MAT JOURNALS

Journal of Computer Science Engineering and Software Testing
e-ISSN: 2581-6969
Volume 6 Issue 1

A Contrast on Blockchain Consensus

Ayush Kamal Anand[1], Manisha R Rao*[2], Madhu B R[3]
[1]UG Student, Department of Computer Science and Engineering, JSSATE, Bangalore, Karnataka, India
[2]UG Student, Department of Computer Science and Engineering, Jyothy Institute of Technology (JIT), Bangalore, Karnataka, India
[3]Associate Professor, Department of Computer Science and Engineering, Jyothy Institute of Technology (JIT), Bangalore, Karnataka, India

INFO

Corresponding Author:
E-mail Id:
**mannu.r.rao@gmail.com*

DOI:

Cite as:

ABSTRACT

Blockchain is a cryptographic database maintained by a network of computers, each of which stores a copy of the most up-to- date version. The Blockchain mainly deals with confidentiality, privacy and authenticity along with consensus. In this paper we analyze the various consensus methods that are bounded with blockchain. Consensuses are set of rules to make sure the transactions done are validated or not.

Keywords: *Blockchain, consensus, algorithm, transaction, system*

INTRODUCTION

Blockchain works as a decentralized system. It involves in checking the authentication of a transaction made in the network. Several users in this network are in the distributed. Proof of Work (PoW), Proof of Burn (PoB) and Proof of Stake (PoS) are most used proofs in this algorithm.

Miners validate the transactions and construct a block of transaction, each pointing to previous block through hash functions which makes the tracing of transactions impossible without the key value [1, 2].

The Bitcoin is backed by concept of blockchain. Bitcoin is a decentralized digital currency that enables instant payments to anyone, anywhere in the world. It has no centralized authority and transaction is held through peer to peer technology. Despite dozens of benefits in bitcoin, it still can be used for money laundering. This is because bitcoins are not linked to a person's profile instead are linked to their private key connected to that account.

Blockchain is not all about bitcoin; it can be used in various other fields like public sector, financial services, retail, insurance service etc. One common usage of blockchain could be citizen identity. A person's identity is needed in every domain of registration [3]. If there is a small change in any one of the details, say address then the person needs separately update it in every domain. Instead if he/she uses the blockchain technology the update can be done at a time in all the fields. The decision of who should and how the update is made is through consensus. The

consensuses are made sure that the transactions made in the ledger are real and authorized. Double spending and unauthorized transaction can be avoided through consensus. These algorithms are used in the cryptocurrency world where one does not truly trust the other party and also it reduces the need of middlemen in the network. Considering different situations, we have different consensuses models [4]. Each blockchain consensus differs mainly in the way they are entrusted and the way reward is earned for the verification of transactions. Most consensus model used in blockchain is a combination of these consensus algorithms. We need not choose only a single consensus for their network.

There are many consensus algorithms available like Proof of Work, Proof of Stake, Proof of Burn, etc. These consensus algorithms are put to ensure a group of people agree that all transactions are validated and authentic. Here, there are no primary authorities are in-charge, in-fact anybody inside the node is equally accountable for every transaction that was proven in the network.

TYPES OF CONSENSUS

- Proof of Work
- Proof of Burn
- Proof of stake
- Proof of Capacity
- Byzantine Fault Tolerance
- Proof of Elapsed Time

Proof of Work

Proof of Work (PoW) was found in 1993, Satoshi Nakamoto used PoW as a consensus mechanism for Bitcoin. A trustless and distributed consensus system implies that if you need to send or receive money from somebody you do not trust in third-party services. After you use ancient ways of payment, you would like to trust in a third party to set your transaction. They keep their own private register that stores transaction history and balances of every account. With bitcoin, everyone has a copy of the blockchain, so no one has to trust in third parties because anyone can directly verify the information written [5].

Proof of work is a consensus protocol introduced by Bitcoin and used widely by many other crypto currencies. This process is known as mining and as such nodes on the network are known as miners. The PoW is just like a solution to the mathematical problems, which needs a lot of work to finish but the solution can be verified easily. These mathematical riddles are solved through the nodes in the network which are running a long random process of representing the solutions on an experience basis. Technically, this means that the problem could be solved on first attempt, although this does not happen. The answer needs to be a lesser in number than the hash of the block for it to be accepted, known as the target hash. At header of a hashed block a numerical value which is called as target hash, lower the number tougher to make a block. A miner tests different distinct values (known as nonce) until the produced one is suitable for using. The miner who manages to unravel the riddle mines the next block, adding it to the chain and validating the transactions in it and receiving the reward for the block. The method involves guaranteeing every confirmed block in the chain rewards the miner in the cryptocurrency that they are mining through the dealings fees collected for sending currency across the network, moreover as any planned reward. It makes sure that miners are motivated to maintain a blockchain by rewarding them. The process of solving these riddles are highly difficult and costly hence to compensate

the efforts of the minor the rewards are given. Since miners play a main role in maintaining the network it is important to keep the miners encouraged for the same. PoW is mainly used for prevention and detection of fake transactions.

Proof of Burn

Proof of burn (PoB) basically deals with destroying or burning the coins to get the rights of a miner. It works like virtual mining. A computer system works for mining bitcoins is called mining rig. A virtual mining rig is bought if the coins are burnt. As the number of coins that are burnt increases, the power of the mining rig also increases. Mining can happen for a long time, but over the period power is lost.

The burned coins are sent to a remote address called 'Eater Addresses". It was a verified address which does not have a private key or user to perform a transaction but the details can only be seen by other users and not access it. For the miners to maintain their position as miners they have to keep burning the coins but with every burn the power of coins decreases. This encourages long term miners in the network [6]. The network functions normally during PoB and the result burnt is rewarded in the form of native cryptocurrency to the miner. The transaction fee in network can also be paid by the same consensus. PoB is a risk factor because there is no guarantee that the burnt coins are gained again. The crypto currencies using this type of consensus are counterparty, slim coin and factom.

Proof of Stake

The Proof of Stake (PoS) consensus algorithm uses a mechanism where blocks are validated in accordance with the stake of the participants. The validator of each block is determined by an investment of the coins or stakes itself and not by the amount of computational power allocated. In PoS if a user has about n% of stake in network then his share of mining would be n% only. And selection method through PoS is either by the user with lowest hash value and highest stake or the user with the oldest highest stakes. PoS will help in avoiding the same miners with highest stake to be used again and again.

A user can mine or validate the transactions through number of cryptocurrency he or she owns. The user who has to validate through PoW must do some computational work. But the electricity required for such power is very high, also the block rewards are either less or none. As the network is used further the number of miners will decrease, since they would not be able to invest for computation with less block rewards. This is called Tragedy of the commons. The only mining fee the miners might get is through the transactions made by the users, but with time the users might want to lessen the transaction cost. These networks are subjected to the 51% attack. In a network when a miner can hold up 51% of the computational power for creating and owning the fraudulent blocks that leads to invalid transactions. In PoS the 51% attack would not happen because the miner's stake is in consideration, so if a miner with 51% stakes does any fraud in network the maximum loss would be on his plate. It would be hard to retrieve his or her lost stakes. Hence PoS are best when one need to avoid the 51% attack.

The security and energy consumption problems faced by PoW is solved here. The first cryptocurrency that used PoS was peer coins. Later NXT, Ethereum, black-coin also adopted PoS.

Proof of Capacity

Proof of Capacity (PoC) can also be referred as proof of space. Hard drives and Storages are main part of PoC. Proofs are created by memory or disk allocations as resources for PoC. These proofs are used to check the authenticity of information stored in by miners in the network. Plotting is a process for PoC needs Energy but considerably lesser than PoW. In a plot file, repeated hashed data that leads to nonce is stored in the given space by miners. The generation of this plot proves that the space is allocated for mining. PoC are used in the traditional client puzzle applications such as denial of service attack prevention. It is also a great help in malware detection.

Byzantine Fault Tolerance

The Byzantine General's Problem was proposed in 1982 as a logical dilemma that illustrates how a group of Byzantine generals may have communication issues when trying to agree on their next move. The dilemma is taken as there are many armies leads by a general each of which is at different locations and is ready for an attack. The generals from each location need to have a unified decision in order to get proper outcome. Therefore, we may consider the following requirements:

- Each general has to decide: attack or retreat.
- After the decision is made, it cannot be changed.
- All generals have to agree on the same decision.

Therefore, the issue in communication arises when one of the general communicate through a courier containing the message for the other general [7]. The challenge arises when the messages are delayed, destroyed or lost. Although the message maybe delivered successfully but if one of the general changes the message while passing it to the other general. This results in total failure. If we consider the same situation in the case of blockchain each node can be said as one general and the nodes are yet to reach consensus. Majority in the network must agree upon a common point to avoid the total failure. Therefore, if there is at least ⅔ or more reliable and honest network nodes the consensus can be achieved. Also, if majority of the nodes are fraudulent then there is still total failure.

To overcome the faults in the above-mentioned issues Byzantine fault tolerance (BFT) came in to rise. The same was used in blockchain with different solutions for each issue.

Proof of Elapsed Time

Proof of Elapsed Time (POET) is a consensus belonging to permissioned blockchain, where the users in network are identified. In POET, every member asks for a hold-up time from its local reliable enclave. Once the member waits for the given time, the one with nearest hold-up time is offered the block. The potential and the results are signed by each privately trusted user thus confirming that there is no cheating in the waiting time by any member. The time they have to be held up will be randomly allocated so that node does not have to choose any short duration and thus claim the reward, it helps in getting proper and fair decision. It does not lead to high power consumption rather allows the users to sleep and let the other tasks for that node is completed and hence efficiency of the node is increased. Even though this method is quite similar to POW, (the work referred to sleep) this method is applicable in a permissioned blockchain which leads to trusted network. It is also cost efficient when compared to other proofs. POET was invented by Intel (Table 1).

Table 1: *Comparative analysis.*

	Proof of work	Proof of burn	Proof of Stake	Proof of capacity	Byzantine Fault Tolerance	Proof of Elapsed Time
Permissioned or Not	Not permissioned	Not permissioned	Not permissioned	Not permissioned	permissioned	permissioned
Energy Consumption	Waste more Energy	Consume more Energy	Less Energy Consumption	Less use of Energy	No Energy use	Energy not used but takes time
Hardware Requirement	Required	Not Required	Not Required	Required	Not Required	Not required
Memory Requirement	significant	yes	Significant	Need a hard drive	Less than Pow and Pos	No need
Security	Attack is possible with 51% hash power	Burned coins may not be regained	Removes 51% attack threat	possibility of malware attacks	May have a single point of failure	It's a trusted network

CONCLUSION

Each consensus has its own pros and cons like even though POW is more efficient bound to high energy consumption. POB cannot be always used due to burning of the assets which sometimes leads to loss. POS is more secure way but to keep the lead one needs to have a good stake which affects the trading process. POC needs considerate amount of hardware which leads to cost effective. BFT and POET both are supported in private blockchain network only where BFT may have single point failure and POET is time consuming process. Hence the consensus to be used mainly depends on the facility that can be utilized.

REFERENCES

1. Dr. Arati Baliga (2017), A white paper "Understanding blockchain consensus models", pp. 1-14.
2. Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, Huaimin Wang (25-30 June, 2017), "An overview of blockchain technology: Architecture, consensus, and future trends", *IEEE 6th International Congress on Big Data*, Honolulu, HI, USA.
3. Prableen Bajpai (25 June, 2019), "Cryptocurrency" *at Investopedia*.
4. L. M. Bach, B Mihaljevic, M Zagar (21-25 May, 2018), "Comparative analysis of blockchain consensus algorithms". *41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, Opatija, Croatia.
5. Achampet Harshavardhan, Dr. T. Vijayakumar, Dr. S. R. Mugunthan (30-31 August, 2018), "Blockchain technology in cloud computing to overcome security vulnerabilities", *2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, India.
6. Kai Lei, Qichao Zhang, Limei Xu, Zhuyun Qi (11-13 December, 2018). "Reputation-based byzantine fault-tolerance for consortium blockchain. *IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS)*, Singapore.
7. D. Mazieres (2015), "The stellar consensus protocol: A federated model for internet-level consensus," *Stellar Development Foundation*, pp. 1-32.