International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

A Systematic Review on Blockchain Security Attacks, Challenges, and Issues

[1]Paritosh Banchhor, [2]Durgesh Sahu, [3]Ankit Mishra, [4]Mohammed Bakhtawar Ahmed
[1] Department of Computer Science, Amity University Chhattisgarh
[2] Department of Computer Science, Amity University Chhattisgarh
[3] Assistant Professor, Department of Electrical and Electronics, Amity University Chhattisgarh
[4] Assistant Professor, Department of Computer Science, Amity University Chhattisgarh

***Abstract*:- In this paper, we have discussed Blockchain technologies and their impact on businesses and industries. Blockchain supports Decentralization, Immutable, Consistent, and Security Hashed Algorithms. This systematic review helps us to understand the blockchain and cybersecurity space, such as the security of blockchain on the Internet of Things (IoT), Sidechain security, and Security of Blockchain for Artificial Intelligent Data. We have also discussed** the **Blockchain architecture and its uses.**

Keywords: Blockchain, Security, decentralization

I. INTRODUCTION

The core ideas behind blockchain technology emerged in the late 1980s and early 1990s. It gained momentum after a person or group called with a pseudo name Satoshi Nakamoto published a whitepaper titled "Bitcoin: a peer-to-peer electronic cash system" in 2008. It eliminates intermediary services, reduces the risk of fraud, speeds up transaction time, and lowers transaction costs. Bitcoin is a digital currency used to trade for commodities on the internet as we do in real life. After the huge success of bitcoin, blockchains are engaged in other fields including supply chain, Digital IDs, Healthcare, Wills, Food safety, voting, real estate. But as the contribution of this technology in our day-to-day life grew, cybercriminals also got new opportunities to get engage in cybercrimes. For example, the 51% attack is one of the famous security issues that hackers try to take advantage of to gain control of the machine.[1]

Blockchain is a distributed, decentralized, and immutable ledger secured by cryptographic.

hash algorithms. It contains cryptography, mathematics, Algorithm, and economic model, combining peer-to-peer network (P-2-P) and using distributed consensus algorithm to solve traditionally distributed database synchronize problem, it's an integrated multi-field infrastructure construction.

Blockchain technology consists *of six key elements.*

Decentralization: is one of the best features of blockchain which removes the dominance of central nodes as the nodes collaborate to take part in decision making with the help of different consensus algorithms.
Transparency: Blockchain is a decentralized distributed ledger that gets updated whenever a fresh block is confirmed and added. This means that anyone in the network can see the ledger whenever they want to thus provide transparency to the blockchain.
Anonymity: In blockchain transactions are made using the generated wallet address and personal identity is kept hidden. Multiple addresses are used to ensure full anonymity.
Immutable: Copy of the ledger is stored by each node in the network which makes it immutable unless anyone can gain control over 51% of the network at a time.
Open source: anyone can create any application using blockchain as it is open source. Ledger is also available publicly which can be checked by any member of the network.
Autonomy: as the transactions are based on consensus therefore every device can safely transfer and update data.

II. BLOCKCHAIN ARCHITECTURE

Blockchain is the chain of ordered backlinked blocks linked using cryptography. Each block comprises data, timestamp, a hash of the block and a hash of the parent block (previous block), and a Merkel root. The first block is known as the genesis block. Transactions are first hashed and a Merkle tree of these hashes is formed. The timestamp is associated with each transaction to maintain the chronological order.

Block: A block can be considered as a page in the ledger it is a data structure that contains a hash of itself, a hash of its parent block, transactions, Merkle root, timestamp, etc. The first block in the blockchain is known as the genesis block. The previous block is known as the parent block.

Hash: A hash can be considered as a fingerprint as it is always unique for each block. A hash can be performed using any complex function h(x). Any small change in the input x will drastically change the output. To make a cryptographic secured hash, highly complex algorithms like SHA-256 can be used. For example

Hash Algorithm	Input	Output
MD5	Paritosh Durgesh	DED0BFAA4806AEA126C004B6BD9253E1
	Paritosh, Durgesh	561FC50124DBC20CE7F5D7B9F14845EA
SHA256	Paritosh Durgesh	C2FDE2E7F29742C22F8EAC4A0BEC0EE7DDF343B611BCAF3AB3AC97067574530C
	Paritosh, Durgesh	3B8C09F31065141F601A039A70801B6042DDA62F5E1B2EBB96A09C4FBC557DA9

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

Merkle tree. It is defined as a binary search tree in which tree nodes are linked to each other using hash pointers. The blockchain transactions are arranged in a Merkle tree structure. The hashes of all nodes are combined to create the Merkle Tree.[1] Each child's pair hash value is repeatedly calculated until there is only one left. This hash is known as Merkel Root or the Root Hash. An advantage of the Merkle tree is that it allows us to prove both integrity and validity of data.

Timestamp: It is the time when the block is generated this also helps in validating a transaction.

Difficulty: The difficulty is the value that decides the difficulty level to calculate a hash threshold for a given target. The level of difficulty increases with the increase in the speed of block formation. This acts as a protective layer from attackers or greedy miners.

Nonce: It is a pseudo-random number used only once during the mining process. A cryptographic nonce can be combined with data to produce different hash digests per nonce:

hash (data + nonce) = digest

Block Header: The block header contains block version, previous block hash, Hash root, timestamp, difficulty, and nonce. A block contains a unique header that is used to identify the block in the entire chain.[2]

Other data: all the other data defined by the user.

III. WORKING OF BLOCKCHAIN

Transactions are secured by an encryption code and composed of the receiver, the transaction information, and the sender.

Transaction definition. It is the initial step where the transaction is created by a sender that holds the receiver's public address information and a cryptographic digital signature that verifies the credibility and validity of the transaction.

Transaction authentication. The message is held temporarily until the nodes validate the transaction used to create a block as nodes perform the message validation by decrypting digital signature cryptographically.

Block Creation. Pending transactions are used by one of the nodes in the network to update

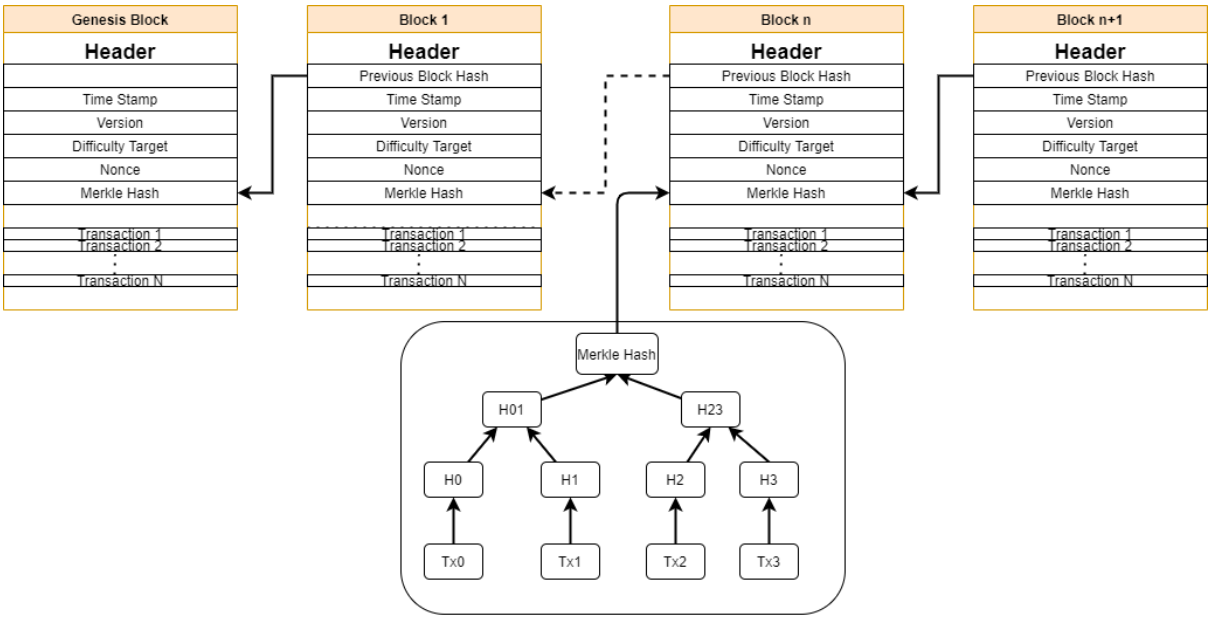


Fig (1) : WORKING OF BLOCKCHAIN

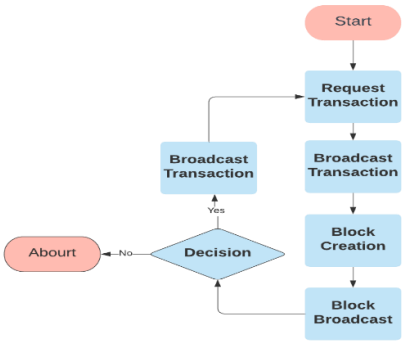
the block or ledger and this updated block is shown to nodes waiting for validation at a particular time interval.

Block validation. In-network when a node receives a request for updated block validation, they perform a repetitive process where nodes seek other nodes' acquiescence in the network to verify the block.

Block chaining. A new block is attached to the present block when all the transactions are approved in the block and conclude in showing the latest state of the block to the remaining block in the network.[3]

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

IV.CONSENSUS ALGORITHMS



Fig(2): Flow chart of CONSENSUS ALGORITHMS

A. Proof of Work (PoW):

The term "Proof of work" was coined by Markus Jakobsson and Ari Juels during a
document published in 1999. The blockchain Proof-of-Work consensus algorithm is the oldest consensus mechanism and the most popular algorithm. In the proof of work consensus process, every node (miners) which wants to participate in the consensus process has to contribute its resources to solve the mathematical puzzle. These complex mathematical problems refer to a diversity of uncommon arithmetic complications. On top of that, these problems require plenty of computational power to solve. The work that goes into solving puzzles generates rewards for whoever solves it called mining. The proof of work consensus verifies that the node that is adding the block is not malicious as it has done some work by spending its computational power as proof of work. When the miner finds the required Nonce, it gets the right to create the new block and store the transactions into it. Then this block is broadcasted into the blockchain network. Other nodes can verify this block by accepting or rejecting it. If the block is accepted, it is appended to their chain.

PoW reduces the risk of 51% attack as it is very hard work to do. If someone tampers with a block will result in changing the hash of the block making it invalid this means that he has to recalculate the hash for all other consecutive blocks which is not tough work in the era of supercomputer PoW solves this problem as it sets a limit on how many new blocks of data can be generated. In the bitcoin network, a miner can only create a Bitcoin block every 10 minutes.

B. Proof of Stake (PoS)

As mentioned in the proof of work miners have to solve a complex problem, which requires a lot of computation power and electricity moreover only the fastest one has the right to create a block this means all the efforts and computation made by other nodes are wasted. Further, if 51% of the miner attain the potential to mine faster than others by having the higher energy to mining compared to other miners, he may rule the whole blockchain network. This problem is solved by proof of stake as only the shareholders can take part in the process of block creation called validators. This saves from the condition of one node owing the network because only one node can't have 51% money of the whole network. There is a probability of owning the network by a single node at the starting but as the network grows it becomes practically impossible for a single node to have that much money to have 51% of the whole network. If the wealthiest person is dishonest and tries to own the network, he has to own more than half of the currency of the network. This process requires a smaller number of validators and significantly reduces energy consumption.[4]

C. Delegated Proof-of-Stake (DPoS)

The Delegated Proof of Stake algorithm is introduced by "Dan Larimer" and implemented in its BitShare project. Delegated Proof of stake is the democratic version of the proof of stake consensus algorithm it has a voting system in which token holders vote for witnesses and delegates in real-time. The number of witnesses lies between 21-101. The witnesses are only responsible for witnessing the transaction, verifying the signature, and timestamping the transaction, but not participating in the trading. They generate one block every 3s in turn, and if a witness did not complete the task at the specified time, it will be skipped and replaced by the next one. Each node on the network can vote for its own trusted witness, the more blockchain stakes he has, the higher possibility of him being a witness. However, due to the mechanism that each witness node takes turns generating blocks, the identity of the witness is already known and always constant, which would make the blockchain system more vulnerable to collusion attacks.

In many cases, witnesses are required to deposit some amount of the currency which is locked. If the witness fails to validate or does some malicious activity, then it will be punished causing him a loss. As it is a democratic model the witness must maintain their reputation to be elected. In this way, DPoS reduces the wastage of efforts and computation resources therefor DPoS can higher transaction volume and provide faster confirmation times than PoW and PoS systems while being more energy efficient.

ALGORITHM	ADVANTAGES	DRAWBACKS
Proof of Work (PoW)	**Provides stable network. Provides evenly powered, controlled decentralized network.**	**High processing power and huge amount of electricity required. Small networks are vulnerable.**
Proof of Stake (PoS)	**Provides quicker transaction. Efficient use of resources.**	**Less decentralized network as compared to PoW.**
Delegated Proof of Stake (DPoS)	**Quicker than PoW and PoS 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**

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

V. APPLICATION OF BLOCKCHAIN TECHNOLOGIES

After the implementation of blockchain in bitcoin it has become the word of mouth and can be used in many areas including finance, health care, etc.

BITCOIN

Bitcoin is a cryptocurrency invented in 2008 by Satoshi Nakamoto. It was the first implementation of blockchain technology. It enables peer-to-peer exchange of value in the digital realm using a decentralized protocol, cryptography, and uses a Proof of work algorithm for the consensus on the state of a public blockchain. The value of Bitcoin is directly proportional to its active users in the network.[5]

The first genesis block of the bitcoin was generated by Satoshi Nakamoto when he sent ten Bitcoins to the noted programmer Finney and completed the first transaction.

BANKING

Blockchain is now overtaking the current Baking system. Using blockchain transactions can be made in seconds due to the validation process done by the cryptographic algorithms. It reduces the need for expensive and time-consuming third-party verification along a payment processor fund transfer, it is estimated that blockchain n technology saves $20bn over the transaction by eliminating the third party.

BLOCKCHAIN IN HEALTHCARE

Blockchain can a big impact on healthcare using smart contracts. Smart contracts get executed automatically when the contract conditions are met. Patients' details can be stored in the blockchain using smart contracts whose key is provided to the patient. Doctors can access the details using this key which will boost the treatment process.

INTERNET OF THINGS

Internet of things is a network of interconnected devices that can interact with others and collect data that can be used for gaining useful insights. The security of the network is determined by the least secured device. The combination of the technologies could enhance secure communications and strengthen privacy agreements.[6]

HYPERLEDGER

Hyperledger is an open-source community focused on developing a suite of stable frameworks, tools, and libraries for enterprise-grade blockchain deployments. It is a global collaboration, hosted by The Linux Foundation, and includes leaders in finance, banking, Internet of Things, supply chains, manufacturing, and Technology. Built under technical governance and open collaboration, individual developers, service and solution providers, government associations, corporate members and end-users are all invited to participate in the development and promotion of these game-changing technologies.
Like the Linux Foundation, Hyperledger has a modular approach to hosting projects. The Hyperledger greenhouse hosts developing business blockchain projects from Hyperledger Labs (seed) to stable code ready for production (fruition). All are invited to contribute to the greenhouse; collectively advancing industry goals of distributed ledger and smart contracts.[7]

VI. BLOCKCHAIN VULNERABILITIES, ATTACKES AND CHHALLANGES

Malleability attack: It is an attack in which transaction unique ID is changed before confirmation on the network. The most common way this occurs is through alteration of transaction signature, which is responsible for generating the transaction ID. If this signature is altered, the transaction ID will also change, making the previous transaction ID invalid. This change makes it possible for the attacker to pretend that a transaction didn't happen. This attack was a success.[8]

Nothing at Stake Problem: This is a theoretical problem with the blockchain networks using PoS the problem occurs when two validators propose the same block simultaneously resulting in the fork of the blockchain. It is in the best interest of the validator to vote both chains. As there is no cost in mining. Mining both chains ensure the mining reward of the voter no matter which fork wins. The attacker can use this scenario to his advantage the attacker will create a fork in the blockchain one block before they spend some coins. If the miners mine both the chains and the attacker mine his chain only, then the attacker's fork will become the longest chain resulting in a double-spend.

Majority Attack: A 51% attack is a situation when a miner or mining pool, owns more than 50% of the network's hashing power acts maliciously.

This is the best know attack against public blockchains. This happens if a certain miner or mining pool has majority hash power. The goal of 51% attack is to perform a double spend. To perform such an attack miner, must control most of the hash rate.

Selfish miner attack: This is an attack where a miner or mining pool, finds a valid solution but does not distribute and publish it to the rest of the network. The selfish miner then continues to mine on top of this block to maintain its lead. When the rest of the network is about to catch up. The selfish miner then publishes his part of the solved blocks. As a result, their chain wins due to the longest chain rules in PoW and claims the block reward. All the efforts made by all other miners are scrapped and they suffer loss. On the one hand, should such an attack be successful, all trust in the chain would be lost, and the value of the attacker's staked

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

coins would drop drastically. On the other hand, the investment needed to acquire such a large influence is usually too high.

Sybil attack: In a Sybil attack a node that tries to control the peer-to-peer network by using multiple identities at the same time. The attacker tries to attain a majority on the network. This attack applies to a blockchain network using Proof of stake as it has a voting scheme the attacker can vote for invalid blocks to make them valid. Although this attack is rarely feasible due to stake requirements.[9]

Double Spending: The attacker will fork the chain which will result in two chains the public chain and a privately mined chain. The malicious person submits a large transaction on the public chain. Once the goods are received, Submit a large transaction for goods/services. The transaction is confirmed on the public chain. Meanwhile, he/she will continue to grow the private chain.Once the goods/services are received, the attacker broadcasted the private chain. As the private chain is longer due to a higher hash rate, forcing the public chain to revert, also reverts the transaction made by a malicious user.

Blocking Transactions: The malicious miner can decide which transactions should be included in a block.[10]

Double Spending Attack: This is generated when a successful transaction is duplicated with the same funds. This problem is specific to digital currency and occurs when a blockchain network is disrupted. This happens when the attacker sends multiple packets to the network, reversing the transaction so that it looks like they never happened.

Attacks related to double spending include are 51% attack, Race Attack, Finney Attack, Vector 76 attacks (combination of Race Attack and Finney Attack), Alternative transaction attack.

DDOS (Distributed Denial-of-Service) attack: A distributed denial of service attack is an attack where a perpetrator overwhelms the target or the related infrastructure with malicious traffic (more traffic than the server or network can accommodate). This is achieved through remotely controlled, hacked computers or bots offer referred to as zombies. They form a network known as "botnet". This is used to do the DDoS attack the primary goal of the attack is to make the resources unavailable for the genuine users. Botnets can range from thousands to millions of computers. This makes it difficult to distinguish the attack traffic in a DDoS attack because of its similarity to the legitimate traffic. The DDoS attack has been proven as a resource battleground between the defenders and attackers; the more the resources, the higher the chance of success. All communications between the handler and the attack are usually encrypted, making the attack invisible from detection. Attackers spoof MAC[11]

There are three types of DDoS attack Application layer attack, Resource exhaustion attack, Volumetric attack.

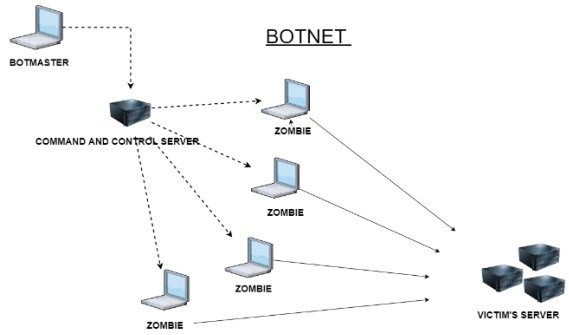


FIG (3): DDoS attack

Blockchain Poisoning:

In this attack, blockchain is loaded with private data (name, addresses, and credit card number), illegal files (malware, malicious content). A malicious user can force blockchain nodes to download malicious files which leads to other attacks in the blockchain such as DoS or DDoS. This can also put the network in conflict with laws. The deletion of these files is hard as blockchain is immutable. The result of this attack is the affected chain cannot be used unless expensive and time-consuming steps are taken to remove these files.

VII. CHHALLANGES

Scalability: After the huge success of Bitcoin, the scalability issue of the blockchain network has been exposed. Block size and block creation time are prefixed for a fixed number of transaction processing, this is efficient to tackle various attacks mentioned above. But a high number of transactions can cause slower transaction processing. Many blockchain applications are suffering from scalability issues such as Bitcoin with block size 1MB and average block confirmation time 10 minutes, whereas Ethereum having block confirmation time of 15 sec. For the high number of transaction processing, the block confirmation time must be low, but to have the security from being attacked by the attacker, this average time should be high. Basically, the fundamental challenge blockchain is facing lies under the concept of scalability trilemma the term was first coined by Vitalik Buterin (founder of Ethereum) which states that it is not possible to equally maximize the three desirable attributes that are decentralization, scalability, and security. The trilemma claims that any two can be maximized by sacrificing the third. Moreover, blockchain-based on PoW consensus e.g., bitcoin has increased electricity consumption as they require huge computation power. The authors of [14] has mentioned the existing solution on the scalability issue.

Storage Management: Blockchain ledger is distributed to all the nodes of the network to provide higher security. The ledger contains all the blocks of the chain starting with the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

genesis block to the latest block mined. This redundancy results in occupying a tremendous space. Bitcoin blockchain size is around 16.5 GB increasing at the speed of around 1 MB per hour. Bitcoin has surpassed 1,00,000 nodes that have occupied nearly 1.5736 Petabytes.

Lack of governance and regulation: Blockchain is a decentralized network there is no third party involved certifying transactions in the permissionless blockchain networks. Many people have faced several issues and lost millions of dollars. There is indeed a requirement to standardize the blockchain network for its integration, governance, and sustainability, etc.

VIII. CONCLUSION

Blockchain is an evolving technology that will revolutionize the IT world. It can be applied to various fields such as healthcare, IoT, management, etc. due to its decentralized nature and peer-to-peer characteristics. Although there are some topics where improvement is required for better adoption of the technology which are discussed in the paper. The technology is getting more mature and stable as it is developing.

The blockchain technology provides many advantages including decentralization, transparency, immutability. At the same time there are various attacks, challenges and issues which are discussed in the paper. There is also need of laws for the regulation of the technology as there is no third party involved. This will also stablish trust which will catalyse the adoption process.

IX. 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 Innovative Computing 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 Toši´c and Michael Mrissa,” Secure and Privacy-Aware Blockchain Design:Requirements, Challenges and Solutions” journal of Cybersecurity and Privarcy, 2021, 1, 164–194 March 2021.