Engineering and Technology Journal e-ISSN: 2456-3358

Volume 09 Issue 09 September-2024, Page No.- 5183-5190

DOI: 10.47191/etj/v9i09.20, I.F. – 8.227

Blockchain Technology: Cryptocurrency Application Arena

***Ms. Priyanka[1], Dr. Ritu Makani[2]**

[1]Research Scholar, GJUST, Hisar, 125001, Haryana, India

[2]Associate Professor, GJUST, Hisar, 125001, Haryana, India

ABSTRACT: The digital currency industry is the one where blockchain technology is most commonly utilized. The distributed and decentralized nature of blockchain technology aids in resolving a number of problems with knowledge processing security, transparency, trust, and dependability in businesses and organizations. Blockchain is a decentralized, peer-to-peer ledger or database that can be used safely with cryptocurrencies to manage all online transactions. Every node that updates its ledger to confirm a new node before adding it to the blockchain does so by updating the ledger with any modifications made to the blockchain. The most recent version of this ledger is then broadcast around the network. The collection of all transactions carried out by different users is known as the blockchain ledger or database. In its most basic form, a blockchain is a distributed ledger that keeps track of individual transactions in a tamper-proof manner. Each block in the chain is linked to the others in a linked list, and each block contains a timestamp and a link to a previous block that provides security. This manuscript will review the many forms of blockchain, how they function, and how they support cryptocurrencies like Litecoin, Ethereum, and Bitcoin.

KEYWORDS: Blockchain, Bitcoin, Cryptocurrency, Consensus, Mining.

1. INTRODUCTION

A blockchain is a peer-to-peer, decentralized technology consisting of linked lists of blocks, each with a distinct set of transitional data according to its intended function. Blockchain uses cryptographic hash methods to determine a block's hash value; the hash of one block serves as the input for the next. The cryptographic hash value of the block makes sure that nobody changes it. Block manipulation is prohibited because every time a block is modified, the hash of that block and all following blocks is likewise altered. The graphical representation of the Block is shown in Fig. 1

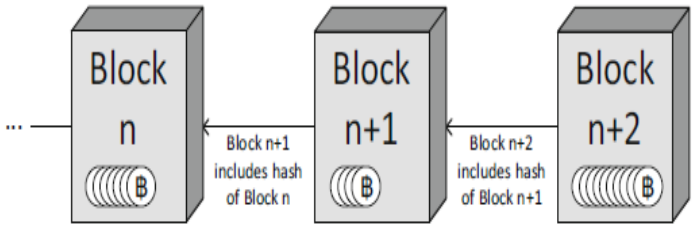

Figure 1 Blockchain Data Structure

One type of distributed database ledger is the blockchain. The enormous issues related to finance can be resolved by this technology. The engagement of a third party and double spending are the two key issues that arose. These issues are resolved by blockchain technology since it eliminates the need for a middleman and allows for the unique information included in each block to prevent double-spending. Each blockchain block is linked to every other blockchain block. Security is provided by several different techniques, including proof of stack, proof of work, and others. Before a newly linked block can be uploaded to the blockchain, it must first be validated using different Conesus algorithms. A hacker needs a lot of processing and computer power to hack the block data. Nodes, or individuals who generate, validate, and compute the hash value of a new block, are known as miners [1] and [2]. Since blockchain provides security and governs how cryptocurrencies operate, this technology aids in the upkeep and transaction of digital currencies. Additionally, the IoT, voting, health care, and other fields all use BT, which raises the bar for their operational procedures. We discuss the advantages and disadvantages of blockchain

technology in this essay. We go into detail about the Bitcoin mining procedure as well.

2. RESEARCH METHODOLOGY

This study uses quantitative methods. We discovered the different cryptocurrencies and Bitcoin mining by gathering information from publications, research papers, and articles about the variables influencing blockchain technology and digital currency as a database to analyze the taxonomy, different issues faced by blockchain, and other topics.

3. BLOCKCHAIN TECHNOLOGY

3.1 The definition of the Blockchain technology

A blockchain could be a distributed ledger where each block is connected to every other block using a linked list structure. These blocks include an ordered set of transactions. Cryptographic hashing techniques are employed to create a secure connection between a block and its predecessor. Any modifications to the block affect not only that block but also the hash of all blocks in the blockchain that come after it. Because no one can change the data on the blockchain, it is secure. These days, blockchain is very popular. However, what is blockchain? What issues do they address, and how are they used? as the name suggests? A blockchain is an ever-expanding list of records, or blocks, connected to one another, containing data, and encrypted for security. Each block has a digital signature and a hash. The initial goal of this technology, which was first presented by a group of researchers in 1991, was to timestamp digital documents to prevent manipulation or backdating. Before Satoshi Nakamoto modified it in 2009 to produce the digital currency known as Bitcoin, it was unutilized. One of their numerous characteristics is that once data is entered into a blockchain, it is highly difficult, if not impossible, for anyone to directly change it.

3.2 Taxonomy of Blockchain

Fig.2 describes the various areas where the Blockchain plays a very important role.

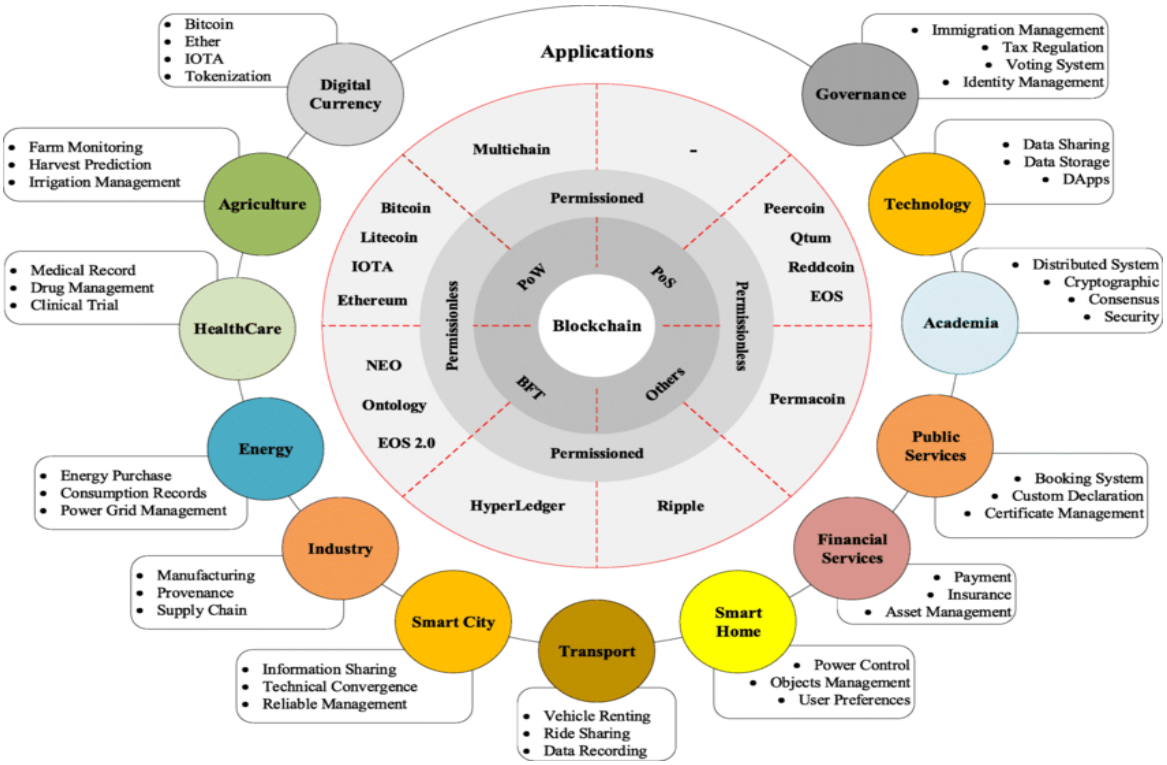

Fig.2 Taxonomy of Blockchain [15]

3.3 Types of Blockchain

1. **Private Blockchain:** Private corporations control the whole private blockchain, and they do not want any public contact with blocks that hold a company's sensitive data. Until authorization is obtained from an authorized company, network administrator, or complete node, no one can join the blockchain directly.
2. **Public Blockchain:** Anyone can join the public blockchain to conduct transactions, join an already-existing chain, and participate in it.
3. **Consortium Blockchain:** This kind of blockchain allows numerous businesses to participate in its management and access control mechanisms, making it semi-decentralized as opposed to being controlled by a single private

company. [3] Various types of Blockchains are described in Fig.3.

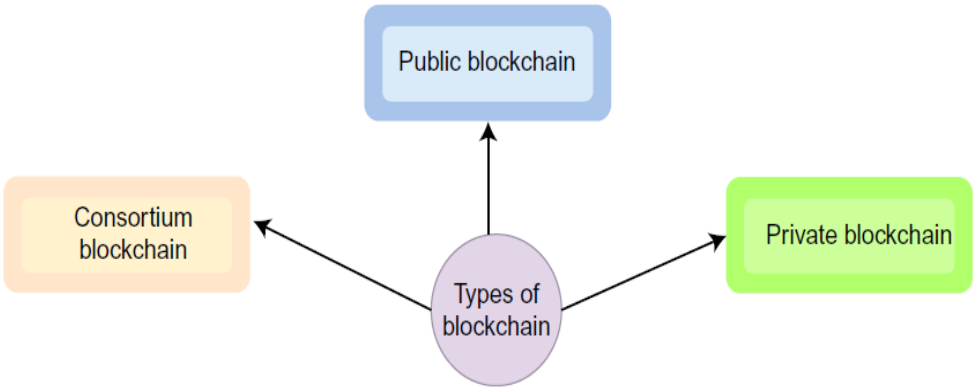

Fig.3 Types of Blockchain

3.4 The Structure of the Blockchain Technology

What makes up a blockchain system is:

1. A blockchain is made up of nodes, or blocks, with transaction data contained in each block.
2. Every block in a blockchain uses the ledger, which functions as a data structure, to store transactional data.
3. Other nodes are referred to as partial nodes or wallets, similar to a mobile device, and are utilized in the mining process that obtains a complete copy of the ledger.
4. A consensus method or network protocol that establishes the rules for all rights, obligations, validation, and verification amongst the nodes in the Blockchain network. Fig. 4 describes the Blockchain structure.

These are some basic components of blockchain architecture:

- **Block header and blocks:** The header of each block in the blockchain serves as a unique identifier for that particular block. There is transactional data in every block. The user has the ability to edit or modify the data whenever needed. The blocks contain the safely saved transactions. The blockchain allows us to add new blocks whenever we need them.
- **Node:** A node in a blockchain network is a computer or user that has a copy of the entire blockchain ledger on it.
- **Merkle Root:** This is a particular, unique hash value that is combined from all of the transactions in a blockchain block. Since it is exceedingly difficult to calculate the independent hash value for every blockchain transaction, we can use the Merkle tree to determine the unique value for every transaction in the block.
- **Transactions:** It is the fundamental unit of a blockchain system, they are the smallest building block or collection of records and data.
- A chain is a collection of blocks joined together using a linked list technique.
- **Miners:** Before a block is added to the current blockchain network, it is validated by these special nodes, called minors. The minors must verify a new node before adding it, and they are rewarded for their efforts.
- **Consensus:** Consensus is the collection of intricate riddles and algorithms that govern how blockchain functions.

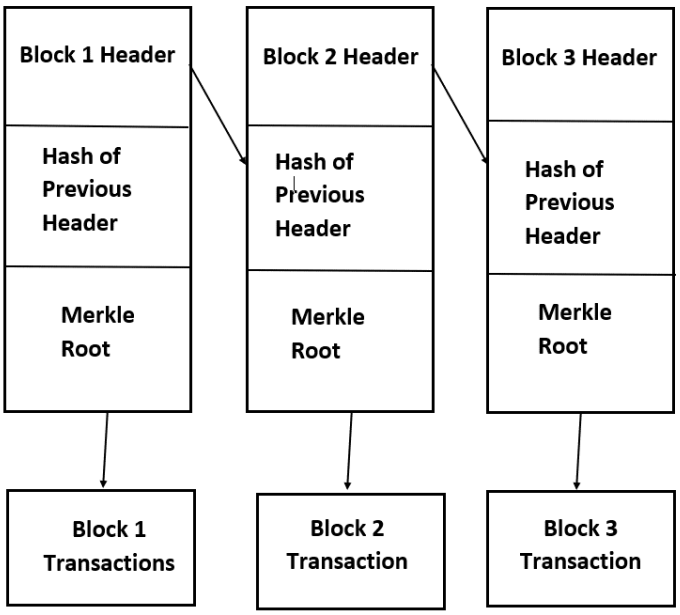

Fig. 4 Blockchain Structure

3.5 Working of Blockchain:

Figure. 5 Describes the working of the blockchain transactions process.

1. Initially, a change is requested for a transaction, and then the new block for that transaction is made.
2. Every block in the network receives this block, which is distributed throughout it.
3. Entire Node verifies the transactional data.
4. The entire node receives rewards following the validation of a new block.
5. The new block is added to the end of the current blockchain if it is validated.
6. The transaction process is ultimately finished.

3.6 Some Problems and Attacks Faced by Blockchain

These are some attacks and problems that are faced by blockchain during their operations or working process:

1. **51 percent attack:** This kind of attack occurs when six out of ten blocks wish to modify the data, or alternatively, when 51 percent of the blocks work together to accomplish an activity, which could involve hacking or data manipulation. This attack is only effective when 51% of the blocks use all of the CPU and GPU power to complete any task.
2. **Double-spending:** The fundamental idea behind this assault is for a user to simultaneously spend the same amount of digital currency on two platforms, however, this issue has essentially been resolved.
3. **Sybil's attack:** In a peer-to-peer network, this attack can also occur when a single node serves several distinct identities, leading an outside observer node to believe that a different node is operational. Obtaining the majority of nodes to engage in any illicit activity is the primary objective of this kind of attack. Data hacking is the main application for this kind of attack.
4. **DDoS attack:** When one or more hostile nodes overload the blockchain network with requests or traffic, an attack of this kind occurs. In this scenario, incoming data may overwhelm the blockchain, forcing it to share processing resources with it.

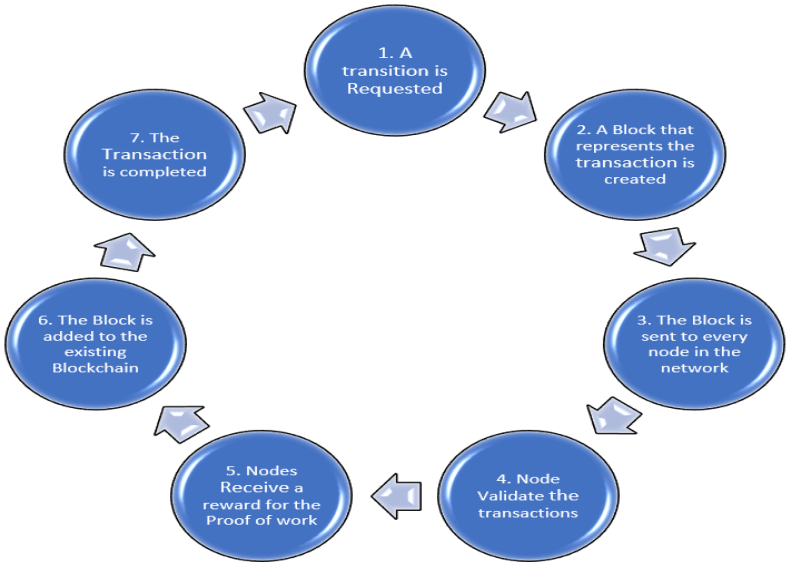

Figure: 5 Working of Blockchain

3.7 Advantages of Blockchain technology:

1. **Decentralization:** Blockchain is a peer-to-peer decentralized system that eliminates the need for an intermediary and all associated transaction fees and overhead.
2. **Immutability and data integrity:** A record can only be removed by using the consensus algorithm once it has been stored in the blockchain ledger. Blockchain users can improve regulatory compliance and decrease fraud.
3. **High accessibility and availability:** data from blockchain technology would be timely, accurate, and complete because of decentralized networks.
4. **Processing Time:** The time it takes to complete a transaction can be slashed by using blockchain technology; it can go from three days to minutes or even seconds.
5. **Security**: Every blockchain transaction has a 64-digit alpha-numeric signature that corresponds to it and is digitally time-stamped with a distinct cryptographic hash code. Every transaction is accompanied by a 64-digit alpha-numeric signature that is digitally time-stamped with a distinct cryptographic hash code.
6. **Automation:** Smart contracts, which are self-executing codes of instructions that can be saved and automatically implemented within the blockchain, are a feature of blockchain technology.
7. **Reliability:** There is no single point of failure and no single control center for blockchain technology.
8. **Transparency**: With blockchain technology, all transactions are transparent. Every node has access to the entire ledger, and everyone may view the specifics of other transactions.

3.8 Disadvantages of Blockchain technology:

1. **Cost issues:** One drawback of decentralization may be that using blockchain technology comes with an upfront cost. The user node bears the cost of the transactions and processing power.
2. **Time issue:** The main problem with the Bitcoin network is that it is too slow for large-scale transactions due to its complex verification process.
3. **Technological immaturity:** A decentralized network may be entirely replaced by blockchain technology, which is a novel technology. Among other things, it has the power to totally alter an organization's culture, strategy, methods, and structure.
4. **Integrity problems:** The blockchain technology's solutions necessitate significant changes to the existing legacy systems.
5. **Wasted Resources:** Requires large amounts of energy. Approximately $15 million per day of energy is spent by the Bitcoin mining Network.[4]

4. BITCOIN CRYPTOCURRENCY WITH BLOCKCHAIN

4.1 What is BitCoin and how it works with Blockchain

In 2009, Satoshi Nakamoto created Bitcoin, a digital currency that runs on the blockchain. It is a peer-to-peer, distributed, decentralized digital currency, or cryptocurrency, created by each and every node that is a part of the blockchain. A chain or collection of connected Bitcoin blocks that are generated via the network is known as the blockchain. Any previous transaction that may have occurred across the blockchain network between different Bitcoin addresses can be simply found. Any time a new block is needed, it can be added to the blockchain. This process of verifying new blocks before they are added is known as the Bitcoin mining process. Bitcoin uses SHA-2 as a cryptographic hash function. wherein the freshly created value—referred to as the "hash value" by SHA-2—is compared with an existing hash value to ascertain the integrity of the material. Large volumes of input data are transferred into a predetermined length of hash value using the SHA-2 method. wherein the same input data will always provide the same hash value, but any slight changes to the input data will result in a whole change in the hash value. Fig.6wo shows various types of cryptocurrencies.

Fig.6 Various types of cryptocurrencies.

4.2 How Bitcoins works:

In order to offer protection, when deciding whether the precise owner or person accesses their Bitcoins or whether an unauthorized person does not, Bitcoin uses an ECDSA cryptographic asymmetric or symmetric algorithm. A transactional node is generated whenever Bitcoin is moved from one location to another, and it is then supplemented with a second public key that is created via ECDSA [10]. Every time a new Bitcoin transaction is created, it is sent to every node in the network in order to provide all of the information regarding the public key of the owner's coins to every node. Figure 7 illustrates how bitcoins operate.

A fresh owner's public key is appended to each bitcoin as it is transmitted, while the sender's private key serves as the signing key. Everybody stores every transaction detail, which aids in the verification process when a new node is added to the blockchain. Message authentication and verification are done using the sender's signature. We can employ different cryptographic methods with their private and non-private keys for data encryption and decryption. When a message is coded or encrypted using a Pk, non-public key, or Sk, we use a combination of both private and public keys. The public key is then used for decryption. In a similar vein, decryption requires a private, non-public, or Sk key when the public key is used for encryption [13].

We do not require a third party because the blockchain is utilized in Bitcoin transactions, which makes use of the public distributed ledger. Those who are interested are welcome to participate in the verification process of Block, which uses powerful CPUs and GPUs with large RAM to validate the new Block, also known as miners. These miners are rewarded for verifying blocks, which is how the verification process works. Every node on the Bitcoin network receives new transactions and Bitcoin currency created by the full node or user throughout the mining process. [14].

Different computers in this network are running specialized software to compete in challenging problems or to figure out the consensus process. After solving the complicated challenge, the main minor or full node receives 50 new Bitcoins, and the relevant block of transactions is appended to the existing blockchain. Every complex puzzle has a

different amount of complexity based on the blockchain network and how many Bitcoin miners are there. [11].

In order to validate the construction of block transactions, which take ten minutes each, the difficulty level of the puzzle increases in proportion to the number of full node miners. Six blocks are formed in an hour, and the rate of creation is modified following the creation of the 2016 block. Since there is no way to increase the monetary base of Bitcoins, the primary objective is to ensure that the total number of Bitcoins created never exceeds 21 million. If Bitcoins are used extensively, this might lead to a significant depreciation of their value [12].

4.3 Prerequisites of BitCoin

a) **Integrity:** Digital signatures and a variety of encryption techniques are used to ensure that Bitcoin transactions are unchangeable at a later time.

b) **Authentication:** BitID, a very useful decentralized protocol in a decentralized cryptocurrency network, can be used to authenticate nodes or blocks. This BitID is linked to Bitcoins, and BitID provides services to customers by utilizing their Bitcoin wallets.

c) **Non-repudiation:** This means that you do not deny having done so. The sender must sign the destination node's public key and prior hash in order to achieve this property.

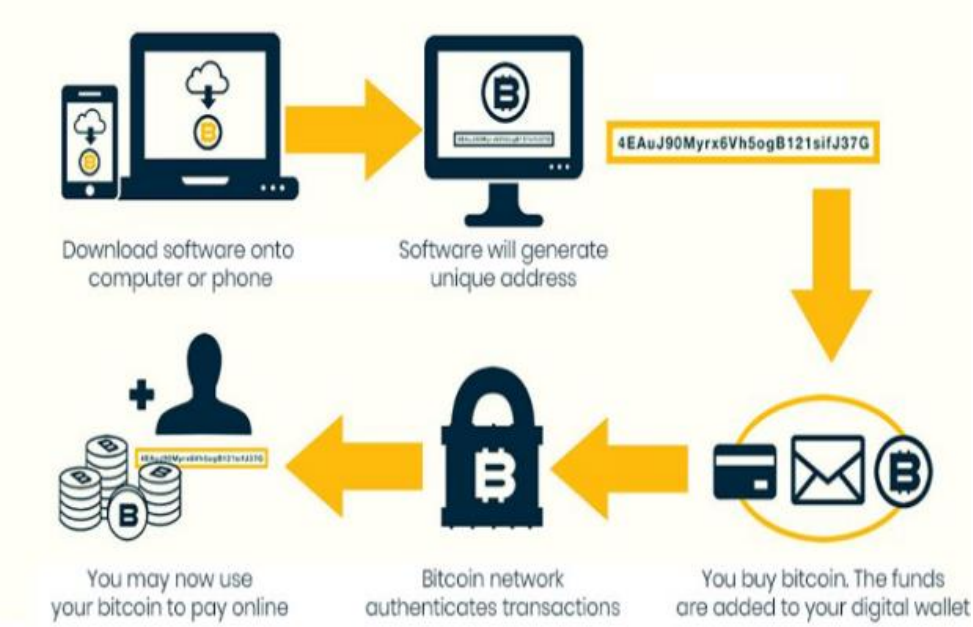

Figure 7 Working of Bitcoin

4.4 Benefits of Bitcoins

a) **Bitcoin mining**: Whenever the mining or verification procedure is completed, we are rewarded through the mining process. A complete node with a lot of CPU and GPU power completes the mining process, if we have all these resources, we can complete the mining process and produce money.

b) **Decentralized Registry:** Because we possess a decentralized network, no third party can exert control over it, meaning that neither the government nor banks can take it away from you. Additionally, there are no transaction fees to pay. Direct transfers of funds between cryptocurrency wallets are possible without involving a middleman or incurring a transaction fee.

c) **Fast & Cheaper:** Cryptocurrency transactions are more affordable and faster than bank-based money transfers. Any cryptocurrency, including Bitcoins, can be transferred between wallets without a transaction charge or bank involvement.

d) **Secure Payment Information:** We employ a variety of cryptography algorithms for crypto transactions to ensure payment security. Together, the public and private keys sign each transaction.

4.5 Deflationary Cryptocurrency

Blockchains are largely used by blockchain technology, which underpins cryptocurrencies such as Ethereum and Bitcoin. Because of its advantages, Bitcoin creates a deflationary cryptocurrency through the creation of many protocols. As we've covered, after a new Block or transaction is verified and validated, new Bitcoins are created through the mining or verification process. Every time a new block is successfully created and added to the end of the block's chain, the minor node is compensated with some Bitcoins for their verification or mining efforts. The block sequences in Figure 3.5 are depicted as they emerge one after the other through the use of mining or verification processes. After every 210,000 blocks, the awards are generated. In 2012, the award value dropped from 50BTC initially to 25BTC.

5. CONCLUSION

According to McKinsey's assessment, blockchain technology has the ability to drastically alter the financial and economic landscape by lowering risks while simultaneously saving money and resources. Using this decentralized blockchain technology will have many wonderful advantages, including reducing the number of database files that financial institutions need to maintain. According to the most recent survey, seven out of ten adoptions in financial trade organizations have made use of blockchain technology, with a primary focus on four areas: reference data, clearing and settlement, overall product payments, issuance of equity and debt, and clearing and issuance of debt. As a result of blockchain technology's increased computer power and falling device costs over time, more IoT device options are available, along with data integrity and security. Additionally, blockchain provides a trustless environment with P2P and decentralized communications transmission protocols, as well as safe distributed and shared data. This essay covered several forms of blockchain technology and how they operate. It also gave a description of the cryptocurrency Bitcoin and how blockchain technology supports Bitcoin mining and security.

6. SOME ABBREVIATIONS USED:

IoT: Internet of Things
P2P: Peer to Peer
ECDSA: Elliptic Curve Digital Signature Algorithm
Pk: Private Key
SK: Secret Key
SHA-2: Secure Hash Algorithm
BT: Blockchain Technology
POW: Proof of Work

- **Competing Interests:** We certify that we have no affiliation with or involvement in any organization or entity with any financial or non-financial interest in the subject matter or material discussed in the manuscript.
- **Funding Information:** Not Applicable
- **Author Contribution and Data availability statement:** All data generated or analyzed during this study are included in this manuscript. The data in this manuscript is based on research done with the help of various research articles, as referenced in the references section. This data can be visible on the journal's home page after publication and to researchers for research purposes only.
- **Involvement of humans or animals:** this research is done by only humans or animals not involved.

REFERENCES

1. A. Bahga, V. Madisetti, "Blockchain Platform for Industrial Internet of Things", Journal of Software Engineering and Applications, No. 9, pp. [36]533-546, 2016.
2. A. Litvi_enko, A. _bolti_š, "Computationally Efficient Chaotic Spreading Sequence Selection for Asynchronous DS-CDMA". Electrical, Control and Communication Engineering, vol.13, pp.75-80, 2017
3. Rahul Rao Vokerla, Bharanidharan Shanmugam, Et.al "An Overview of Blockchain Applications and Attacks", International Conference on Vision Towards Emerging Trends in Communication and Networking, IEEE 2019.
4. Thomas kitsantas, Athanasios Vazakidis, Et.al. "A Review of Blockchain Technology and Its Applications in the Business Environment", Research Gate,2019.
5. BitFury Group, "Proof of Stake versus Proof of work. White paper", September 2015
6. D. Balaban, "Blockchain Networks: Possible Attacks and Ways of Protection" [online]. Available from: https://resources.infosecinstitute.com/blockchain-networks-possibleattacks- ways-protection/#gref.
7. J. Golosova, A. Rom_novs, "Overview of the Blockchain Technology Cases". In Proceedings of the 59th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS), October 10-12, 2018, Riga, Latvia. IEEE, 2018, pp.1-6. ISBN 978-1-7281-0098-2.
8. Blockchains and the Internet of Things, http://www.postscapes.com/blockchains-and-the-internet-of-things/.
9. Chapter 7. The Blockchain, http://chimera.labs.oreilly.com/books/1234000001802/ch07.html/
10. .bitcoin/src/chain params.cpp, https://github.com/bitcoin/bitcoin/blob/3955c3940eff83518c186facfec6f50545b5aab5/src/chain params.cpp#L123
11. Why Use Bitcoin? http://www.coindesk.com/information/why-usebitcoin/
12. How to Set Up a Bitcoin Miner, http://www.coindesk.com/information/how-to-setup- a-miner
13. The Rise and Fall of Bitcoin, https://www.wired.com/2011/11/mf_bitcoin
14. State Of Bitcoin 2016 – A Summary for Bitcoin Investors, http://cryptorials.io/state-of-bitcoin-2016-investors-summary
15. https://www.google.com/search?q=taxonomy+of+blockchain&sxsrf=ALiCzsaHCbamfNnpYyik0lNxP_WZltp8lA:1655206617370&source=lnms&tbm=isch&sa=X&ved=2ahUKEwje6tST7az4AhUyiOYKHWsyDU0Q_AUoAXoECAIQAw&biw=1920&bih=880&dpr=1#imgrc=XpKOWLzYVmo7eM