A Survey of Different Consensus Algorithm used by Various Cryptocurrencies

Richa Bansal
Extension Lecturer, Department of Computer Science,
Pt. J.L.N. Govt. College Faridabad, India

***Abstract*— Decentralized digital money is the future of transaction. Based on blockchain technology, they consist of a distributed ledger where the records of transactions are stored across many nodes instead of storing the information on a single central authority. Now when there are different nodes involved in transaction, we need to have some methods to authenticate those transactions. Such methods are called consensus algorithms. And the process of authenticating each transaction is called mining. This paper discusses different consensus algorithms being used in some popular cryptocurrencies.**

Keywords*— *Transactions, Consensus Algorithm, Cryptocurrencies

I. INTRODUCTION

When a digital transaction is made in a decentralized system, there are a few things that need to be verified such as

- Sender (the one who initiated the transaction using his digital signature)
- Validity of transaction (whether the sender has enough balance to complete the transaction)
- Receiver (the person receiving the money)

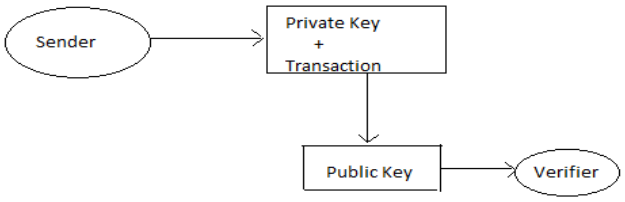

Fig. 1. Data being verified by the verifier

While in decentralized systems, there are a number of participants that verify the transactions and add them to the block of verified transactions, so we need a mechanism such that all the participants agree on the status of the transaction. Consensus mechanism refers to methods that validate a set of transactions or a single data value. It also refers to choosing a non-malicious node for validating a new block to the blockchain on a distributed network. Some consensus algorithms also help in dealing with the problem of forking [1] which occurs when multiple miners mine a common block of transaction. Further in this paper we are going to discuss about the various consensus algorithms being used in different cryptocurrencies.

II. CONSENSUS ALGORITHM

Let us discuss some of the common consensus algorithms and the cryptocurrencies they are used in.

A. *Proof of Work (PoW)*

In this consensus algorithm, the authenticity of a transaction is based on the hash value. There are a number of miners that are mining the hash value of the transaction. This hash value computes whether the transaction should be added to the block of verified transactions or not. The miner who calculates the correct hash value in minimum time period is rewarded with some precise cryptocurrency. Bitcoin, Litecoin and

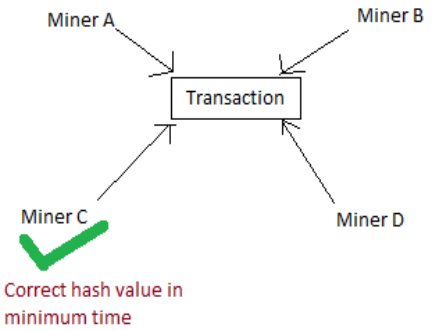

Fig. 2. Miners calculating the hash value of the transaction

DogeCoin are some of the cryptocurrencies using the Proof of Work algorithm to authenticate the transactions.[2]

B. *Proof of Stake (PoS)*

In the previous algorithm the problem that occurs is consumption of high amount of energy to compute the hash value of single transaction. *PoS* uses the concept of coinage to allow the mining of a transaction. [2] The miners are encouraged to maintain a stake of coins for which they are rewarded with some interest. The one having maximum stake is allowed to mine the transaction. The miner is also rewarded for holding the stake of the digital currency. Though Ethereum was initially using *PoW* to authenticate the transactions but Ethereum 2.0 would be using *PoS* consensus algorithm.

C. *Proof of Authority (PoA)*

Proof of Authority algorithm is based on authorizing the node before adding any transaction to the block. Only the authorized node is allowed to create a new node. [5] The nodes that are authorized are added to the list of validating nodes and the node that is currently adding a new block is the leader node. The popular cryptocurrency using this algorithm is the Binance Coin (BNB).

D. *Proof of Vote (PoV)*

Another efficient algorithm to add block to the network is the Proof of Vote (*PoV*). [3] This procedure consists of:

- Commissioner: The one who is responsible to add a block to the network.
- Butler: The one who is responsible to generate a block.
- Butler Candidate: The one who applies to become a Butler.

Let' see how the actual procedure works: when a user makes a transaction, the transaction is verified by the Butler. Now the butler will generate a block of such transactions that are verified. Now the commissioners will vote for the block that whether the block should be added to the network or not. To add the block, we need at least 51% of the votes by the commissioners in the favor of the block. [3] Further we have Butler Candidates waiting online to be selected as Butler. The Butler is also selected by election from all the Commissioners.

E. *Proof of Capacity (PoC)*

Proof of Capacity evolved as the best solution to solve the problem of energy consumption in *PoW*. In this case, the nodes use the space on their hard drives to mine the hash value. The more the space on the hard drive, the more are the chances to match the hash value in minimum time and get rewarded. The logic behind this algorithm is to keep a record of possible hash values before starting the mining procedure. The algorithm goes through two phases:

- Plotting- This process starts with repeated hashing of data and storing the nonce values calculated from these hashing techniques.
- Mining- Now these nonce values are used to calculate the deadline and the one having the minimum deadline gets the chance to add the new block to the blockchain and get rewarded.

BurstCoin and Chia are some of the cryptocurrencies using this algorithm.

III CONCLUSION

There have been many researches in developing an efficient consensus algorithm to decide the authenticity of a transaction. There are many factors on which these algorithms are evaluated such as computational complexity, power consumption, maintenance cost. This paper discusses a brief about the procedure of various Consensus Algorithms and their use in Cryptocurrencies.

A future work may consist of a hybrid technique of two or more consensus algorithm to produce a more efficient algorithm that uses less power consumption and providing high securities.

REFRENCES

[1] Siva Sankar Lakshmi, M. Sindhu, Sethumadhavan M. "Survey of Consensus Protocols on Blockchain Applications", 2017 International Conference on Advanced Computing and Communication Systems (ICACCS -2017), Jan. 06 – 07, 2017, Coimbatore, INDIA

[2] Mingxiao Du, Xiaofeng Ma, Zhe Zhang, Xiangwei Wang, Qijun Chen "A Review on Consensus Algorithm of Blockchain", 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC) Banff Center, Banff, Canada, October 5-8, 2017

[3] Li Kejiao,Li Hui , Hou Hanxu , Li Kedan and Chen Yongle ," Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism & Consortium Blockchain", 2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems

[4] Masseport Samuel, Lartigau Jorick, Darties Benoît, Giroudeau Rodolphe, "Proof of Usage: User-centric consensus for data provision and exchange"

[5] Ekparinya Parinya, Gramoli Vincent, Jourjon Guillaume," The Attack of the Clones Against Proof-of-Authority"

[6] Wahab Abdul, Memood Waqas," Survey of Consensus Protocols"

[7] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Consulted, 2009.

[8] https://www.investopedia.com/terms/p/proof-capacity-cryptocurrency.asp

[9] https://www.geeksforgeeks.org/proof-of-authority-consensus/