work algorithm used to confirm transactions and add new blocks to the blockchain.

- A proof of work (PoW) is a piece of information that is difficult to duplicate but easy to verify.
- PoWs can be generated by a process of random guesswork or through the coordination of mining pools.
- For example: find a number X, such that SHA256 (Text + X) has 10 leading zeroes = = network difficulty.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 60-81

- Mining is the process of solving the crypto problem. Each node in the network plays the role of miner when it engages in mining operations. A miner is a person who does mathematical calculations in order to confirm a transaction.
- A mining pool is a group of miners working together to share computational power. The miners pool their computing resources in order to fairly distribute the rewards earned for solving a block.

Several problems with the proof-of-work algorithm are as follows:

- **The 51% risk**: In a decentralized proof-of-work system, overall computational power equals the sum of individual node computing powers. Hardware choices affect the available processing power. Mining pools form because the likelihood of winning the reward for discovering a new block improves as the size of the pool grows. When a mining pool controls 51% of the network's hashing power, it can reverse network transactions and cause double spending.
- **Time consuming**: It takes time for miners to find the correct answer for mining a block since they rely on nonce values. Only by completing the puzzle will the answer become clear.
- **Resource consumption**: In order to resolve the complex mathematical problem, miners use massive amounts of computational power. It causes a waste of time, effort, money, energy, space, and material.

2.1.2. Proof of stake

The proof of stake (stakers) algorithm is a consensus mechanism in which nodes validate transactions by staking their own crypto assets. The method uses the block's wealth (or stake) as a deterministic factor in selecting its creator. If there is no block reward, miners will only receive transaction fees. When compared to proof of work, proof of stake (PoS) is more economical. To implement its consensus mechanism, the proof-of-stake algorithm chooses validators based on the amount of the associated cryptocurrency they hold. Peercoin was the first cryptocurrency to use proof of stake in 2012. Cardano, Qtum, PIVX, Bitconnect, etc., are all examples of proof-of-stake cryptocurrencies.

- It is made to make networks safer and stop wasting resources.
- The person who makes the next block is chosen by a combination of luck and money.
- For instance, if you hold 1% of the coins, you can verify 1% of the proof of stake blocks.
- A PoS validators checks whether a transaction is legal or not as part of the validation process. If a transaction is against the law, it could be because of fraud, double spending, etc.
- The algorithms used by Proof-of-Stake (PoS) save money and energy.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 60-81

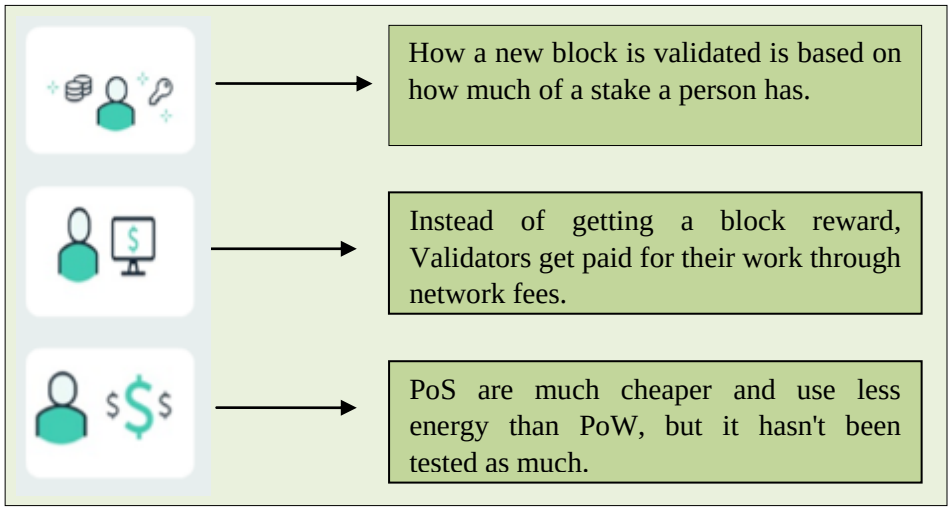

Figure 3. Illustration of the proof of stake algorithm [9]

Figure 3 illustrates the proof of stake algorithm. Monopoly problem is when a person with the most coins can double spend or refuse to do business. The attack is much more expensive to run than the proof-of-work attack.

2.2. Voting based consensus

For the voting-based consensus mechanism to function, it requires a well-understood and adjustable set of nodes within the verifying network to facilitate message passing. This is a major departure from proof-based consensus techniques, in which nodes in the verifying network are often allowed to freely join and leave at will. In a voting-based consensus mechanism, all of the nodes in the network must jointly verify the transactions or blocks, in addition to maintaining the ledger. Before deciding whether or not to add their proposed blocks to their chain, they will consult with others. Almost all of these variations impose the condition that a node must see at least T other nodes sharing the same proposed block with it before it may do the adding operation (T is a given threshold). As a result, voting-based consensus needs to be built to handle certain edge cases:

- There was a crash in some nodes.
- Certain nodes are not only taken down, but also tampered with.

In the event of a failure, each node will patiently await communications from the others. Nevertheless, certain nodes don't execute, which prevents the regular nodes from receiving enough evidence for an accurate conclusion. Unusual behavior on the part of nodes during subversion attempts could produce incorrect results. The Byzantine general's dilemma, first stated by Lamport, is a typical example of this type of issue. Each node in a blockchain network is responsible for executing the consensus task, but some nodes can be compromised to broadcast false or inconsistent results to the network as a whole. The network may have been unable to hold out against them, leading to inconsistent ledgers at various nodes[11].

Crashing nodes prevent them from communicating their results to other nodes, which delays the decision-making process. The voting-based consensus algorithms can be broadly categorized into two subtypes, Byzantine fault tolerance-based consensus and Crash fault tolerance-based consensus, in light of these undesirable events.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 60-81

2.2.1. Byzantine Fault Tolerance

Byzantine fault tolerance-based consensus has the potential to eliminate the occurrence of node crashes and node compromises. Hyperledger fabric makes use of a byzantine fault tolerance, also known as practical byzantine fault tolerance (PBFT), introduced by Castro and Liskov. There are two types of nodes in PBFT: the leader node and the validating peers (nodes) and it is the latter that will carry out the rounds necessary to append a block to the chain. Symbiont and R3 Corda are two further popular blockchain technologies that employ byzantine fault tolerance-based consensus methods. The ability of a distributed network to achieve consensus (i.e., agreement on the same value) even if some of its nodes do not respond or provide erroneous information is known as byzantine fault tolerance. Participation in a group decision-making process (both - accurate and incorrect nodes) is utilized in a BFT mechanism with the intention of reducing the influence of the faulty nodes, therefore protecting the system from failure[11].

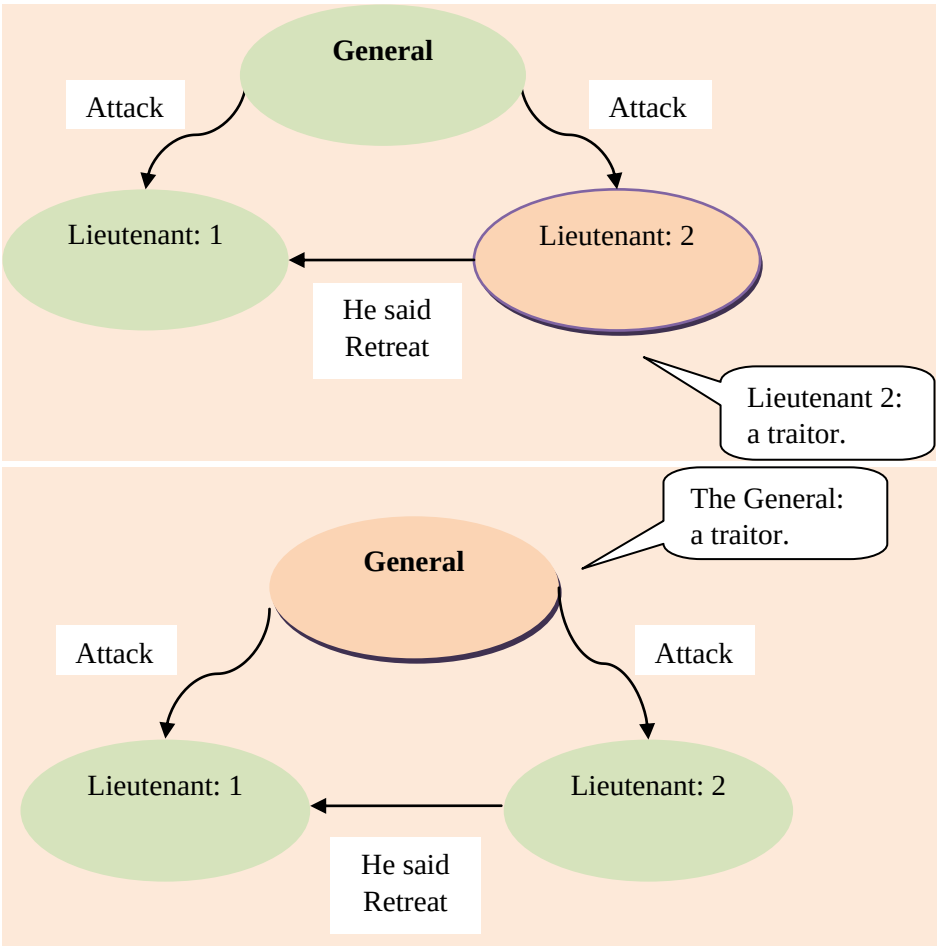

Figure 4. Illustration of the byzantine fault tolerances

Tolerating data corruption and malicious attacks, byzantine fault tolerance (BFT) is a consensus technique that can function even when computing nodes on a network fail. BFT guarantees that all nodes receive the same information. As a result, the protocol is immune to both faulty hardware and malicious attacks. To put it another way, if over two-thirds of the nodes are trustworthy, then the consensus will always be correct. Robert Shostak, Leslie Lamport, and Marshall Pease are credited with designing the byzantine general's dilemma, which led to the invention of BFT. Think of this issue in terms of a meeting of byzantine

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 60-81

generals as they lead their troops into battle, depicts in the Figure 4. All attacks must come at once for the generals to have any chance of victory. Now, how are they going to organize an attack if even one of the generals is a traitor?

It is possible to apply this scenario to the blockchain's consensus mechanism. Even in this case, it only takes one bad actor to destroy efforts to reach a consensus. For this, BFT employs an algorithm that allows consensus to be reached with as few as two-thirds of the nodes in agreement. With BFT, consensus cannot be destroyed by either a single point of failure or a group of uncoordinated bad actors.

2.2.2. Crash Fault Tolerance

The only way for the crash fault tolerance based consensus to work was to eliminate the possibility of nodes crashing completely. A consensus algorithm used for fault tolerance is Paxos and Raft. Raft was designed to be more accessible and usable in real-world systems than its predecessor, Paxos. There are three possible roles for validating nodes to play in the Raft consensus algorithm's execution: follower, candidate, and leader. Request Vote messages are used to elect a leader node, and Append Entries messages are used to forward the requests to other nodes in the network. There are many dangers that can affect a distributed system. There is always the risk of a process or device crashing or a network connection going down. In a business setting, it is essential that the consensus algorithm be resistant to interference from multiple sources[11].

Using crash fault tolerance (CFT), the protocol is made more robust so that the algorithm can continue executing and reach a consensus even if any of its parts fail. When one part of a system breaks, CFT is a suitable option. When blockchain is employed by large organizations, however, it's possible that distinct entities (such as corporations, departments, or teams) will be in charge of certain aspects of the system. Because the system's security relies on the cooperation of many entities with potentially conflicting goals, such as businesses, departments, and teams, it is susceptible to attacks. If one participant is malicious, the entire CFT fails to reach agreement.

3. APPLICATIONS OF BLOCKCHAIN

Being a relatively new technology, blockchain has attracted interest in expanding its use across a wide variety of industries, including supply chain management, energy, banking, healthcare, government, insurance, and more. The supply chain management covers various sectors like supply chain finance, maintenance tracking, supply chain compliance, provenance. The energy sector covers energy savings, energy consumption records, automating the trading of renewable energy. The financial institution covers trade finance, cross currency payments, mortgages, KYC. The healthcare covers medical records, medicine supply chain. The public sector takes care of registering assets and making sure people know who they are. The insurance covers how claims are handled, where risks come from, and how assets have been used in the past.

4. SECURITY ISSUES IN BLOCKCHAIN

In many cases, information is lost or corrupted during online transactions and conversations using decentralized P2P networks. So manage the data for privacy and confidentiality over network plays vital role in network security. Every year researchers worked hard to develop mechanisms for detecting and preventing possible cyber attacks. Some of the major security attacks of weak protocol[6] related to blockchain service are explained in this part[12]. The demand of blockchain is increasing because it provides transparency, but the security risks cannot be overlooked. The consensus algorithm is affected by following attacks:

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 60-81

4.1. Sybil attack

A rival can try to gain control of the network by establishing a number of false virtual identities. Sybil nodes are fictitious nodes that pretend to be real. The trustworthy nodes of the blockchain are temporarily severed after an attack[13]. As shown in Figure 5, a rogue node might assume multiple identities in the network[14]. A malicious node within the network appears as a large cluster of nodes, representing a sizable fraction of the network. As legitimate nodes have no way of knowing when malicious ones are acting fraudulently, some of them may even choose to share data with the bad guys [12].

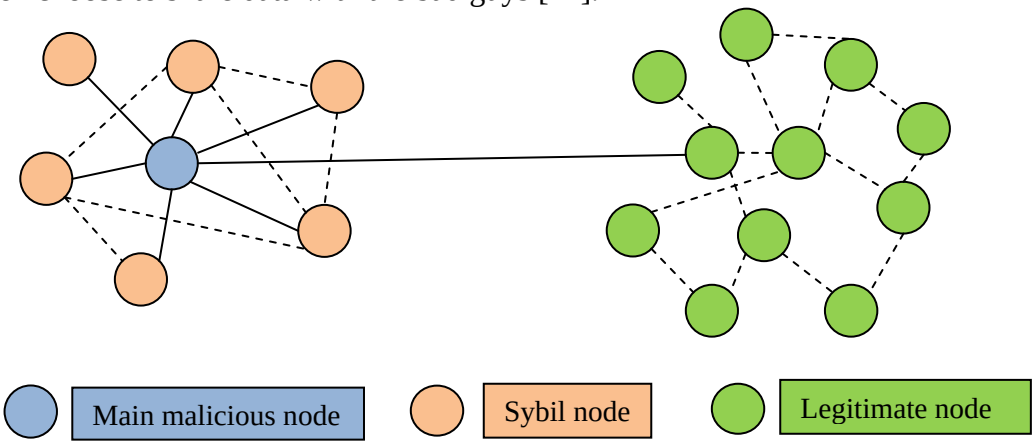

Figure 5. Sybil attacks [12]

Three types of nodes (legitimate, sybil, and attacker) make up the sybil attack algorithm. They are denoted by the letters L, S, and A. Sybil attacks are launched when an adversary in a peer-to-peer network creates a large enough number of fake nodes, or "sybils," and establishes connections with the legitimate nodes so as to interrupt the legitimate communications between the legitimate nodes themselves. The following steps of algorithm shows the process of sybil attack:

Algorithm 1: Sybil attack

```
L ← legitimate nodes;
S ← sybil nodes;
A ← attacker node;
while (true) do
    A creates S;
    A connects S with L;
    A gains fraction of the system ← Δ;
    If (Δ == true) then
        A uses attack method;
        A triggers threat;
        A damages reputation system;
    end
end
```

When an attacker achieves an abnormally big effect on a peer-to-peer network (Δ), he gains control of the system. Sybil nodes and the associated attack mechanism pose a significant risk to peer-to-peer networks and are therefore used by attackers to initiate threats [15].

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 60-81

4.2. Double spending

The biggest problem with digital currency is that it is easy to double-spend. In double spending, the attacker must spend the same currency twice to achieve their goal. In one common scenario, the attacker duplicates a transaction and then changes its state by spending it twice. The possibility of illegal double-payment reduces confidence in the ledger. Threats like Sybil-based double spending and the 51% attack are only two examples of the many that can lead to wasteful spending. The following steps of algorithm shows the process of double spending by 51% attack:

Algorithm 2: Double spending by 51% attack

```
L ← legitimate nodes;
LC ← legitimate chain;
M← malicious node;
MC ← malicious chain;
MCP ← malicious computing power;
while (true) do
    M→ separates private chain from LC;
    if (MCP ≥ 51%)then
        if (M→ creates conflicting transactions) then
            TX1 →LC;
            TX2 → MC;
            M→ starts mining MC;
            if (MC.length>LC.length)then
                MC becomes valid;
                L adopts MC;
                M gets spent funds back;
            end
        end
    end
end
```

Iqbal and Matulevicius[15] provide an algorithm illustrating the steps required for a 51% attack, also known as double spending. The double spending attack consists of legitimate nodes, a legitimate chain, a malicious node, a malicious chain, and malicious computation power. L, LC, M, MC, and MCP stand for these, in that order. The above code demonstrates how a 51% attack might lead to double spending. If the malicious chain is longer than the legitimate one (MC > LC), then the malicious chain is considered valid, and legitimate nodes will switch over to it. Thus, the double-spend transactions are validated, and the attacker gets his money back.

5. OTHER ISSUES IN BLOCKCHAIN

To address issues with virtual currencies, blockchain technology was created. The widespread adoption of blockchain technology holds great promise for enhancing the safety and availability of a wide range of goods and services. Although blockchain has many promising applications, it also has a number of issues that developers are now trying to address. Since blockchain systems are flawed in numerous application areas, widespread adoption of the technology remains a long shot. Here are some of the most urgent issues with blockchain technology.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 60-81

5.1. Scalability

The larger a blockchain is, the more vulnerable it becomes. There is a scalability problem with blockchain because of redundancy. Each node in your network must be able to see every transaction that has ever taken place, beginning with the genesis block and ending with the latest one. That's literally just hundreds of copies of the same data. Due to the sheer volume of data, massive blockchain demands intensive processing from the nodes. Nodes may require greater transaction fees from users in order to execute blockchain transactions in large public blockchain like Bitcoin (CRYPTO: BTC) and Ethereum (CRYPTO: ETH) due to the scaling problem.

5.2. Energy consumption

Power consumption for blockchain infrastructure is far greater compared to a centralized system. Even while their redundancy makes them more energy-intensive than a standard centralized cloud system, their transaction validation process also greatly contributes to this. When compared to other systems, the amount of space they need to store data is the largest drawback. The cost of powering a blockchain rises proportionately with the number of nodes it contains. In comparison to traditional systems, in which data is processed and stored mostly in a central body, each node stores and processes nearly as much information. If a blockchain network uses a proof-of-work mechanism to choose the node that will validate the next block in the chain, the network's energy consumption may increase. All these Bitcoin and Ethereum employ the proof-of-work approach, in which nodes attempt to resolve a complicated equation. An increasing number of competitors mean a constant struggle for harder to obtain resources, such as electricity, as the network expands.

5.3. Speed

Because of its decentralized structure, blockchain transactions are very quick but require validation by all nodes before being added to the next block. By placing faith in a centralized authority, centralized systems are able to handle millions of transactions daily. It takes only a few seconds to verify a purchase made with a debit or credit card at most stores when you use the card's magnetic strip reader. By the use of a network, monetary value is moved from your wallet to the wallet of the merchant; however this may take a day or two. Meanwhile, the issuing bank has the merchant's confidence. Credit card networks can handle hundreds of transactions per second because of the confidence their customers have in them.

Because of the decentralized nature of a blockchain like Bitcoin's, a transaction may only be considered finalized after it has been confirmed by the network. Since the Bitcoin blockchain can only execute a small number of transactions per second, this can be a time-consuming operation. When a customer makes a purchase, it could be an hour before the store owner learns whether or not the transaction went through. However, there are many practical blockchain applications in the financial industry; this makes it impracticable for most retail transactions.

5.4. No universal standards

Every implementation of blockchain technology is unique. This presents a number of difficulties for corporations and software engineers. Lack of blockchain standards mean interoperability solutions don't match the varied specifications of blockchain implementations, and vulnerabilities in code increase as programmers learn to work with unfamiliar environments. One company will need to build supplementary tools to facilitate the exchange of data with another company's blockchain.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 60-81

Although there are a number of different approaches to blockchain interoperability, no single approach meets the diverse requirements of the many blockchain implementations. To offer the same goods on another blockchain, developers must rethink everything when they produce something on one blockchain (a smart contract) but there are no common standards. Code vulnerabilities could be made worse by the absence of standards, as programmers would have to adapt to new environments.

5.5. Privacy

Personal private keys may be vulnerable in a decentralized system. When a wallet is created, a unique private key is generated that may be used to access any and all saved information. The theft of this item threatens both personal information and financial resources. If your wallet is lost, you will never get it back.

6. INVESTIGATIONAND FINDINGS OF BLOCKCHAIN

These are examples of what has been called a "systematic investigation" of blockchain technology in order to develop the facts that have been previously stated. Here, we provide a summary of what is currently known about blockchain technology, including empirical discoveries and theoretical and methodological advancements. Research in practically any academic discipline begins with a literature review.

Table 1. Findings of existing study

Iqbal &Matulevicius, 2021	**Method:** Detect sybil and double spending attacks using security risk management[15].
	Outcomes: This paper proposes a system that shows protected assets, threats that the attacker could activate using sybil attack, threats that cause double-spending, their vulnerabilities, and their solutions.
	Limitations: Permission blockchain lacks interoperability.
Platt & McBurney, 2021	**Method:** Sybil attacks on identity-enhanced proof-of-stake can be simulated with agent-based simulation[16].
	Outcomes: In this work, author presents mitigating measures that, while not entirely eliminating the risk of an attack on an identity-augmented proof-of-stake system, can significantly delay its complete takeover.
	Limitations: Better outcomes can be achieved by validating the area of research in an increasingly digitalized and fragmented world.
Sayeed et al., 2020	**Method:** Smart contract vulnerabilities can be detected using tools like Slither, MythX, Mythril, Manticore, Securify, SmartCheck, Echidna, Oyente, Vandal, and Zeus[6].
	Outcomes: This article showed that smart contract technology is vulnerable.The author developed a smart contract code vulnerability attack categorization based on the attack vector. This paper, examined 10 security tools to detect vulnerabilities and discovered that some were

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 60-81

	missed, giving attackers a false sense of security.
	Limitations: It has been discovered through research that this technology is not completely safe against hacks and exploits. Protecting smart contracts from flaws in the code still requires attention.
Begum et al., 2020	**Method:** Assess the security threats posed by double spending, and provide a possible theoretical countermeasure[17].
	Outcomes: An overview of blockchain security issues and possible countermeasures is presented in this study. Both the damaged and executed areas, as well as the double spending attack, have been thoroughly investigated.
	Limitations: This research has not lead to a practical application. As a result, the findings cannot be considered reliable.
Gong & Lee, 2020	**Method:** Blockchain-based smart contracts that add sybil protection to the cyber threat intelligence (CTI) system[18].
	Outcomes: This article described a three-layered blockchain-based CTI system. This research gathers CTI data from multiple sources and examines data and contributor validity. Authors performed simulations in terms of the attacker's reliability. In simulations, technology can identify the rogue contributor without harming other contributors.
	Limitations: Most of the work done is on simulation which brings inaccurate results as compared to experimentation on real-world environment deployments.
Rajab et al., 2020	**Method:** Analyze sybil attacks against shard based protocols[19].
	Outcomes: This article modeled Elastico and defined two sybil attacks, BCP (Break Consensus Protocol) and GFT (Generate Fake Transaction). With system metrics like shard number, capacity, and blockchain network nodes, it can determine attack possibility.
	Limitations: Top blockchain cryptocurrencies and standards like Ethereum, Cardano or Bitcoin etc. were not used targets.
Arslanian & Fischer, 2019	**Method:** Comparison of permission and permissionless blockchain[20].
	Outcomes: This article discusses how blockchain technology is changing the financial services community's viewpoint of financial transaction systems' design. This demonstrates blockchain's features, difficulties, and prospective uses.
	Limitations: Blockchain challenges are well explained in the paper, but solution related to the security challenges is not provided.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 60-81

Lu et al., 2019	**Method:** Three different nodes are evaluated for quality checks[21].
	Outcomes: In this work, author presents an uBaaS platform that offers deployment as a service, design pattern as a service, and support facilities all in one place. This study uses a real-world quality tracing use case to analyze the feasibility and scalability of uBaaS, showing that it is possible and scalable to create and implement blockchain-based applications with uBaaS.
	Limitations: Unified blockchain as a service have been found feasible by authors on the terms of deployment and performance, but they have not marked security of blockchain over cloud.
Wan et al., 2018	**Method:** Hyperledger over cloud deployed on docker cluster[22].
	Outcomes: BaaS is utilized to speed up blockchain implementation in this article. It's a method that may be used by everyone and is straightforward to implement. Author's solution to the problem was to suggest a new perspective. The new paradigm includes scalable components in the blockchain service. Cloud or on-premises, deployment is a simple with these portable parts.
	Limitations: Major focus was on deploying blockchain on docker and cloud, but less emphasis on security.
Chen & Zhang, 2018	**Method:** Serverless architecture[23].
	Outcomes: Using a serverless architecture, this article proposes the first blockchain service model, FBaaS. It makes developing business logic on blockchain networks easier and more efficient.
	Limitations: Storage related issues were faced by author during the deployment of blockchain on server less architecture, but security related configurations were not done by the author.
Wust & Gervais, 2018	**Method:** Author followed a systematic process to identify the optimal technical approach for resolving a specific problem in an application context[24].
	Outcomes: This paper presents the first organized strategy for selecting the best technology solution for each application case (permissionless and permissioned blockchains, and centralized). Author's technique considers trust assumptions, application needs, parties, and technological features like throughput and latency.
	Limitations: Authors have worked on performance parameters like throughput and latency and not have importance to security in blockchain.
Zheng et al.,	**Method:** Comparative study of blockchain technologies[25].

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 60-81

2018	**Outcomes:** In this article, authors provide an in-depth look at the blockchain. In detail it give an overview of the blockchain technologies, blockchain architecture, characteristics, applications, challenges and consensus algorithms.
	Limitations: Author has found limitations in smart contract languages and then plans to do in-depth investigation on smart contract.
Gai et al., 2018	**Method:** In both cases, cloud computing and blockchain technology will be used in combination[26].
	Outcomes: Cloud datacenters are essential to a cloud over blockchain (CoB) implementation, where the blockchain supports a cloud system. Blockchain capabilities, such as tamper-resistant performance, are only used in the subsystems where the blockchain is used (e.g., traceable data usage). This deployment strategy offers simplicity, a verifiable function, and compatibility with existing cloud systems.
	Limitations: Blockchain over cloud have disadvantage that it makes the cloud a blockchain system as a whole.
Puthal et al., 2018	**Method:** Analyzed how blockchain applications are work[27].
	Outcomes: This article provides an overview of blockchain technology for the transparent and secure implementation of security across separated parties. Deployment of the blockchain is only warranted if doing so is both feasible and likely to result in improved security, as well as improved chances of generating more money while spending less. A widespread implementation of blockchain technology would likely have unpredictable results for current society.
	Limitations: Several authors have made the point that blockchain is not a remedy for all transaction security problems.
Park & Park, 2017	**Method:** Different security related issues and solutions of blockchain[28].
	Outcomes: In this study, authors evaluated the current state of research on blockchain technology and associated fundamental technologies. Using blockchain in a cloud computing setting requires consideration of a number of critical problems. With its presentation of a secure blockchain removal and usage protocol, this study offers peace of mind to users.
	Limitations: Although author has discussed and reviewed various security related issues and solutions in deploying blockchain.

7. DISCUSSION OF VULNERABILITY METRICS

The CVSS is a system for sharing information about the nature and severity of software vulnerabilities. Base, Temporal, and Environmental metrics make up the entirety of CVSS.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 60-81

Three types of vulnerability have been identified: those that are intrinsic and remain constant over time and across user environments (represented by the Base group), those that change over time (represented by the Temporal group), and those that are specific to a user's environment (represented by the Environmental group)[29].

7.1. Base metric

Vulnerability's inherent qualities that are stable over time and amongst different user contexts are represented by the base metric set. Scope Metrics, Impact Metrics, and Exploitability Metrics make up the whole.

7.1.1. Exploitability metrics

The features of the vulnerable thing are reflected in the exploitability metrics, which are also referred to as the vulnerable component. All the scores are displayed in relation to the weakest part. The vulnerable component has four parts: Attack vector, Attack complexity, Privileges required, and User interaction. The vulnerable component is often a software application, module, driver, etc. (or possibly a physical device).

i) Attack vector

The attack vector indicates the type of access an attacker would need to exploit the vulnerability. Exploiting a weakness that requires direct access to a system is far more challenging than exploiting a flaw that can be triggered from across the Internet. With the attack vector metric, you can get a score in one of four categories:

- Network (N) – In this category, vulnerabilities can be exploited from anywhere in the world, even across the Internet.
- Adjacent (A) – Adjacency in the network is required to exploit the vulnerability. The attack must originate from the same real or virtual network, such as Bluetooth or IEEE 802.11. (e.g., local IP subnet).
- Local (L) – This rating indicates that the vulnerability cannot be exploited through a network. In order to exploit a system, an attacker must either get access to it directly (through keyboard or console) or remotely (using a protocol such as SSH or Secure Shell), or else rely on social engineering or some other method to get an unsuspecting user to assist in the exploit.
- Physical (P) – The attacker in this scenario must make direct physical contact with the system they are attempting to penetrate. (Attacker decrypts disk after gaining physical access to the system.)

ii) Attack complexity

This metric represents the external factors that an attacker must overcome to successfully exploit the vulnerability. This usually refers to some action on the part of the user or some setting in the intended system. An attack's complexity might be rated as Low or High.

- Low (L) – There is no certain criteria that must be met before exploiting someone.
- High (H) – The success of an attack depends on factors beyond of the attacker's control.
- To carry out this kind of attack, the attacker must first carry out a series of preliminary procedures. Gathering intelligence through surveillance, avoiding or defeating countermeasures, or playing the role of the mediator is all examples.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 60-81

iii) Privileges required

This measure does exactly what it sounds like it would do: it describes the minimum amount of access an attacker must have in order to exploit the system. The necessity of privileges can be categorized in three ways:

- None (N) – The attack can be carried out without the need for any kind of specific permission or access.
- Low (L) – In order to take use of the exploit, the attacker must have "user" level access.
- High (H) – A successful attack requires administrative credentials or equal access.

iv) User interaction

With respect to the user interaction metric, we may learn whether or not the vulnerability can be exploited without the involvement of any users other than the attacker. An easy yes/no indicator, user Interaction measures how often a user takes action.

- None (N) – There is no need for input from the user.
- Required (R) – For this exploit to work, the user must do a series of actions. A user may be forced to install software, for instance.

7.1.2. Impact metrics

The well-known CIA triad (Confidentiality, Integrity, and Availability) of a system is the focus of impact metrics. Anything from a piece of software to a piece of hardware to a network resource could be affected.

i) Confidentiality

Confidentiality refers to the degree to which only authorized users have access to the target data, and it is the opposite of access for unauthorized users.

Generally speaking, there are three measures of privacy:

- High (H) – The compromised system's whole resource set is available to the attacker, including sensitive data like encryption keys.
- Low (L) – The attacker has access to some data but cannot choose which parts they examine.
- None (N) – There is no risk of data exposure because of the vulnerability.

ii) Integrity

When talking about data security, integrity refers to whether or not the data has been altered in any way. Information is considered to have been kept in its integrity if there is no method for an attacker to compromise its validity or completeness. There are three ways to measure integrity:

- None (N) – No data has been compromised in any way.
- Low (L) – The integrity of the protected system can be compromised to some degree, but only to the extent that a small amount of data is tampered with or changed.
- High (H) – All data integrity is destroyed if the attacker is able to change any data on the system.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 60-81

iii) Availability

Information must be available as required. If an attack causes data to become lost, like when a system fails or through a distributed denial of service (DDOS) attack, then availability is compromised. There are three possible measures of availability:

- None (N) – There is no reduction in accessibility.
- Low (L) – In the event of a successful attack, availability may be patchy or performance may suffer.
- High (H) – The affected system or data is no longer accessible in any way.

7.1.3. Scope

While evaluating the scope of a problem, it is important to consider whether or not a given vulnerability could spread to other parts of the system. A shift in scope happens if vulnerability in one component can have an effect on another component that is subject to a different security scope. For the criterion of scope, there are two alternative values:

- Changed (C) – An affected system may affect other systems in the network.
- Unchanged (U) – The vulnerability's impact is restricted to the local security department.

8. CONCLUSIONS

We have provided a comprehensive analysis of the blockchain and its security concerns in this article. It touches briefly on double-spending and sybil attacks, blockchain system flaws, and the CVSS framework. A blockchain always promises to improve the security of data. The research community is focusing on various challenges and problems in blockchain technology from the last decade. The important challenge in blockchain technology is security issues. Some concessions to the original goal of blockchain as outlined in the bitcoin white paper published over a decade ago are necessary to solve the sybil and double spending threats. This research can help security analysts to get good understanding on sybil and double-spending attacks. Firstly, this paper analyzes the review on blockchain classifications and its algorithms. Secondly, concerning security, this article examines both the current state and future prospects of the framework. Also, it will be helpful in the long run to incorporate the blockchain security vulnerabilities into the CVSS framework.

ACKNOWLEDGEMENTS

I'd like to express my gratitude to the Punjabi University, Patiala for providing the resources required to write this research article. I am also grateful to my supervisors for guiding to complete this paper.

REFERENCES

[1] Xu J.J. (2016) “Are blockchains immune to all malicious attacks?,” *Financial Innovation*, vol. 2, no. 1, pp. 1–9.

[2] Sriman B., Kumar S.G., and Shamili P. (2021) “Blockchain technology: Consensus protocol proof of work and proof of stake,” in *Intelligent Computing and Applications*, Springer, pp. 395–406.

[3] Nakamoto S. (2008) “Bitcoin: A peer-to-peer electronic cash system,” *Decentralized Business Review*, pp. 1-9.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 60-81

[4] Wegrzyn K . E. and Wang E. (2021) "Types of Blockchain: Public, Private, or Something in Between | Foley & Lardner LLP". https://www.foley.com/en/insights/publications/2021/08/types-of-blockchain-public-private-between (accessed Dec. 07, 2021).

[5] Ghosh A., Gupta S., Dua A., and Kumar N. (2020) "Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects," *Journal of Network and Computer Applications*, vol. 163, pp. 1-35.

[6] Sayeed S., Gisbert H. Marco, and Caira T. (2020) "Smart contract: Attacks and protections," *IEEE Access*, vol. 8, pp. 24416–24427.

[7] Dwork C. and Naor M. (1992) "Pricing via processing or combatting junk mail," in *Annual International Cryptology Conference*, Springer, pp. 139–147.

[8] Jakobsson M. and Juels A. (1999) "Proofs of work and bread pudding protocols," in *Secure Information Networks*, Springer, pp. 258–272.

[9] Ledger S. (2019) "What is Proof-of-Work | Ledger". https://www.ledger.com/academy/blockchain/what-is-proof-of-work (accessed Dec. 06, 2021).

[10] Bashar G., Hill G., Singha S., Marella P., Dagher G. G., and Xiao J. (2019) "Contextualizing consensus protocols in blockchain: A short survey," in *First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications*, IEEE, pp. 190–195

[11] Nguyen G. T. and Kim K . (2018) "A survey about consensus algorithms used in blockchain," *Journal of Information Processing Sys*tems, vol. 14, no. 1, pp. 101–128.

[12] Asfia U., Kamuni V., Sutavani S., Sheikh A., Wagh S., and Singh N. M. (2019) "A blockchain construct for energy trading against sybil attacks," in *27th Mediterranean Conference on Control and Automation*, IEEE, pp. 422–427.

[13] Swathi P., Modi C., and Patel D. (2019) "Preventing sybil attack in blockchain using distributed behavior monitoring of miners," in *10th International Conference on Computing, Communication and Networking Technologies*, IEEE, pp. 1–6.

[14] Singh R. and Singh S. (2011) "Detection of Rogue Base Station using MATLAB," International journal of soft computing and engineering, pp. 198-201.

[15] Iqbal M. and Matulevičius R. (2021) "Exploring Sybil and Double-Spending Risks in Blockchain Systems," *IEEE Access*, vol. 9, pp. 76153–76177.

[16] Platt M. and McBurney P. (2021) "Sybil attacks on identity-augmented Proof-of-Stake," *Computer Networks*, vol. 199, pp. 1-12.

[17] Begum A., Tareq A., Sultana M., Sohel M., Rahman T., and Sarwar A. H. (2020) "Blockchain attacks analysis and a model to solve double spending attack," *International Journal of Machine Learning and Computing*, vol. 10, no. 2, pp. 352–357.

[18] Gong S. and Lee C. (2020) "Blocis: blockchain-based cyber threat intelligence sharing framework for sybil-resistance," *Electronics*, vol. 9, no. 3, pp. 1-20.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 60-81

[19] Rajab T., Manshaei M. H., Dakhilalian M., Jadliwala M., and Rahman M. A. (2020) "On the feasibility of sybil attacks in shard-based permissionless blockchains," arXiv preprint arXiv: 2002.06531, pp. 1-10.

[20] Arslanian H. and Fischer F. (2019) "Blockchain as an enabling technology," in *The Future of Finance*, Springer, pp. 113–121.

[21] Lu Q., Xu X., Liu Y., Weber I., Zhu L., and Zhang W. (2019) "uBaaS: A unified blockchain as a service platform," *Future Generation Computer System*, vol. 101, pp. 564–575.

[22] Wan Z., Cai M., Yang J., and Lin X. (2018) "A novel blockchain as a service paradigm," in *International Conference on Blockchain*, Springer, pp. 267–273.

[23] Chen H. and Zhang L. J. (2018) "Fbaas: Functional blockchain as a service," in *International Conference on Blockchain*, Springer, pp. 243–250.

[24] Wüst K. and Gervais A. (2018) "Do you need a blockchain?," in *Crypto Valley Conference on Blockchain Technology*, IEEE, pp. 45–54.

[25] Zheng Z., Xie S., Dai H. N., Chen X., and Wang H. (2018) "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375.

[26] Gai K., Choo K. K. R., and Zhu L. (2018) "Blockchain-enabled reengineering of cloud datacenters," *IEEE Cloud Computing*, vol. 5, no. 6, pp. 21–25.

[27] Puthal D., Malik N., Mohanty S. P., Kougianos E., and Yang C. (2018) "The blockchain as a decentralized security framework [future directions]," *IEEE Consumer Electronics Magazine*, vol. 7, no. 2, pp. 18–21.

[28] Park J. H. and Park J. H. (2017) "Blockchain security in cloud computing: Use cases, challenges, and solutions," *Symmetry*, vol. 9, no. 8, pp. 1-13.

[29] "CVSS Base Score Explained," (2020) "*Balbix*". https://www.balbix.com/insights/base-cvss-scores/ (accessed Feb. 09, 2022).

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 60-81

Authors

Ramanpreet Singh has completed his Masters of Technology in Computer Engineering in 2011 from Yadavindra College of Engineering, Punjabi University Guru Kashi Campus, Talwandi Sabo, Bathinda, Punjab, India and pursuing PhD from Department of Computer Engineering, Punjabi University, Patiala. I am working as an Assistant Professor in Department of Computer Engineering, YCOE, Punjabi University Guru Kashi Campus, Talwandi Sabo, Bathinda, Punjab, India. My research interests are Worldwide Interoperability for Microwave Access and Blockchain Technology.

Sukhwinder Singh Sran, completed his Doctorate from Department of Computer Engineering, Punjabi University, Patiala in 2018 and Masters from YCOE, Punjabi University, Patiala in 2007. He is working as Assistant Professor in Department of Computer Science and Engineering, Punjabi University, Patiala, India. He has guided around 50 students in dissertation of master programs and many students are currently pursuing their PhD under him. His research interests are in wireless sensor networks, internet of things and energy aware routing in MANET.

Meenakshi Bansal, presently working as Assistant Professor in Yadavindra Department of Engineering, Punjabi University Guru Kashi Campus, Talwandi Sabo. She has completed her doctorate in 2019 from Punjab Techinal University, Jalandhar, M.Tech from Punjab Agriculture University Ludhiana in 2006 and B.Tech from MIMIT, Malout in 2004 all in Computer Science and Engineering. Her areas of research are Data Security, Networking and NLP. Around 40 students have done Post Graduation thesis under her guidance and 4students have been enrolled under her for Ph.D. She has around 40 research paper to her credit in good journals (that include Scopus and UGC Care).