Relative Analysis of Blockchain, Bitcoin and Consensus Algorithm

[1]Sameeka Saini, [2]Ritu Payal, [3]Arpit Mishra

[1]Assistant Professor, [2]Assistant Professor, [3]Assistant Professor
[1]CSE Department, [2]MCA Department, [3]CSE Department
Dev Bhoomi Group of Institutions, Dehradun, India

***Abstract*: The decentralized ledger in which the transactions of cryptocurrency are recorded and securely exchanged is commonly known as Blockchain. Blockchain (commonly known chain of blocks) is the latest trend that follows decentralization concept. The collections of previously executed Bitcoin transactions are linearly arranged in a sequence, commonly known as Blockchain ledger. The addition of new completed block in Blockchain is done by the help of consensus protocols. Blocks on Blockchain consist of some information and timestamp value and they are interconnected by a link in such a way that every block points to its previous block. Blockchain is nearly impossible to tamper because of Hashing function used in it. Blockchain relies on consensus algorithm to reach on an agreement among nodes participating in it. There are numerous consensus algorithms among which PoW- Proof of work algorithm and PoS- Proof of Stake algorithm are the most widely used consensus algorithms. This paper covers the basic detailed overview and review of Blockchain along with its architecture and characteristics, Bitcoin and comparison of various consensus algorithms.**

***Index Terms*: Blockchain, Bitcoin, Cryptocurrency, Consensus algorithm, Distributed, Decentralized.**

I. INTRODUCTION

The continuous growth of the Internet usage and the dependency on internet for online transactions has increased online vulnerabilities. Blockchain is a distributed ledger that is used to record transactions in the form of interconnected secured blocks[1]. Blockchain is named so because it stores blocks in chain where block stores the data of online transactions and they all are linked in chain. The digital pieces of information in Blockchain are called as "Blocks". Blocks consist of transactional information such as time, date and amount along the participant's information. For making the Blockchain more secure and tamper proof we use hash value. The hash values are one way and it is impossible to calculate same hash for two slightly different messages. Figure 1 shows basic of Blockchain with block and each block's hash value.

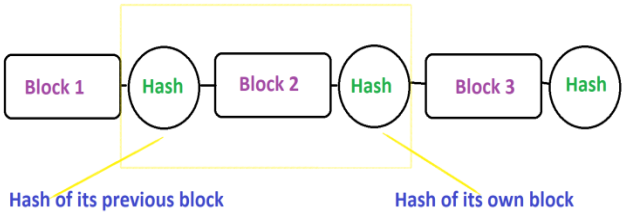

Fig.1 General view of blockchain

The Blockchain is considered secure because after a block has been added to the end of chain can't be altered. Hash value of each block and the hash value of previous block are stored in every block. If for a particular block its information is edited or changed then its hash is also changed along with actual content of that block. For adding a block to the Blockchain a certain procedure has to be followed. All the nodes present in the chain or network participate in the algorithm. For a block to be approved and to be added in the chain a node needs to get majority in its favor and after that its computed block can be added in the chain[3].

There is no centralization in Blockchain meaning there is no central control. The validity and security is achieved by the consensus algorithms. It is the part of consensus algorithm that only the winner node, that is declared winner by mutual agreement between all nodes present in the network, should add the block in the chain.

There are 3 types of ledgers: Centralized, Decentralized and distributed ledgers. In Centralized all nodes follows the decision taken by a single node. They mutually choose a node as their leader and follow every decision taken by that node. Whereas in Decentralized there does not exists a single point for decision making, the final result is the aggregated response of decisions taken by every node present in the network. In Distributed ledgers the processing is shared across multiple nodes, and then a decision is formed. It may be of two types Public or private. This paper will give a brief review of Bitcoin, Blockchain, Consensus algorithm and the difference between them. Figure 2 shows the architecture of Centralized, Decentralized and Distributed ledgers.

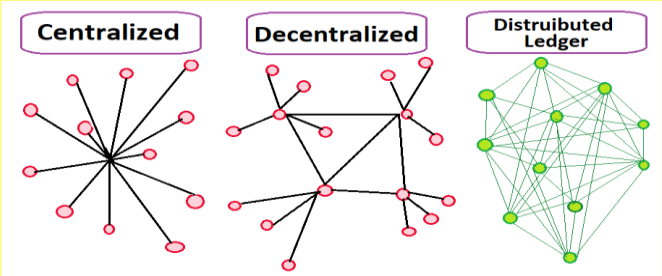

Fig.2 Centralized, Decentralized and Distributed ledgers

II. Background And Related Work

Satoshi Nakamoto [2] described design of digital currency Bitcoin in his research paper in 2008. He suggested a system for electronic transactions that doesn't rely on trust. In this section we will discuss various technologies related to Blockchain, Bitcoin and consensus algorithm.

1. TECHNICAL TERMS

Various terms are there like Cryptocurrency, Miner, Fork, Consensus, Transparent, Hash, smart contract[4] etc. Table 1 shows the definition of basic terminology used in Blockchain.

Table 1. Technical Terms

Terms	Meaning
Cryptocurrency	Also known as digital or virtual currency used to exchange online.
Blockchain mining	Process of adding transactions to the existing Blockchain among all users.
Miner	The one who validates new transactions and record them on Blockchain.
Consensus	Method used to verify the transactions.
Forks	The problem that arises when the node is used for different versions of Blockchain.
Hash	For checking the integrity of transaction of a message in one-way hash functions.
Nodes	The ledgers participating in the Blockchain.
Timestamp	A date and time in the computer system used as an electronic time stamp for the transaction.
Smart contract	Line of codes present on Blockchain that are executed automatically when some predetermined conditions are met.

2. BLOCKCHAIN

The Blockchain is a new and innovative technique that is Decentralized, Distributed ledger and open. In simple terms Blockchain is a linear series of blocks, called as records that are linked with each other using cryptography. According to Wikipedia Blockchain is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". Figure 3 shows the basic architecture of Blockchain.

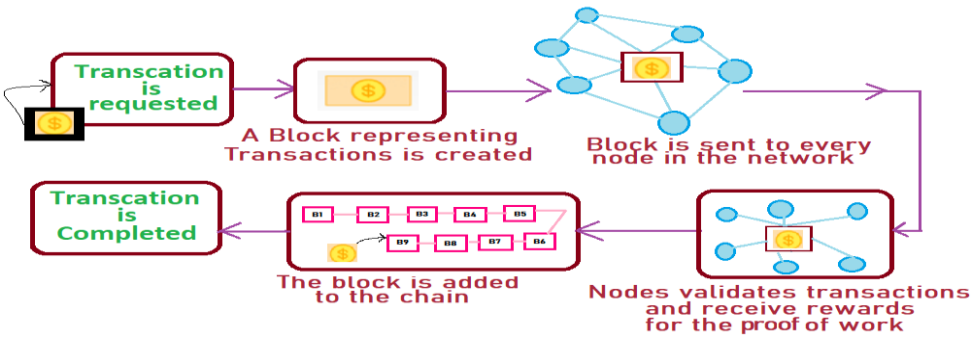

Fig.3 Blockchain Architecture

Blockchain is made up of blocks consisting a complete transactions records list executed previously[5]. First block of Blockchain is called genesis block and parent block. Each block of Blockchain consists of: certain type of computed data, the hash of the block and the hash from the previous block of the same chain. All nodes participating in the network competes and the one who wins adds the block into the Blockchain. The consensus algorithm plays an important role in this competition.

The basic difference between a database and a Blockchain is about the concept of centralization. In Database all the records are centralized. Blockchain is distributed and hence each participant has a secured copy of all records and all changes so each user can view the provenance of the data.

Decentralization, Persistency, Anonymity, Auditability are some of the key characteristics of Blockchain[6]. Blochchain are categorized into 3 types: public Blockchain, private Blockchain and consortium Blockchain[7]. In Public Blockchain anyone randomly can participate in consensus algorithm and the records of the Blcokchain is visible to every person. The private Blockchain is a kind of centralized that is controlled by any specific organization and the only members of that particular organization are allowed to participate in consensus. The Consortium Blockchain is constructed by several organizations. The following Table 2 shows the comparisons among public, private and consortium Blockchain[6].

Table 2. Public, private & Consortium Blockchain

Public	**Private**	**Consortium**
Consensus determination is by all miners	Consensus determination is by 1 Organization	Consensus determination is by selected set of nodes
Distributed	Centralized	Partially Centralized
Consensus process is permission less	Consensus process is permissioned	Consensus process is permissioned
Efficiency is low	Efficiency is high	Efficiency is high
Tampering of data is impossible here	Tampering of data can be there	Tampering of data can be there

The components of a Blockchain system consists of those functionalities that start from collecting transactions, propagating blocks, mining, achieving consensus and maintaining the ledger and so on. Figure 4 shows the layer of Blockchain Architecture [10].

1. Application Layer: This layer is used by end users to interact with the Blockchain network. This layer can be divided into application and execution two sub layers. The execution layer consists of smart contracts, underlying rules etc. A transaction executes from application to execution layer. Blockchain's semantic interpretation is defined by this layer.

2. Consensus Layer: It is responsible for validating, ordering and ensuring that all other nodes agree on the block added in the network. It provides the distributed consensus mechanism that decides the order in which the blocks are added in the chain. "Proof protocols" is an important component of this layer that can be used as consensus algorithm (e.g., proof of stake and proof of work). It also ensures that power remains distributed and decentralized.

3. Network Layer: It is responsible for internode communications. It also handles network functionalities like to maintain valid state of network it ensures that nodes can discover each other, can communicate with each other and also can propagate and synchronize among themselves.

4. Data Layer: Blockchain's data structure has 2 main things linked list and pointers. The data used is stored in this layer just like the hash and other important transactional data.

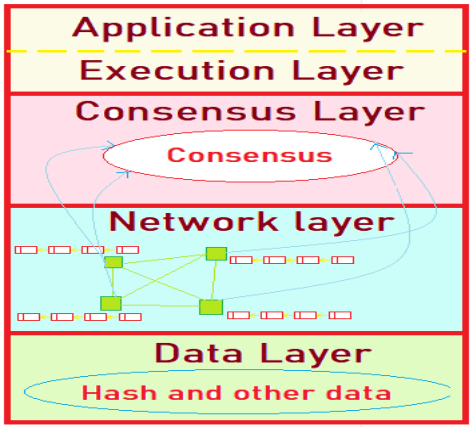

Fig. 4 Blockchain Layers

Apart from all the advantages that Blockchain have some disadvantages are also there.

1. The Scalability issue. Block size is limited to 1 MB while the mining is about every 10 minutes [6].

2. Secondly, it is extremely volatile. The main reason for this can be decentralization and Bitcoin is new to the market that's why the price is fluctuating day by day.

3. Thirdly, wastage of power. Some consensus algorithms require much higher power consumption; like Proof of work wastes too much electricity energy and no energy saving concept is there.

Some other disadvantages may include high cost, data is visible to all, performance is low and once done you can't alter the data of the block even if you want to.

3. BITCOIN

The digital or virtual currency used for exchange is termed as cryptocurrency. In simple terms a virtual currency or money secured by cryptographic technique is termed as a cryptocurrency. Bitcoin is a famous example of cryptocurrency that was introduced by Satoshi Nakamoto in 2009. He introduces crytocurrency in independent transactions that were decentralized and distributed, means no central authority was present in that transaction.

Blockchain and Bitcoin are two different concepts yet interconnected. Blockchain is a distributed ledger a decentralized approach for online transactions whereas Bitcoin is a cryptocurrency or electronic currency used in online transactions. Bitcoin is basically invented for Blockchain and it was Blockchain's first application. A cryptocurrency Bitcoin is transferred between two users but Blockchain is used to transfer other things like information or rights regarding property etc.

4. CONSENSUS ALGORITHM

Since in Blockchain there is no central control we need some mechanism to ensure the proper working of it. For the same purpose we use consensus protocol or consensus algorithms. All the nodes of network participate in the process to mutually agree on a decision and then only a verified block is added to the Blockchain. Applications of Consensus algorithm includes: Deciding whether to commit a transactions to database, Synchronizing state machine replicas designating node as a ledger for some distributed task and ensuring consistency among them. Figure 5 shows some of the properties on the basis of which we can compare the consensus algorithms[10].

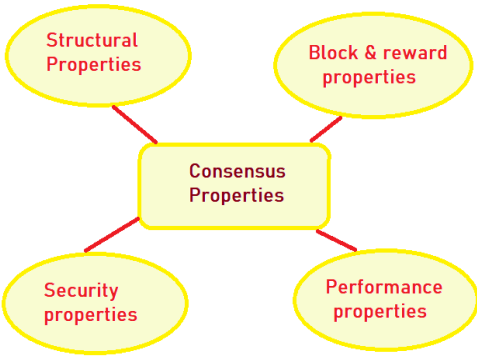

Fig. 5 Consensus Properties.

A number of consensus algorithms are present like

- PoW- Proof of Work,
- PoS- Proof of Stake,
- PoB- Proof of Burn,
- PBFT- Practical Byzantine Fault Tolerance,
- PoC- Proof of Capacity,
- PoI- Proof of Importance,
- Proof of Elapsed Time etc.

Following table shows the comparison of various consensus algorithms[6].

Table 3: The performance of various Consensus algorithms

Proof of Work algorithm	**Proof of Stake algorithm**	**Delegated Proof of Stake algorithm**	**Practical Byzantine Fault Tolerance algorithm**
Node identity management is open	Node identity management is open	Node identity management is open	Node identity management is permissioned
No Energy saving	Energy saving is partial	Partial energy saving	Yes it saves energy
Tolerated power of adversary <25% computing power	Tolerated power of adversary <51% stake	Tolerated power of adversary <51% validators	Tolerated power of adversary <33.3% Faulty replicas

III. CONCLUSION

The paper described the brief idea about Blockchain, Bitcoin and Consensus algorithms. The differences among them and how these terms are related with each other are also discussed in this paper in brief. Since the Blockchain is generated using the blocks created by nodes by participating in consensus algorithms and the hash is also attached, the current one and previous one, we can use

Digital signature along with Hash value to make it stronger and identify the node who have participated, won and added the block in the existing Blockchain. Also in the private Blockchain, where an organization participates in the consensus algorithm, Digital signature can be used in identifying the authorized person of an organization who can add block in Blockchain. This can reduce the one of the disadvantage of Blockchain and it also keeps it distributed. In the future work we can work in this aspect and can see the comparative results on the efficiency of Blockchain.

IV. ACKNOWLEDGMENT

We would like to acknowledge and extent our sincere thanks to Mr. Subhashish Goswami, Joint Director, Dev Bhoomi Group of Institutions and Mr. Dhajvir Rai, HoD CSE, Dev Bhoomi Group of Institutions for their regular guidance and encouragement in all aspects for successfully completion of this paper. Thanks to all the direct and indirect motivations present with us every time.

REFERENCES

[1] M. lansiti and k. Lakhani, “The truth About Blockchain”, Hardvard Business Review [Online], Available: https://hbr.org/2017/01/the-truth-about-blockchain.

[2] S. Nakamoto, “Bitcoin: A peer-to-peer Electronic Cash System”, 2008.

[3] Sachchidanand Singh and Nirmala Singh, “Blockchain: Future of financial and Cyber security”, 2nd International Conference on contemporary computing and informatics, 2016, IEEE 463-467.

[4] Pinyaphat Tasatanattakool and Chain Techapanupreeda, “Blockchain: Challenges and Application”, International Conference on Information Networking (ICOIN), 2018, IEEE, pp. 473-475.

[5] D. Lee Kuo Chuen, Ed., “Handbook of Digital Currency”, 1st ed. Elsevier, 2015.

[6] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen and Huaimin Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends”, IEEE 6th International Congress on Big Data, 2017.

[7] V. Buterin, “On public and private blockchains” [Online] Available: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

[8] I. Eyal and E. G Sirer, “Majority is not enough: Bitcoin mining is vulnerable”, In proceedings of International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2014, pp. 436-454

[9] A. Biryukov, D. Khovratovich, and I. Pustogarov, “Deanonymisation of clients in bitcoin p2p network” in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications security, New York, USA, 2014,pp. 15-29.

[10] Md Sadek Ferdous, Mohammad Jabed Morshed Chowdhury, Mohammad A. Hoque and Alan Colman, “Blockchain Consensus Algorithms: A Survey”, arXiv:2001.07091v2 [cs.DC], 7 Feb 2020.

[11] G.-T. Nguyen and K. Kim, “A survey about consensus algorithms used in blockchain," J. Inf. Process. Syst., vol. 14, no. 1, pp. 101-128, 2018.

[12] M. Iansiti and K. R. Lakhani, ``The truth about blockchain," Harvard Bus. Rev., vol. 95, no. 1, 2017, pp. 118-127.

[13] K. Fanning and D. P. Centers, ``Blockchain and its coming impact on nancial services," J. Corporate Accounting Finance, vol. 27, no. 5, 2016, pp. 53-57.

[14] I. Eyal, “Blockchain technology: Transforming libertarian cryptocurrency dreams to nance and banking realities," Computer, vol. 50, no. 9, 2017, pp. 38-49.

[15] A. Schaub, R. Bazin, Omar Hasan, and L. Brunie, “A trustless privacypreserving reputation system," in Proc. IFIP Int. Conf. ICT Syst. Secur. Privacy Protection, Cham, Switzerland: Springer, 2016, pp. 398-411.

[16] P. Ciaian, M. Rajcaniova and d. Kancs, "The digital agenda of virtual currencies: Can BitCoin become a global currency? ", Information Systems and e-Business Management, vol. 14, no. 4,2016, pp. 883-919.

[17] https://medium.com/distributed-economy/what-is-the-difference-between-decentralized-and-distributed-systems-f4190a5c6462

[18] https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture