Third International Conference on "Materials, Computing and Communication Technologies"
International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

A Comprehensive Analysis of Blockchain Cyber Attacks, Problems, and Considerations

Mrs. M. Sharon Nisha[1], Dr. S. Raja Ratna[2]

[1]Department of Computer Science and Engineering, Francis Xavier Engineering College Tirunelveli, Tamil Nadu, India

[2]Department of Computer Science and Engineering, V V College of Engineering Tisayanvilai, Tamil Nadu, India

Article Info
Volume 8, Issue 7
Page Number : 47-57
Publication Issue :
May-June-2022
Article History
Accepted: 01 June 2022
Published: 20 June 2022

ABSTRACT

They examined Blockchain technology and their influence on companies and sectors in this paper. Decentralization, immutability, consistency, and privacy hashed algorithms are all supported by blockchain. This systematic study aids our understanding of the cryptocurrency and information security environment, including blockchain security on the Iot devices (IoT), Sidechain secure, and Blockchain Security for Artificial Intelligence Data. We've also gone over the Blockchain network and its applications.

Keywords—blockchain, security, decentralization

I. INTRODUCTION

The essential principles of blockchain technology were initially articulated during the 1980s. After a group or individual known as Satoshi Nakamoto produced a whitepaper titled "Bitcoin: a peer-to-peer electronic money system" in 2008, it gained momentum. It eliminates intermediary services, cuts transaction costs, minimizes the danger of fraud, and speeds up transaction times. Bitcoin is a cryptocurrency that can be used to trade things on the internet in the same manner that we do in real life. Following the spectacular success of cryptocurrencies, blockchains are now being utilized in a range of areas, including supply chain management, digital identity, medical, wills, food security, voting, and real estate. However, as the significance of technology in our everyday lives has expanded, hackers have had more options to engage in criminality. For instance, the 51 percent attack is a well-known security issue that hackers seek to exploit in order to acquire control of a computer [1].

Blockchain is a cryptographically secured distributed, decentralized, and immutable ledger.

Algorithms for hashing It's an integrated and multi infrastructure construction that integrates peer-to-peer network (P-to-P) and employs distributed consensus technique to handle normally distributed database synchronize problem.

Six important components make up blockchain technology.

- **Redistribution:** One of the finest aspects of blockchain is that it eliminates the hegemony of central nodes by allowing nodes to cooperate and participate in decision-making via the use of various consensus methods.
- **Accountability**: Blockchain is a distributed ledger that is updated every time a new block is confirmed and added. This means that everyone on the network can see what you're doing. The ledger whenever they desire, guaranteeing that the blockchain is transparent.
- **Confidentiality and privacy**: Personal identification is kept concealed by utilizing the created wallet address in blockchain transactions. To maintain complete anonymity, several addresses are utilized.
- **Inalterable**: Every node in the networks stores a copy of the ledger, making it unchangeable until someone gains control of 51 percent of the network at once.
- **Open-source license**. Because blockchain is open source, anybody may design any application using it. The ledger is also open to the public and may be seen by any participant of the network.
- **Sovereignty**: Because the interactions are created on consensus, any device may securely send and receive data.

II. ARCHITECTURE FOR BLOCKCHAIN

Blockchain is a cryptographically connected series of ordered backlinked blocks. Each block comprises data, a timestamp, a block hash and a parental block (prior block) hash, as well as a Merkel root. The genesis block is the very first block. First, the transactions are hashed, and then a Merkle trees of all these hashes is produced. To retain the chronological sequence, each transaction has a timestamp linked to it.

- **Block**: A block is a data structure containing a hashing oneself, a hash of its hash of the previous block, transactions, the Merkle root, timestamp, and other information. The genesis block is the first block on the blockchain. The parent block is the block that came before it.
- **Hash**: Because each block's hash is always unique, it may be compared to a fingerprint. Any complicated function h may be used to create a hash (x). Any minor change in the work points has a significant impact on the output. Highly sophisticated algorithms like SHA-256 may be used to create a cryptographic safe hash. As an example,

TABLE I. MD% AND SHA256 ALGORITHM SAMPLE I/P AND O/P

Hash Algorithm	Input	Output
MD5	Paritosh Durgesh	DED0BFAA4806AEA1 26C004B6BD9253E1
Hash Algorithm	Input	Output
	Paritosh Durgesh	561FC50124DBC20CE 7F5D7B9F14845EA
SHA256	Paritosh Durgesh	C2FDE2E7F29742C22 F8EAC4A0BEC0EE7D F343B611BCAF3AB3 AC97067574530C

	Paritosh Durgesh	3B8C09F31065141F601 A039A70801B6042DD A62F5E1B2EBB96A09 C4FBC557DA9

- **Merkle tree**: It is described as a tree data structure in which the tree nodes are connected by hash pointers. A Merkle tree structure is used to organize blockchain transactions. The Merkle Tree is created by combining the hashing of all nodes. [1] The pair hash value of each child is computed until there's no one remaining. Merkel Root, or the Root Hash, is the name given to this hash. The Merkle tree has the benefit of allowing us to confirm data integrity and authenticity.
- **Time and date**: It is the timestamp because when block is produced, and it also aids in transaction validation.
- **Altitude**: The ambiguity determines how tough it is to compute a hash criterion for a particular target. With each increase in block creation speed, the difficulty level rises. This serves as a defense against attacks or greedy miners.
- **Nonce**: It's of the once pseudo-random number used in the mining process. Data might well be paired with a cryptographic nonce to create various hash digests per nonce: $digest = hash\,(data + nonce)$
- **Block Header**: Block version, preceding reference hash, Hash root, time zone, difficulty, and nonce are all included in the block header. A block has a distinctive preamble that is being used to identify it in the chain as a whole [2].
- **Other assets**: The every one of the additional data that the user has defined

III. BLOCKCHAIN STRUCTURE AND OPERATION

Transactions are protected by an encryption code that includes the sender, the recipient, and the transaction information.

- **Definition of a transaction**: It is the initial step of the transaction, in which the sender generates the transaction using the receiver's public name and address and a cryptographic digital signature that certifies the transaction's authenticity and validity.
- **Authentication of transactions**: The message is temporarily retained until the nodes authenticate the transaction that was used to generate the block, while nodes conduct message validation by cryptographically decrypting digital signatures.
- **Creating Blocks**: One of the network's nodes uses pending transactions to update the state of the network. At a certain time period, the block or ledger, as well as this modified block, is exposed to networks waiting for validation.
- **Validation of blocks**: When a node in the network receives the request for latest update block validation, they go through a repetitive process in which they seek the approval of other nodes in the network to authenticate the block.
- **Block chaining**. When all of the transactions in the current block have been approved, a new block is appended to it, and the current state of the block is displayed to the other blocks in the system [3].

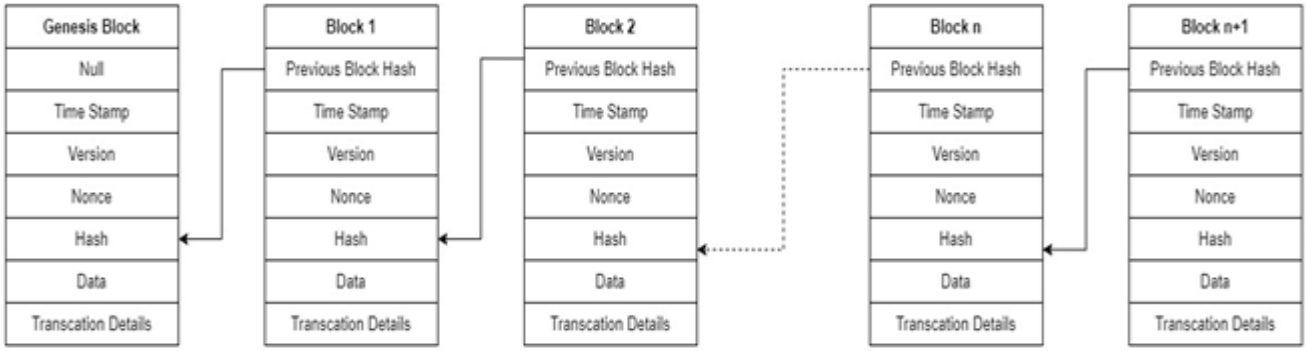

Fig. 1. Working of Blockchain

A. Proof of Work (PoW)

Markus Jakobsson and Ari Juels created the phrase "proof of work" in a paper released in 1999. The cryptocurrency Proof-of- Work consensus procedure is the most prevalent and oldest consensus approach. Every node (miner) that wished to participate in the consultation process must offer their solution to tackle the mathematical problem in the proof of work consensus process. These uncommon arithmetic tasks are referred to as complex mathematical problems. Furthermore, fixing these challenges demands a large amount of processing capability. Mining is a phrase used to describe the act of producing rewards for whoever answers a puzzle. The proof of work agreement certifies that the node supplying the block isn't actually malevolent as it has spent some computing capabilities as proof of work. When the miner finds the appropriate Nonce, it is given permission to create a new element and store the activities within it. The block is subsequently broadcast to the full blockchain network. Other nodes may accept or reject this block for verification. The block is added to their chain if it is accepted.

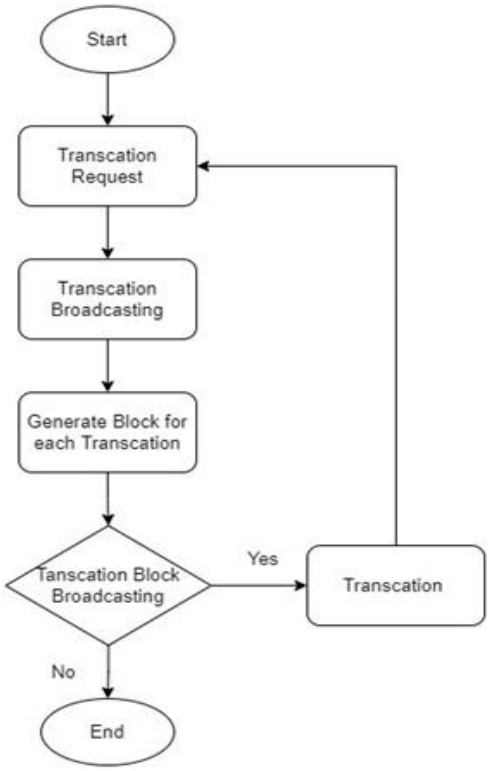

Fig. 2. Flow chart of Consensus Algorithms

Due to the complexity of the undertaking, PoW diminishes the possibility of a 51 percent attack. That if someone tampers with a block, the hash of the block will be modified, making it invalid. This implies that he will have to reset the hash for all following blocks, which is not a tough process in the age of supercomputers. PoW addresses this problem by restricting the amount of new data blocks that may be produced. A miner can only create a Bitcoins block ever 10 minutes on the bitcoin network.

B. Proof of Stake (PoS)

As previously said, proof of work miners must solve a hard issue that necessitates a large amount of computer power and energy. Furthermore, only the quickest node has the privilege to construct a block, implying that all other nodes' efforts and computation are useless. Furthermore, if 51 percent of miners get the ability to mine quicker than others because of having more energy to mine than those of other mining, he may even be able to govern the whole permissioned blockchain. Proof of stake solves this issue since only shareholders may participate in the block generation process, which is called validators. This prevents the circumstance where one node controls the network because no one node can have 51 percent
of the network's money. A single node has a chance to purchase the network at initially, since as the network increases, it becomes extremely hard for the average node to have enough money to hold 51 percent integrity of the whole network. If the wealthiest person is dishonest and wants to seize control of the network, he will need to have more than 50 percent of the network's money. This solution employs a limited number of consensus processes and requires substantially less energy [4].

C. Delegated Proof-of-Stake (DPoS)

"Dan Larimer" presents the Authorizing Proof of Stake approach, which is applied in the BitShare project. The democratic variation of something like the proof of stake consensus process, Delegated Proof of Stake, contains a voting system in which token holders vote in real time for witnesses and delegates. The number of persons varies from 21 to 101. Witnesses are structural framework for witnessing the transaction, verifying the signatures, and timestamping it; they are not authorized to trade. They each create one block every three seconds, and if a witness fails to perform the job within the time limit, it is discarded and substituted by the next one. Each network node has the opportunity to vote for their own trustworthy witnesses, and the more bitcoin interests he has, the more likely he is to be a witness. However, since each witness node generates blocks in turn, the identification of the witnesses already is known and constantly constant, making the bitcoin blockchain more susceptible to collusion assaults.

TABLE II. ALGORITHM EFFICIENCY

Algorithm	Advantages	Drawbacks
Proof of Work (PoW)	Ensures a stable network. Decentralized network that is equitably powered and governed.	Requires a lot of computing power and a lot of energy. Small networks are particularly susceptible.
Proof of Stake(PoS)	Provides quicker transaction. Efficient use ofresources.	Less decentralized network as compared to PoW.

Delegated Proofof Stake (DPoS)	Quicker than PoW andPoS Good protection from double-spending. Sustainable and more scalable as requires less power and hardware resources.	Limited number of witnesses can lead to centralization of network. AF

In many circumstances, witnesses are asked to deposit a portion of the locked money. If the witnesses fails to authenticate or engages in malevolent behaviour, he will be penalized, resulting in a financial loss. Because it is a democracy concept, the witness must keep their good name in order to be chosen. As a result, DPoS uses less effort and compute resources, allowing it to process more transactions and give quicker information and establishing than PoW and Operating systems while being extremely energy efficient.

IV. BLOCKCHAIN TECHNOLOGIES IN ACTION

Following the introduction of blockchain in bitcoin, it has gained popularity and may be utilized in a variety of fields, including banking, health care, and so on.

A. Bitcoin

Bitcoin is a digital currency invented by Satoshi Nakamoto in 2008. That was the first instance blockchain technology had been employed. It utilizes a decentralised system, cryptography, and a Proof of Work algorithm for negotiation on the construction of a public blockchain to enable mentoring exchange of value in the electronic medium. Bitcoin's value is directly related to the number of active users on the network [5].
Satoshi Nakamoto created the first new blocks of bitcoin when he delivered 10 Bitcoins to famed developer Finney and accomplished the first transaction.

B. Banking

The existing Baking mechanism has been surpassed by Blockchain. Due to the cryptographic algorithms' validation process, transactions on the blockchain may be completed in seconds. It removes the need for expensive and time- consuming third-party validation along a payment processing money transfer. It is projected that by eliminating the third party, cryptocurrency n technology saves $20 billion over the transaction.

C. Healthcare

Smart contracts on the blockchain might have a significant influence on healthcare. Smart contracts, whose key is handed to the patient, may be used to store patient information on the blockchain.

D. Internet of Things

The Internet of Things (IoT) is a network of connected devices that can interact with one another and collect data for analysis. The network's security is selected by the device with the least security. The combination of technologies has the ability to increase secure communications while simultaneously enhancing privacy agreements [6].

E. Hyperledger

Hyperledger is an open-source initiative that intends to offer a dependable set of foundations, technologies, including modules for enterprise-grade blockchain deployments. The Linux Foundation offers an international collaboration that comprises specialists in finance, banking, the Internet - Of - things, distribution networks, manufacturing, and technology. Individual programmers, services and system integrators, government organizations, corporate members, and end-users are all invited to join in the creation and refinement of the aforementioned game-changing innovations through technical governance and open collaboration.

Hyperledger, such as the Linux Foundation, takes a flexible approach to project hosting. Through Blockchains Labs (seed) to stable code suited for production, this Hyperledger greenhouse hosts evolving corporate blockchain initiatives (fruition). Everyone is interested in contributing to the greenhouse, which will help to further the industry's shared system and smart contract ambitions [7].

V. VULNERABILITIES, ATTACKS, AND CHHALLANGES IN THE BLOCKCHAIN

A. Malleability attack

A malleability attack occurs when the transaction's unique ID is modified before it is confirmed on the network. The most typical method for this to happen is when the transaction signatures, which is in charge of producing the transaction ID, is changed. The data Format will change if this signature is changed, rendering the prior transaction ID invalid. This update allows the attacker to make it seem as though a transaction never took place. This assault went off without a hitch [8].

B. Nothing at Stake Problem

With PoS-based blockchain networks, this is a potential problem. The problem occurs when two validators submit the same block at the same moment, splitting the blockchain. Voting both sequences is in the validator's best interest. Because there are no costs involved with mining. Mining both chains assures the voter's mining gain regardless of which fork wins. The attacker might exploit this situation by splitting the network in one transaction before spending any money. If the miners mine both chains but the attacker only mines his, the attacker's fork will become the longest, resulting in a double-spend scenario.

C. Majority Attack

When a miner or mining pool with considerably more than 50% of something like the network's hashing power participates in aggressive behavior, this is known as a 51 percent attack. This is the most well-known attack against public blockchains. When a single miner or mining pool controls the majority of hash power, this is known as a monopoly. The 51 percent attack aims to make a twofold investment. To launch such an attack, the miner will need to control the majority of the hash rate.

D. Selfish miner attack

This seems to be an attack in which a mining pool or individual miner finds a viable alternative but does not inform the rest of the network. To maintain its advantage, the selfish miner proceeded to extract on the block's top edge. Because when the rest of the system is about to catch up to you. The arrogant miner then releases his share of the decrypted blocks. Their chain wins as a result of anything like the game's adds another level

regulations. claiming the block prize in PoW The efforts of the other miners were ultimately vain, and they lost money. On the one hand, if such an attack is successful, the chain's trust would be destroyed, and the attacker's staked coins will lose value. On the other hand, the sum of money necessary to get such a massive quantity of electricity is usually prohibitively high.

E. Sybil attack

A Sybil assault occurs when a node tries to dominate a peer-to-peer network by assuming many identities at the same time. The attacker tries to acquire control of the whole network. Because a Proof of Stake blockchain network has a voting process that enables an attacker to vote for flawed transactions to make them legal, this attack is relevant. This attack is seldom feasible because to stake constraints [9].

F. Double Spending

The attacker will fork the chain, creating two separate chains, one public and the other privately mined. The vengeful actor sends a huge transaction on the public blockchain. Once the things have been received, provide a single transaction for goods/services. The transaction is verified on the public chain. He would continue to grow the private chain in the meanwhile. After receiving the goods/services, the attacker made the private chain public. Because the private chain has a higher hash rate than the broadcast chain, forcing the broadcast chain to revert also forces a rogue user's transaction to be reverted.

G. Blocking Transactions

The rogue miner has complete control over which transactions were involved in the a block [10].

H. Double Spending Attack

Whenever a completed transaction is replicated with the identical money, this is produced. When a bitcoin blockchain is interrupted, this issue is unique to digital money. When an attacker sends several photons to the network, the transaction is reversed, making it seem as though it never occurred. 51 percent operation, Racing Attacker, Hathaway Inflict damage, Quaternion 76 threats (composite of Race Assassination attempt and Finney Attack), and alternative transaction attack are all attacks connected to double spending.

I. DDOS (Distributed Denial-of-Service) attack

When an attacker floods the target or related equipment with malicious activity, this is known as a distributed denial of service attack (more traffic than the server or network can accommodate). Zombies, which are remotely controlled, hacked computers or bots, are used to do this. A botnet, or computer network, is made up of them. This is used to initiate a DDoS attack, with the goal of blocking genuine users from accessing resources. Botnets may be made up of tens of thousands of devices. It's hard to detect the difference in a DDoS attack since the attack traffic looks so similar to legitimate traffic. DDoS assaults have been shown to be a resource war between attackers and defenders. The more resources you have, the more likely you are to succeed as an attacker. All communication between the controller and the attack is often encrypted, making the attack untraceable. Attackers are spoofing MAC[11]. DDoS assaults may be categorized into three types. Application layer assaults, resource depletion attacks, and volumetric attacks are all possible.

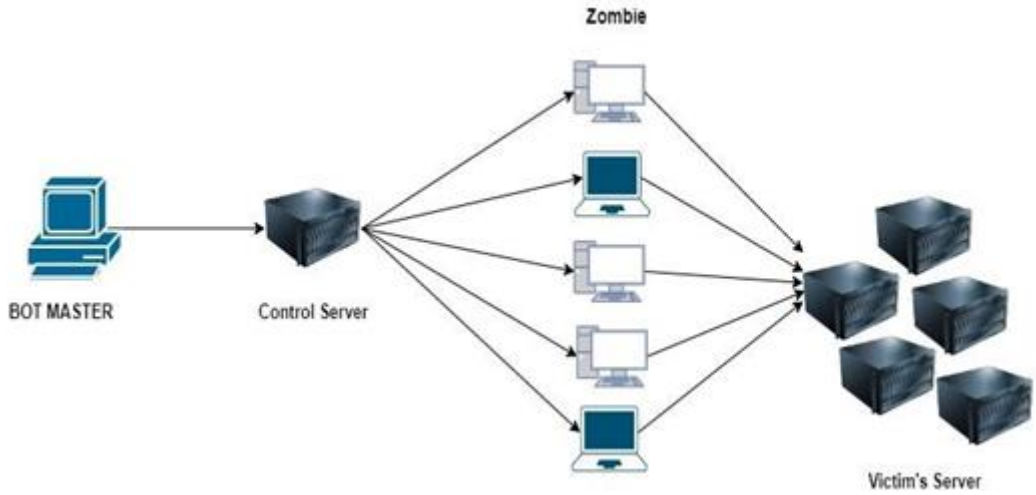

Fig. 3. DDoS Attack

J. Blockchain Poisoning

The blockchain is stuffed with personal information (names, residences, and credit card numbers) as well as unlawful files in this assault (malware, malicious content). A malevolent user may compel cryptocurrency networks to download malicious data, which might result in DoS or DDoS assaults on the blockchain. This may put the connection in violation of the law. Because blockchain is unchangeable, deleting these files is difficult. As a consequence of this assault, the impacted chain can no longer be utilized unless costly and time-consuming efforts to delete these files are conducted.

VI. CHALLENGES

A. Scalability

After In this attack, the blockchain is loaded with personal information (names, addresses, and credit card details) as well as illegal downloads. A malicious user might force bitcoin nodes to get malicious data, resulting in DoS or DDoS attacks on the blockchain. This might put the networks in legal trouble. Delete these files is impossible due to the immutability of blockchain. As a result of the attack, the chain in question can no longer be used unless expensive and time- consuming measures are made. As a consequence of Bitcoin's huge success, the scalability challenge of something like the Ethereum blockchain has been emphasized. For a particular number of transactions to be handled, the quantity of bytes and block generation time are specified, which is effective against the dangers described above. However, if there are a significant number of transactions, transaction processing may take longer. Many blockchain systems, such as Bitcoin, which has a 1MB block size and a 10 minute average block confirmation time, although Ethereum has a 15 second block confirmation time, have scalability difficulties. For a high number of transactions to be handled, the transaction verification time must be quick, yet the average time must be lengthy to prevent being attacked by an attacker. The scalability trilemma is the major issue that blockchain is dealing with. Vitalik Buterin (the Ethereum founder) used the term to illustrate how the three ideal attributes of democratization, scalability, and security cannot all be realized at the same time. According to the trilemma, any two of the three may be kept while the third is abandoned. Furthermore, owing to the high computer power needed, blockchain-based on PoW consensus,

such as bitcoin, has increased energy use. The developers of [14] note an existing solution to the scalability problem, which is to delete these files.

B. Storage Management

To increase security, the blockchain ledger is disseminated to all network nodes. Beginning with the initial block from the blockchain network and ending with the most current block mined, the ledger preserves all of the chain's blocks. A considerable quantity of space is needed as a result of the redundancy. The Bitcoin blockchain is around 16.5 GB in size and expanding at a pace of about 1 MB per hour. Bitcoin now has over a million nodes, occupying about 1.5736 petabytes.

C. Lack of control and regulation

Because cryptocurrency is a decentralized network, no third party is required to verify transactions in permissioned blockchain networks. Many individuals have experienced a variety of problems and have lost huge amounts of money as a result. The blockchain network must be established in order to assure interoperability, governance, and long-term survival, among other things.

VII. CONCLUSION

Blockchain is a developing technology that will transform the IT industry. Because of its decentralization and peer-to- peer qualities, it may be used in a variety of industries including healthcare, IoT, management, and so on. Although, as highlighted in the study, there are several areas where development is needed for improved technology adoption. As time goes on, the technology becomes more sophisticated and stable.

Decentralization, transparency, and immutability are just a few of the benefits of blockchain technology. At the same time, the study discusses a number of different assaults, obstacles, and concerns. Since there is no foreign entity engaged, legislation for technological regulation are also required. This will also aid in the development of trust, which would also aid the user acceptance.

VIII. REFERENCES

[1]. Sidra Aslam , Aleksandar Toši´c and Michael Mrissa," Secure and Privacy-Aware Blockchain Design: Requirements, Challenges and Solutions,"in mdpi journal, 1, 164–194, march 2021;

[2]. Saurabh Singh, A. S. M. Sanwar Hosen and Byungun Yoon, (senior member, IEEE)," Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network," in IEEE access,2021

[3]. Nils Amiet," Blockchain Vulnerabilities in Practice", Digital Threats: Research and Practice, Vol. 2, No. 2, Article 8,March 2021

[4]. Erjon Hasanaj,"blockchain and its security issues and challenges, "in Researchgate, march 2019

[5]. Prasanth Varma Kakarlapudi and Qusay H. Mahmoud," A Systematic Review of Blockchain for Consent Management," in mdpi journal , Healthcare 2021, 9, 137.

[6]. Arun kumar, Akhilendra pratap Singh ,P.H.J.Chong ," blockchain: basics, applications, challenges and opportunities ,"in researchgate, jan 2021.

[7]. Iuon-Chang Lin and Tzu-Chun Liao," A Survey of Blockchain Security Issues and Challenges," International Journal of Network Security, Vol.19, No.5, PP.653-659, Sept. 2017

[8]. Min-Bin Lin ,Kainat Khowaja ,Cathy Yi-Hsuan Chen and Wolfgang Karl H¨ardle," Blockchain mechanism and distributional characteristics of cryptos," IRTG 1792 Discussion Paper 2020- 027.

[9]. blockchain technology, Available online: (https://www.leewayhertz.com/blockchain-technology-explained/#:~:text=A%20block%20can%20be%20considered%20as%20a%20page,a%20block%20depends%20on%20the%20type%20of%20blockchain) (accessed on march 2020)

[10].Application of blockchain, Available online (https://www.businessinsider.in/finance/news/the-growing-list-of- applications-and-use-cases-of-blockchain-technology-in-business- and-life/articleshow/74447275.cms) (accessed on march 2020)

[11].Sahil Gupta , Shubham Sinha , Bharat Bhushan," Emergence of Blockchain Technology: Fundamentals, Working and its Various Implementations," International Conference on InnovativeComputing and Communication (ICICC 2020)

[12].Sharyar Wani , Mohammed Imthiyas , Hamad Almohamedh ,, Khalid M Alhamed , Sultan Almotairi , and Yonis Gulzar," Distributed Denial of Service (DDoS) Mitigation Using Blockchain—A Comprehensive Insight",mpdi journal, jan 2021

[13].Fan Yang , Wei Zhou, Qingqing Wu , Rui Long , Neal N. Xiong , (Senior Member, IEEE), And Meiqi Zhou," Delegated Proof of Stake With Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism,"IEEE access,august 2019.

[14].Huawei Huang and Zibin Zheng "Solutions to scalability of blockchain: A Survey": School of Data and Computer Science, Sun Yat- sen university, Guangzhou 510006, China: IEEE Access, jan 2020

[15].Sidra Aslam, Aleksandar Tošić and Michael Mrissa," Secure and Privacy-Aware Blockchain Design:Requirements, Challenges and Solutions" journal of Cybersecurity and Privarcy, 2021, 1, 164–194 March 2021.