Asian Journal of Multidimensional Research
ISSN: 2278-4853 Vol. 11, Issue 10, October 2022 SJIF 2022 = 8.179
A peer reviewed journal

CONSENSUS ALGORITHMS IN BLOCKCHAIN TECHNOLOGY: A COMPARATIVE STUDY

Satpal Singh*

*Assistant Professor in Computer Science,
University College Chunni Kalan,
INDIA
Email id: spsingh.mohali@gmail.com

DOI: 10.5958/2278-4853.2022.00238.5

ABSTRACT

Blockchain, nowadays, is a fastest growing distributed and secured technology that can be used in various fields. Bitcoin, that works on the PoW (Proof of Work) Consensus mechanism and commenced its services in 2009, is the most successful crypto currency today. The idea of Blockchain emerged out in 1991 by Stuart Haber and W. Scott Stornetta that a technology can run on a peer to peer network without any centralized authority. However it took almost 18 years to develop first Blockchain based application. In this type of network, each node contains the copy of Blockchain transactions that has been added to the system after validation. Consensus is a general agreement that has to be done between two parties in order to achieve an output. This mechanism guarantees that all the nodes in network are well coordinated and any illegal transaction must not occur in the system. Every Blockchain network uses different Consensus mechanism as per its requirements. In case of Blockchain technology, 51% of the present network nodes need to be agreed according to the contract in order to achieve the consensus. If a malicious node tries to control the network then it needs to gain the faith of 51% of the networks nodes that however is impossible. The main motive of Consensus mechanism is to secure the network and control any unauthorized activity that could be harmful for the network. Miners are the nodes that validate every new transaction that has to be linked in Blockchain. The consensus mechanism verifies that the block added in Blockchain is validated by the miners and a copy of this is distributed among all other nodes. Consensus algorithm becomes the backbone of a Blockchain network as it plays a major role in appending a block in a chain and ensures security. Consensus mechanisms can be differentiated in terms of difficulty level of computation, scalability, throughput, security and efficacy.

KEYWORDS: *Consensus, Scalability, Computation, Malicious.*

INTRODUCTION:

Blockchain is an open distributed ledger made up by the blocks of transactions carried upon by the nodes present in the network. Satoshi Nakamoto developed Bitcoin crypto currency in 2009 which is most successful digital currency yet. The idea of distributed network is the brainchild of Stuart Haber and W. Scott Stornetta which was fulfilled by developing Blockchain based Bitcoin

crypto currency [1]. Blockchain, nowadays, is a fastest growing distributed and secured technology that can be used in various fields. It is a chain containing blocks, whenever a transaction occurred, it appends into the chain by creating a new block. The foremost block of the chain is genesis block and it is not linked with previous hash. Every transaction recorded in a Blockchain is immutable, irreversible and every member of the Blockchain can see every recorded transaction. A copy of every transaction, in form of a block, is send to all the nodes present in the network. In contrast to traditional systems, where a centralized authority is supreme to take decisions and make transactions, Blockchain is decentralized technology in which every node especially mining nodes plays an important role to transact valuables and decision making. A block contains significant information about the transaction and link itself with the last block by using previous hash. Most of the Blockchain use SHA56 hashing algorithm to save its data from the hackers [2]. Other than information, a block consists of hash value, previous block's hash, block number, timestamp and a nonce.

A fault-tolerant method to attain a general agreement by following the predefined set of rules between two parties is called consensus mechanism. The major issue in a decentralized peer to peer network is to gain the confidence of all the network nodes in the presence of harmful nodes in the network. In case of Blockchain technology, 51% of the present network nodes need to be agreed according to the contract in order to achieve the consensus [3]. The consensus algorithm develops on the basis of agreement through which every network node reaches common consensus to add a block in Blockchain. This builds the trust between nodes of the network and provides better reliability. Verification of a block that will be added to the Blockchain, whether this block is validated by miner and copy is scattered among all participant nodes, is done by the Consensus mechanism. An algorithm to reach a consensus is must to follow Blockchain protocol. Validators or miners are responsible for kicking the faulty nodes out of the network. There are numerous Blockchain platforms available in the market today however Bitcoin, Ethereum and Hyper Fabric are most popular among all. The pivotal characteristics [4] of a Blockchain are –

- Peer to peer network
- Reliability
- Scalability

The consensus mechanism of a Blockchain mostly depends upon the above three features. The majority of consensus mechanisms allow only those users to append block in the chain that shares some assets or indulges him seriously in the process so that only genuine participants in the network perform duties reliably.

Following are the Consensus mechanisms those are yet discovered and used in Blockchain technology:

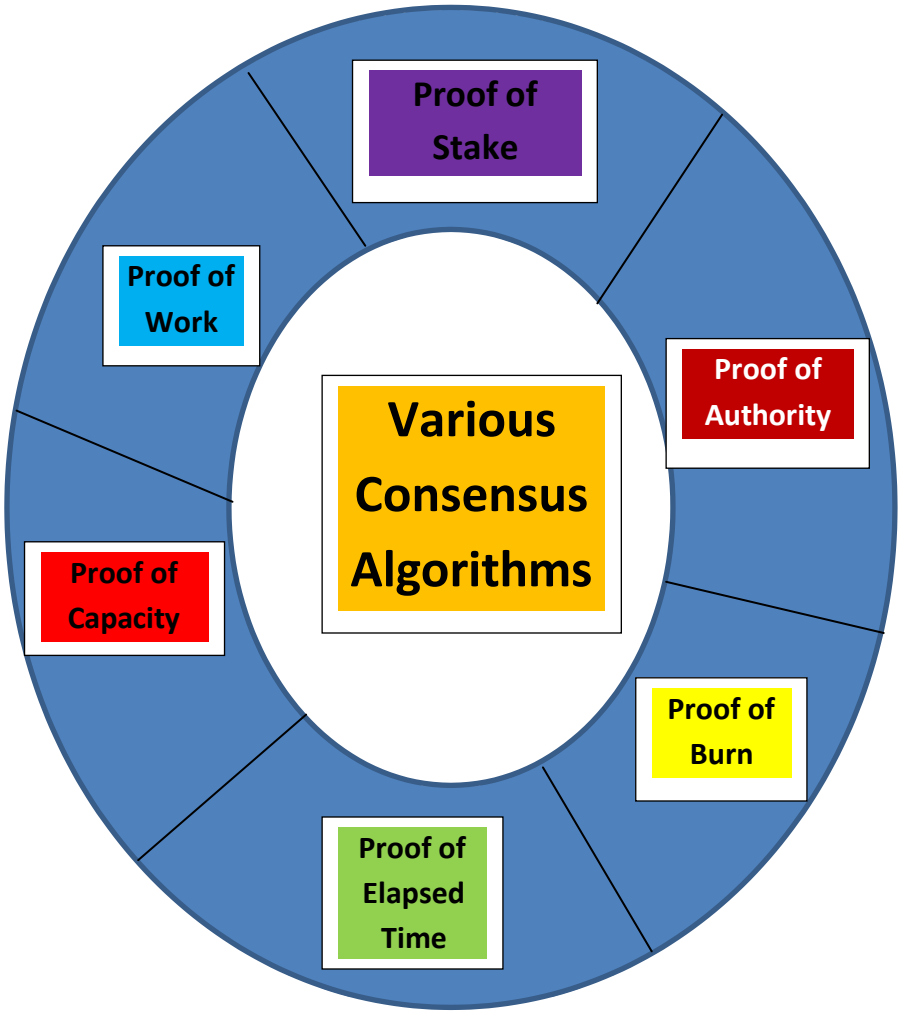

Figure 1: Various Consensus Algorithms

Proof of Work (PoW):

The most preferred and simplest mechanism and that was used in Bitcoin, first application of this type, is Proof of Work. This mechanism actually reveals the miner who will add next block in the chain. This algorithm is based on mathematical calculation to crack an equation in order to find a required number; the node that solves this riddle earliest will win and become the next miner [5]. Though the algorithm is manageable yet a lot of energy is consumed while solving the arithmetic equation. The whole process of solving the puzzle and adding a block into a chain is known as mining. Most of the time, miners took many transactions together in a block and try to mine it. Miners need to solve the problem to achieve the target hash. It becomes more complicated to mine a block if target number is low and whosoever mine the block gets a reward in return. It consumes a lot of time and energy of miners; hence they need to check different

nonce values to solve the puzzle. Despite of this, the cost of mining is much high because numerous electricity and special hardware i.e. graphic card is needed to complete the process.

Proof of Stake (PoS):

The most suitable alternative of Proof of Work algorithm is Proof of Stake. Miners in PoW are called validators in PoS. In this mechanism, the node that has more stake value has much chance to get the opportunity to become a validator. However, it doesn't give any guarantee to be a validator for biggest stakeholder rather it follows a randomized process to find a validator with high chances for a node with maximum stake. User need to put some amount of crypto currency as a debt to become a validator and can lose that money if it plays unfairly. Validator has to create and append a block in chain rather to waste its energy by doing unnecessary computation as in PoW. If a faulty user wants to alter the block in the chain by becoming validator, it needs to have 51% stake and it's unsafe for the malicious node because whenever it attests false node it risks losing its stake [6]. In this mechanism, electricity usage is much lower than PoW and no special equipment is requirement hence it isan energy efficient algorithm.

Proof of Authority (PoA):

PoW and PoS works in permission less network whereas PoA is designed to work in permissioned network. It's obvious that every node available in network is first authorised then let it to enter the network. According to the algorithm, nodes, those are reputed and successfully validate blocks in the past, or preapproved nodes, likely to be validators [6]. PoA's performance is much better than that of PoW and PoS, that's why it is suitable for private blockchain. It's not an easy task to become a validator in PoA, it follows a robust process and one needs to put its reputation on stake and needs to invest more money. Just like PoW and PoS, hacker needs to get control of 51% of nodes to commit any faulty activity in PoA, hence it is a permissioned network and controlling 51% pre authenticated nodes is impossible task. Comparatively, a few numbers of validators are there in PoA and it consumes less power and resources during validation.

Proof of Capacity (PoC):

In this mechanism, miners utilize memory of computer system rather than using computational power as in PoW. In this, node needs to provide its hardware space to the network so that it can store solutions of hashing issues. Node, that can assign larger storage unit to the network, it will store more hashing solutions hence get more chances to become a miner. It doesn't mean if a node constitute itself in mining activity through PoC can never use that space for other business, rather it can wipe off the mining data anytime from its computer and utilize that space for any other project. PoW takes 10 minutes to create a block whereas PoC takes only 4 minutes [5]. Blockchains that run on proof of capacity include Storj, Burst, Chia, and Space Mint.

Proof of Burn (PoB):

The most common alternative of Proof of Work algorithm is Proof of Burn because it consumes minimal energy as compared to the former one. In PoB, system doesn't need any super gadget to solve the mathematical problem rather it burns crypto as an investment in the blockchain system so by consuming these coins just for investment sake, users could not take risks to validate invalid transaction. More the investment a user do, more the chances a node get to become validator because it get more power to mine a block. The difference between PoS and PoB is that

in PoS, a user can withdraw any from the system and get its money back but in PoB, user have to destroy the coins forever to gain profit [9].

Proof of Elapsed time (PoET):

In Proof of Elapsed Time, nodes get a certain amount of time that is randomly decided by the system. The "miners" must first join the network, gaining a membership certificate. Once they are in the network, the nodes need to wait a certain amount of time that is randomly decided. The miner must wait at least the amount of time that was defined before starting of mining a new block into the blockchain. In PoET, the miner that has the shortest amount of time is elected to do the block mining that round. The system tends to be fair and choose miners with a good degree of randomness. It doesn't require much electricity consumption and miners can "go to sleep" while they wait for their turn [8]. The PoET algorithm is for permissioned blockchain networks. That is, a special verification is required from a node when it tries to join the network.

Layers in Blockchain System:

Whole Blockchain system is divided into three layers:

1. Incentive Layer: It consists of incentive model, rewarded elements, amount of rewards, reward distribution etc.
2. Consensus Layer: It consists of consensus protocol, transaction execution, block generation and reception, fork resolution etc.
3. Network Layer: This layer consists of number of nodes, network configuration, and information to be propagated, broadcast protocol etc.

Consensus Algorithm	**Energysaver**	**Access**	**Transationrate**	**Example**
Proof of Work (PoW)	No	Public	Low	Bitcoin
Proof of Stake (PoS)	Partial	Public	High	Ethereum
Proof of Authority (PoA)	Yes	Private	High	VeChain
Proof of Capacity (PoC)	Yes	Public	Medium	Burstcoin
Proof of Burn (PoB)	Yes	Public	Very high	Slimcoin
Proof of Elapsed Time (PoET)	Yes	Private	Medium	Hyperledger Sawtooth

Table 1: Consensus Algorithms.

DISCUSSION:

As discussed above, nowadays, a lot of consensus algorithms are there to be utilized in blockchain based technologies. Users of these technologies need to choose a consensus protocol

among many options as per their requirement. In order to enhance the standards and upgrade the durability, features of different consensus protocols must bind together in a library according to the need of software and user. When a variety of protocols are combined together, it will strengthen the capability of application by reducing its weaknesses , it results in improving the performance and efficiency.

REFERENCES:

1. Nikita Storublevtcev, (June-2019). "Cryptography in blockchain" In book- Computational science and its applications- ICCSA-2019.

2. Sheping Zhai, Yuanyuan Yang, Jing Li, Cheng Qiu. (2019). "Research on the applications of cryptography on the blockchain". IOP Conf. series. Journal of Physics, 1168-2019

3. Jameel, F.; Khan, W.U.; Shah, S.T.; Ristaniemi, T. (Dec. 2019). "Towards intelligent IoT networks: Reinforcement learning for reliable backscatter communications". In the Proceedings of IEEE Globecom Workshops, Waikoloa, HI, USA.

4. Jidian Yang , Shiwen He, Yang Xu, Linweiya Chen and Ju Ren, (2019). "A Trusted Routing Scheme Using Blockchain and Reinforcement Learning for Wireless Sensor Networks". MDPI, Basel, Switzerland.

5. Arshiya S Mohammad , M Nawaz Brohi , Iftikhar Alam Khan, ((2021). "Integration of IoT and Blockchain". Technium Vol. 3, Issue 8 pp.32-41 ISSN: 2668-778X.

6. D. Sivaganesan, (2021). "A Data Driven Trust Mechanism Based on Blockchain in IoT Sensor Networks for Detection and Mitigation of Attacks". Journal of trends in Computer Science and Smart technology (TCSST).

7. Sung-Jung Hsiao and Wen-Tsai Sung, (2021). "Utilizing Blockchain Technology to Improve WSN Security for Sensor Data Transmission". Computers, Materials & Continua, DOI:10.32604/cmc.2021.015762.

8. Cuong V. Nguyen, Minh T. Nguyen, Trang T.H. Le, Thang A. Tran, Duy T. Nguyen, (Dec. 2021). Blockchain technology in Wireless Sensor Network: Benefits and Challenges, ICSES Transactions on Computer Networks and Communications, Vol. X, No. Y.

9. Olfati-Saber, R., Fax, J. A., & Murray, R. M. (2007). Consensus and cooperation in networked multi-agent systems. Proceedings of the IEEE, 95(1), 215-233.

10. Cachin, C., & Vukolić, M. (2017). Blockchain consensus protocols in the wild. arXiv preprint arXiv:1707.01873.

11. Sukhwani, H., Martínez, J. M., Chang, X., Trivedi, K. S., & Rindos, A. (2017, September). Performance modeling of pbft consensus process for permissioned blockchain network (hyperledger fabric). In 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS) (pp. 253-255).

12. Yang, J., He, S., Xu, Y., Chen, L., & Ren, J. (2019). A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks. *Sensors (Switzerland)*, *19*(4). https://doi.org/10.3390/s19040970.