JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Blockchain Technology - A Pedagogical Review

Mrs. Dnyaneshwari Shantanu Patil

Research Scholar,

Bharati Vidyapeeth Deemed University, Pune.

❖ Abstract –

With the continuous development and advancements in Blockchain Technology researchers, academicians, scientists, and developers are constantly exploring the practical applications of blockchain for real-life problems. Blockchain is the fundamental principal used to create cryptocurrencies, like Bitcoin, Litecoin, Ethereum, Altcoins, Polygon, etc. More often the terms bitcoin and blockchain come together. Many people think that Bitcoin is a blockchain, but both are different. Bitcoin is an application of blockchain14 technology. The current paper first introduced the fundamental concepts of blockchain. Cryptocurrency, Smart contracts, Supply chain management, Identity Management, Cross border payments these are some real-world use cases of blockchain. The blockchain is a peer-to-peer, distributed, decentralized, public, ledger1514 that has changed the mechanism of various sectors.

Blockchain was introduced in 2008 by Satoshi Nakamoto and since then blockchain has been growing. The blockchain provides security, anonymity, transparency and data distribution without the need of any intermediator. With the help of blockchain transactions may occur in a trusted environment. Hence blockchains are used for validating transactions, authenticating users, registering transactions, recording data etc. This paper conclusively describes the fundamental concepts of blockchain, real-life applications, the pros and cons of blockchain and the working of blockchain.

❖ Aim and Methods –

This paper focuses on the basics of a blockchain, its applications, working, pros and cons etc.

As it is a literary review of blockchain, the data is collected from many popular journals such as Springer, PubMed, IEEE and some books related to blockchain which are mentioned in references.

❖ Keywords –

Blockchain, Cryptocurrency, Bitcoin, Decentralized, Consensus, Proof of Work, Proof of Stake, Ledger.

❖ Introduction –

The blockchain technology has been evolving for the last 15 years and now it's spreading its roots in many sectors like finance, healthcare, agriculture, supply chain management, cryptocurrency, IoT, etc. Bitcoin is the first application of a blockchain. Blockchain was 1st introduced in 2008 by Satoshi Nakamoto1,

Since then, there are 3 versions of blockchains are available, namely – Blockchain 1.0, Blockchain 2.0 and Blockchain 3.0.

❖ Preface of Blockchain Technology -

By definition, a blockchain is a distributed, decentralized, immutable, peer-to-peer, public ledger that keeps track of each and every transaction2. Blockchain is an amalgamation of all these technologies. In blockchain, all the transactions that have taken place and those that are getting consensus from the blockchain network are stored as a block on the network. These blocks are linked together via a hash value like a linked list data structure and it forms a chain of blocks. The popular consensus algorithms in Blockchain technology are Proof of Work, Proof of Stake, Proof of Authority, Proof of Burn, Proof of Identity, Byzantine Fault Tolerance, Proof of Elapsed Time, etc. Whenever a new transaction takes place, a block is created for it. Then it is compulsory to validate that new block by every participant in the blockchain network before attaching it to the existing blockchain. If a transaction is validated then only it is added to the blockchain otherwise it will be rejected and hence not added to a blockchain. Blockchain was very little popular in the early days (in 2008) but Nowadays it has become more and more popular in our daily lives.

Literature Review -

Before accelerating deep into the topic of Blockchain Technology, the researcher has done a pedagogical review of relevant articles and books on blockchain technology. The works of (Bashir, 2018), (Drescher, 2017), (Gousia Habib, 2022) (Karen Czachorowski, 2019), (Kulhari), (Guang Chen, 2018), O'Reilly, and IBM have been referred. Moreover, some legitimate websites are visited. The focal objective of this literature review is to get precise, faithful and accurate information about the said topic and to write a well-ordered research article. The main idea behind this literature review is to identify the research gap and collect the relevant information.

Fundamental Jargon in Blockchain Technology -

- **Block –**

Block is a basic unit of Blockchain Technology. A Block contains metadata about that block and the hash value of the previous block. It stores transactions. The very first block in any blockchain is known as the Genesis Block.

- **Blockchain –**

It is a chain of validated blocks only in a blockchain network. It stores blocks as a linked list data structure stores. Each block is linked with its previous/next block by using a hash value of that previous block.

- **Node –**

Any participating node/entity in a blockchain network.

- **Transaction –**

An exchange of assets between two parties/entities.

- **Consensus –**

Consensus is a synonym for an agreement among independent individuals3. Consensus is an algorithm for validating a block (i.e. a new transaction) by every node on a Blockchain network. Some famous consensus algorithms are- PoW, PoS, PoC, PoET, etc.

Key Characteristics of Blockchain -

- **Decentralized –**

Blockchain is a decentralized system which implies that there is no central authority that takes responsibility of the overall network. Instead, all nodes work together to validate newly added transactions.

- **Distributed-**

Blockchain follows distributed architecture, which means every node in a blockchain network has the same copy of the ledger. This ledger is public and it provides information about all participating nodes and transactions.

- **Immutable –**

Immutability means something that cannot be changed once it happens. So blockchain is immutable in nature. Once a transaction has taken place, then it cannot be altered, modified or deleted. This helps in keeping the blockchain transparent and tamper-proof.

- **Transparent –**

The blockchain is public and transparent, which denotes any authorized user can access and view the transactions on the network. This makes the blockchain tamper-proof.

- **Unanimous –**

Whenever a transaction takes place, all nodes in the blockchain work together and validate every block. If a block is failed to validate then it is rejected and will not be added to the blockchain but if validation becomes successful then it will be added to the blockchain network. So, the decision to either validate or reject a block is totally depends on all the nodes in a network.

- **Consensus –**

A consensus is a decision making algorithm that will help nodes in the blockchain to arrive at a decision quickly.

Types of Blockchain -

There are two main types of blockchain – Permissionless and Permissioned

- **Permissionless Blockchain –**

A permissionless blockchain is trustless as it is public in nature. Permissionless blockchains are open networks that are available to everyone to participate.

Examples – Bitcoin, Ethereum, BNB Smart Chain

- **Permissioned Blockchain –**

Permissioned blockchains are a closed network which are more secure. Only preselected nodes are allowed to participate in a process of consensus.

Examples - Hyperledger Fabric13

- **Public Blockchain –**

In a public blockchain, all the participating users can perform read and write operations. Anyone can join a public blockchain.

- **Private Blockchain –**

In a private blockchain, only trusted participants are allowed to perform read and write. Private Blockchains are mostly adopted by private organizations as they do not want any interference from the public.

- **Consortium Blockchain –**

The consortium Blockchains are semi-decentralized blockchains. Instead of controlling access to the blockchain by a single authority, multiple companies are allowed to become a part of the blockchain.

	Public	Consortium	Private
Participants	Without permission • Anonymous • Could be malicious	Permissioned • Identified • Trusted	Permissioned • Identified •Trusted
Consensus mechanisms	Proof of work, proof of stake, etc. • Large energy consumption • No finality • 51% attack	Voting or multi-party consensus algorithm • Lighter • Faster • Low energy consumption • Enable finality	Voting or multi-party consensus algorithm • Lighter • Faster • Low energy consumption • Enable finality

Figure 1: Types of blockchain and their characteristics6

Applications of Blockchain -

Since the evolution of blockchain, it has shown its benefits for real-life problem-solving. Nowadays, blockchain is widely accepted and implemented in every sector because of the nature it possesses, such as distributed, decentralized, transparent, public, secure, unanimous, etc. Following are some sectors where blockchain has its applications –

- **Asset Management –**

Asset Management is the biggest application of blockchain. Asset management involves exchanging assets between parties involved in a transaction. Assets could be a real estate, fixed income, equity, shares, commodities etc. The regular process of asset management can be very expensive. So blockchain will become helpful because it removes the need of third parties who monitor or conduct a transaction like a broker or a settlement manager etc.

- **Identity Verification –**

Most of the time we need to verify our digital identity for a reason such as to complete banking transactions. With the help of blockchain, the identity of a user can be verified and validated. Then the user can share his/her identity with others if required. Also, a user can choose a method of identity verification like Fingerprints, Voice, and Facial Recognition.

- **Healthcare –**

Blockchain has a big advantage in the Healthcare Sector. With the help of blockchain, it is easy to maintain the HIPPA Privacy where the information or record of the patient is kept private. Blockchain assists in keeping records of all the patients and with the help of Smart Contracts, these records are only accessible to the specified person.

- **Internet of Things –**

Internet of Things is a network of interconnected devices such as physical devices with sensors, software that exchange data with each other5. The blockchain gives its assistance to IoT devices as they collect a huge amount of data. Blockchain ensures the data which is gained by IoT devices is kept secure in a blockchain network and it is only visible to trusted nodes.

- **Cross-Border Payments-**

One of the characteristics of a blockchain is that it has no geographical barriers. You can transfer money to any location on the earth without any physical barrier. Cross border payment is quite a complicated and time-consuming process. It may take many days to transfer your money across the globe and sometimes it is not trustworthy. In such cases, blockchain ensures a secure money transfer across the boundaries of the sender's country. It is also less expensive due to no involvement of a third party. With blockchain, you can send money globally unlike regional payment apps like Paytm, which is only limited to India.

- **Cryptocurrency –**

A cryptocurrency is the most popular and the first application of a blockchain. Crypto coins are used to make cross-border payments without any location barrier. There is no exchange of real money so if the currencies of the sender's and receiver's are different then it will not affect a transaction.

Working of Blockchain6 -

Step -1: Initiating a Transaction

A transaction is initiated by an authorized user.

Step - 2: Verifying a Transaction

All the participating nodes checks the validity of the transaction.

Step - 3: Creating a Block

Once a transaction is verified and validated then a block is created for each new transaction.

Step - 4: Taking Consensus for a Block

After creation, the node tries to insert a block in a blockchain network permanently. But every node is not allowed to add a block. That's why the node uses a consensus algorithm which ensures every node in a blockchain network agrees upon accepting/rejecting the newly created block.

Step - 5: Inserting a Block

After taking consensus, the new block is then added to the existing blockchain network. This new block is linked with its previous block using a cryptographic hash value.

Step - 6: Transaction Completion

As soon as the block is inserted, the transaction gets completed. And the block is permanently stored in the blockchain. Now no one cannot remove the block or revoke or change the block or the transaction.

Structure of a Block -

A block is a core part of blockchain technology. Block is a distributed database that stores the metadata and transactions. Every block has 2 parts – block header and body**Error! Reference source not found.**.

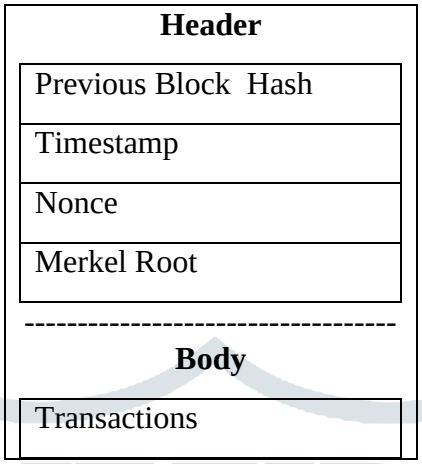

Figure 2 – Structure of a Block9

- **Header –**

Header helps to identify each block uniquely.

The block header is made up of hash of the previous block, timestamp and a nonce number7.

- **Previous Block Hash –**

A hash of the previous block is stored in the header of every node. This will helps to connect the next block to the previous block and helps in forming a chain of blocks. Hash of the previous block is a reference to the previous block.

- **Timestamp –**

When a block is added to the blockchain, a timestamp is attached to it. The timestamp consists of an approximate date and time of creation of a block.

- **Nonce –**

Nonce stands for number used only once which is used for proof of work algorithm. Also nonce helps in getting the desired hash value7.

- **Merkel Root –**

A Merkel Tree is also known as a Binary Hash Tree8. It is a data structure that stores the hash values of all the blocks. It is a tree data structure where all the leaf nodes are at the same level and can contain a hash of every transaction. A Merkel Root is the root of all the hashes of all the transactions that are part of a blockchain.

Advantages of a Blockchain -

- **Immutability –**

Immutability refers to data of the blockchain that cannot be altered or modified. This will keep blockchain secure and tamper-proof.

- **Transparency-**

As blockchain is distributed in nature, everyone on the blockchain network has the same information in their ledger. This will make a blockchain transparent.

- **Less Expensive –**

Blockchain doesn't need a third party to perform its operations. This leads to cost reduction of the business that uses a blockchain.

- **Security –**

Blockchain uses a hashing technique to generate a unique hash value for every block. This hash value is stored as a reference under the next block's 'Previous Hash Value' field. If anyone tries to change the data from the block, it will change the hash value of the block and automatically hash value mismatches which shows the data alteration. It uses SHA 256 hashing technique for generating hash value9.

Disadvantages of a Blockchain -

- **High Implementation Cost –**

Although the uses of blockchain are less costly, its implementation cost is too high. It involves hiring developers, training and supervising a team, etc.

- **High Energy Consumption –**

Some blockchains consume too much energy. It requires energy for updating a ledger, solving complex mathematical problems, mining etc.

- **Speed –**

Blockchain is comparatively slower than traditional systems because it performs too many operations.

- **Immutability –**

Data immutability is one critical feature of a blockchain. Although blockchain is beneficial because of its immutability, it is difficult to modify the data once written.

- **Privacy –**

A public Blockchain is accessible to all nodes in the network regardless of anonymous and encrypted users. This will result in the accessibility of the data to anyone. This leads to privacy breaches11.

❖ Conclusion -

The main highlights of the present paper -

A blockchain is a distributed ledger technology that uses a consensus algorithm and there is no involvement of a third party. The paper reviews blockchain technology in detail, including applications of blockchain technology, its characteristics and its evolution. The paper highlights blockchain technology's benefits, properties and challenges. The paper describes blockchain technology in the transaction system and its cryptocurrencies. The study broadly discusses blockchain applications in multiple sectors. From the current study, I conclude that the blockchain has some limitations like scalability, sometimes it requires high power to

process transactions. It is necessary to work on the issues like high power consumption, scalability, data storage, additional security, etc. in the future.

❖ Abbreviations used –

- PoW – Proof of Work
- PoS –Proof of Stake
- PoC – Proof of Capacity
- PoET – Proof of Elapsed Time

❖ References -

1. Lorne Lantz, Daniel Cawrey. Mastering Blockchain. O'Reilly Media, November 2020. oreilly.com,https://www.oreilly.com/library/view/mastering-blockchain /9781492054696 /ch01.html
2. IBM. (n.d.). topics/blockchain. Retrieved from ibm.com:https://www.ibm.com/topics/blockchain
3. Drescher, Daniel. Blockchain Basics. 2nd . Germany: Apress, 2017.
4. Karen Czachorowski, Marina Solesvik , Yuriy Kondratenko. "The Application of Blockchain Technology in the Maritime Industry." Green IT Engineering: Social, Business and Industrial Applications (2019): 561-577.
5. What is IoT. n.d. , https://www.oracle.com/in/internet-of-things/what-is-iot/ .
6. University, Stanford. How does blockchain work. n.d. Stanford , https://online.stanford.edu/how-does-blockchain-work .
7. mastering-bitcoin. n.d. O'Reilly. https://www.oreilly.com/library/view/masteringbitcoin/9781491902639/ch07.html
8. Bashir, Imran. Mastering Blockchain. Ed. Suresh M Jain Ben Renow-Clarke. 2nd . Birmingham: Packt Publishing, 2018.
9. Gousia Habib, Sparsh Sharma,Sara Ibrahim,Imtiaz Ahmad,Shaima Qureshi. "Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing." Future Internet (2022): 4pg. https://www.mdpi.com/journal/futureinternet.
10. Guang Chen, Bing Xu, Manli Lu & Nian-Shing Chen. "Exploring blockchain technology and its potential applications for education." Smart Learning Environments Journal (2018): 3 pg.
11. Kulhari, Shraddha. Data Protection, Privacy and Identity. Nomos Verlagsgesellschaft mbH, n.d.
12. Gurinder Singh, Vikas Garg,Pooja Tiwari. "A Study on Blockchain Technology: Application and Future Trends." Blockchain Technology and the Internet of Things (2020): pp.317-337.
13. Amazon, AWS. blockchain. n.d. https://aws.amazon.com/blockchain/what-is-hyperledger-fabric/#:~:text=Hyperledger%20Fabric%20is%20an%20open,2015%20by%20The%20Linux%20Found
14. wikipedia. (n.d.). Blockchain. Retrieved from wikipedia.org: https://en.wikipedia.org/wiki/Blockchain
15. blockchain-technology. (n.d.). Retrieved from simplilearn.com: https://www.simplilearn.com/tutorials/blockchain-tutorial/blockchain-technology

JETIR