DOI: 10.56452/2021SP-8-037

ISSN: 0974-5823 Vol. 6 (Special Issue 4, November 2021)

International Journal of Mechanical Engineering

Consensus Methods: Analyzation for Blockchain Technology

Sakshi Sharma[1] and Rohit Sharma[2]

[1]Department of Computer Science & Engineering, Chandigarh Engineering College, Jhanjeri-140307, Punjab, India
[2]Department of Computer Science & Engineering, Jaypee University of Information Technology, Waknaghat-173234, Himachal Pradesh, India
E-mail: imsakshivk@gmial.com

Abstract: In blockchain technology, the consensus method act as a key function in maintaining the security and authentication of filling recorded in the blocks. an assortment of blockchain consensus methods have been proposed. Still, there is no scientific investigation and assessment as a directive to conclude which type of consensus method should be agreed to in a exact situation/application. The main focus of this work is to investigates soem major consensus methods in the blockchain, namely, Proof of work (POW), Proof of stake(POS), Delegated proof of stake (DPOS), Practical Byzantine fault tolerance (PBFT), Proof of capacity(POC), Proof of elapsed time (POET), Proof of activity (POA), Proof of publication(POP), Proof of retrievability (POR), Proof of importance (POI), Proof of ownership (POO), Proof of burn (POB), Proof of History (POH).

Keywords: Bitcoin, Blockchain, Consensus, Cryto, Digital Currency Ledger.

Introduction

Consensus method/mechanism/method is utilized in blockchain to supervise all the nodes that make transactions on the network. The main purposed of these methods is to assure the synchronization of all available nodes in the network and let them reach on single desicion like which transaction is authentic and which node will process that transaction and finally add it to network. Consensus Methods is as important to blockchain as brain is for human.

Every of blockchain has diverse purpose situation. The accepted consensus method desires to fit the needs of exact purpose situation. In this paper, we introduce some main consensus methods of blockchain and analyze their presentation and relevance of situation.

Consensus methods

In disseminated arrangement, no ideal consensus method exists [8]. The consensus method desires to build a swapping among steadiness, accessibility and separation fault acceptance [1]. We craft a comprehensive portrayal of some accepted blockchain consensus methods in the following section.

Proof-of-Work

PoW is the generally known consensus component used by the majority of digital money like Lit coin and Bit coin. The PoW is recognized as minning component and the nodes took part in system to complete the process are known as miner. In this, excavators tackle perplexing and troublesome numerical issues and riddles with the assistance of high estimate power and high hanling time. The key miner who settles the riddle to make a block gets a prize with digital currency [2].

DOI: 10.56452/2021SP-8-037

Proof-of-Stake (PoS)

PoS is the number two used normal consensus component option in contrast to PoW. PoS utilizes loss-energy, minimal handling time, minimal expense, less computational power as compared to PoW. PoS utilizes a randomized strategy to pick who will make the subsequent new block in the chain. Validators are available in PoS, in place of the miners [2]. The clients can bet their tokens to turn into a decider node which implies they bet their cash for a specific timeframe to make another block. The client with highest stake has the most elevated opportunity to turn into a decider node(validator) and an opportunity to make another block. The energy of other validators can be saved by using PoS as the choosen validator can make new blocks. PoS is exceptionally helpful consensus component on the grounds that when a validator makes wrong commitments he loses all his stakes and hence a new node can be selected as the validator. The validator are compensated for authentically according to work they do. . The other validators who check and approve the block get their exchange charges since they acquire no reward, in contrast to PoW. It utilizes the Ethereum stage.

Delegated-Proof-of-Stake(DPoS)

DPoS is an exceptionally quick consensus component and utilized for the execution of EOS. Right off the bat, we figure out "delegate." It implies an individual or an association that can deliver blocks on the organization. It gets the most extreme figure of votes as of every one of the hubs of the organization to make a block and obtain compensation [2]. The representatives are compensated with the exchange charges or with a proper measure of tokens that are made during expansion. The hubs of the organization can stake their tokens to decide in favor of representatives while using DPoS. The amount of stakes decides the heaviness of the vote.

Practical Byzantine Fault Tolerance (PBFT)

Byzantine adaptation to non-critical failure (BFT) is the opposition of a shortcoming lenient dispersed PC framework against part disappointments. NEO has used PBFT as consensus component. BFT has a similarity for the issue looked by a dispersed registering framework [5].

Practical Byzantine adaptation to non-critical failure was created to tackle the issue of a dispersed processing framework in BFT. PBFT consensus system worked on the guideline of BFT for confirming and the blocks utilizing a political decision process comes after the approval cycle.

Hyperledger fabric is one of the most successful implementation of blockchain that is using PBFt as Consensus Component [5].

Proof-of-Capacity (PoC)

For plotting tasks , the consensus component widely used is Proof-of-Capacity (PoC). PoC arrangements are pre-stored in the memory hard-disk in contrast to PoW where diggers utilize computational ability to pick a right arrangement. The diggers utilized the stored capacity information to draw a plot, along selected line and the interaction formed is entitled plotting. Once the capacity information is plotted, excavators can partake during the time spent block creation. The greater capacity, excavators have, the more arrangements, a digger can store. Hence, along selected lines, the excavators with bigger stockpiling capacity have a high likelihood to make another block utilizing this system.

Proof-of-Elapsed Time (PoET)

PoET is a consensus system that picked diggers in an irregular and reasonable way. It likewise concludes that who will deliver another block by picking a digger. This consensus component depends on the time that the diggers have sat tight for the making of the block. The interaction relegates an irregular and fair stand by time to every one of the hubs on the organization. The hub on the organization whose stand by time completes first will deliver another block. This instrument functions admirably for check in the event that a framework has no different hubs and a doled out stand by time is really an irregular worth.

Proof-of-Activity (PoA)

PoA consensus component utilizes considerably more work like PoW with decreased intricacy as the arrangement requires additional time from a small portion of seconds to a few minutes. PoA can be seen as a consolidate of PoW and PoS. Diggers tackled the cryptographic riddles as done in PoW and afterward, movements is done as done in PoS. The thing that matters is that where blocks contain formats rather than exchanges that incorporate header data and address of mining reward. Using PoA, the blocks are checked by restricting the base conceivable time for the production of a block that permits the greatest number of blocks added to the chain. It also keeps the organization away from the conditions of spams like flooding.

Proof-of-Publication (PoP)
When the situation is to check whether some specific data has been distributed at a specific time and date, then the PoP consensus method is mosty appropriate to be used. PoP utilizes the hashing tehnology to safely encrypt plain text to cipher on the blockchain.

Proof-of-Retrievability (PoR)
When we have to deal with a client and server based application on blockchain network the PoR is the ideal choice for such application. Using poR we an keep trackl of a files being downloaded completely on client machine from the server and vice versa. Productivity is increased using PoR as compared to other consensus methods in case of client and server based model.

Proof-of-Importance (PoI)
During the new economy development (NEM) the concept of PoI was introduced. PoI is utilized to check the substance mindful to confirm the blockchain exchanges [6].

Proof-of-Ownership (PoO)
At a specific time to validate some particulatr data PoO is utilized. This consensus instrument can be utilized by elements, like business associations, to affirm the uprightness, distribution date, and their manifestation’s ownership or agreements. Here, the purchaser (consumer) and the merchant (verifier) first checjk the ownership of product, which helps to achieve safe P2P interactions. The purchaser verify whether dealer really claims the pass prior to settling on the choice to purchase. Then again, the beneficiary is ensured with a moment installment (because of the advantages of blockchain) as long as the dealer is the real proprietor [4].

Proof-of-Burn (PoB)
For PoS and PoW, the elective consensus developed is PoB. Proof-of-burn (PoB) system works as, the diggers demonstrate that they burn one digital money to make coins, i.e., they are shipped off a bitcoin address which is cannot be suspended. The PoB relies upon the burning of tokens in such a way that they cannot be recovered. Likely near to PoW and PoS, PoB effectively irrefutable however difficult to fix [6].

Proof-of-History (PoH)
Proof of History is a gathering of estimation that can give a way to deal with check section of time between two events cryptographically. It uses a cryptographically protected capacity made so that outcome can't be expected from the data, and ought to be completely executed to make the outcome [6, 7, 8].

Analyses

The following tables are showing the analysis for all the discussed consensus methods on the basis of resource usage, cost, throughput, platform and other criteria.

DOI: 10.56452/2021SP-8-037

Table 1: Analysis on the base of node(public or private) and programming language can be used.

Consensus Method	ID of Node	Programming language
Proof-of-Work	Public	Golang, C++,Solidity
Proof-of-Stake	Public	GO, C++
Delegated-Proof-of-Stake	Public	GO, C++, JAVA
Practicla byzantine Fault Tolerance	Private	Java, Golang
Proof-of-Concept	Public	Mostly All
Proof-of-elased-Time	Public	Python
Proof-of-Activity	Public	Solidity, Java, Python
Proof-of-Publication	Private	Golang, C++,Solidity
Proof-of-Retrievability	Public	Golang, C++,Solidity
Proof of Importance	Public, Private	Java
Proof-of-Ownership	Public, Private	Mostly All
Proof-of-Burn	Public	Golang, C++,Solidity
Proof-of-History	Public	Mostly All

Table 2: Analysis on the base of resources like Efficiency, Resource Consumption, Cost(H-high, L-low, M-medium), Throughput(H-high, L-low, M-medium).

Consensus Method	Efficiency in term of energy	Consumption of resources	Cost	Throughput rate
Proof-of-Work	No(most emery consumption)	High CPU	H	L
Proof-of-Stake	Yes	Fast	M	H
Delegated-Proof-of-Stake	Yes	Fast(more than PoS)	L	H
Practicla byzantine Fault Tolerance	Yes	High CPU, High Bandwidth	L	H
Proof-of-Concept	Yes	High Memory	H	H
Proof-of-elased-Time	Yes	high	M	M
Proof-of-Activity	NO(\much better as compared to PoW)	H	H	H
Proof-of-Publication		L	L	H
Proof-of-Retrievability	YES	L	L	M
Proof of Importance	YES	M	M	M
Proof-of-Ownership	YES	M	M	M
Proof-of-Burn	YES	M	M	M
Proof-of-History	YES	M	M	M

Table 3: Platforms and Drawbacks pointed out from Analyses.

Consensus Method	drawbacks	Platform for implementation
Proof-of-Work	Its not secure as compared to new consensus methods, and also uses very high resources	Native, Ethereum virtual machine
Proof-of-Stake	Sometimes the richest is the solo consensus controller	Native, Ethereum virtual machine
Delegated-Proof-of-Stake	Only delegated have the power and has controller of all tokens	Native, Ethereum Virtual Machine, EOSIO
Practicla byzantine Fault Tolerance	On large scale nodes the communication overload is very high	Docker , Hyperledger Fabric
Proof-of-Concept	Can be infected from malicious miners	
Proof-of-elased-Time	Requires dedicated hardware and security	Hyperledger Sawtooth
Proof-of-Activity	Its more scalable but security is compromised at the same time	Decred (D-Cred)
Proof-of-Publication	Can only be used to check the publication details	Native, Ethereum virtual machine
Proof-of-Retrievability	Very small node network , not scalable	Native, Ethereum virtual machine
Proof of Importance	Risky in terms of zilch at stake	NEM Blockchain
Proof-of-Ownership	Requires the authorizations hence increases the cost of consensus	Crytocurrency
Proof-of-Burn	Not cost effective for single node and resource usage is very high	Crytocurrecny
Proof-of-History	Effective only in the case where similar type of work is done.	Solana

DOI: 10.56452/2021SP-8-037

Conclusion

We have successfully analyzed the all discussed consensus methods. Although, there is no clear winner for permanent use as everyone has their own benefits and limitations. Some can be good in term of resource usage and some are good in term of throughput. So choice of consensus will be depending on the scenarios one want to deal with. But if we have to generalized one as best so we can say the most popular one use like DPOS and PBFT can be used but they also have their limitations. For future these consensus methods can be implemented for one problem and them a detailed implementation based analysis can be produced.

References

1. S. Gilbert and N. Lynch, "Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services", *ACM SIGACT News*, vol. 33, no. 2, pp. 51-59, 2002.
2. S. SHARMA, A. BAHGA, T. SHARMA and R. KRISHNA, "Time-Efficient Auditable Blockchain-based Pharma Drug Supply Chain using Delegated Proof-of-Stake", in *International Conference on Emerging Technologies: AI, IoT and CPS for Science & Technology Applications (ICET 2021)*, VIRTUAL MODE, 2021.
3. "EOSIO/Documentation", GitHub, 2021. URL: https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md.
4. R. Raj, N. Rai and S. Agarwal, "Anticounterfeiting in Pharmacy Supply Chain by establishing Proof of Ownership", IEEE Region 10 Conference (TENCON), Kochi, India, 2019, pp. 1572- 1577.
5. "Hyperledger Fabric – Hyperledger", Hyperledger, 2021. URL: https://www.hyperledger.org/use/fabric.
6. S. Aggarwal and N. Kumar, "Cryptographic consensus mechanisms", *Advances in Computers, Elsevier*, vol. 121, pp. 211-226, 2021.
7. Shijie Zhang, Jong-Hyouk Lee. "Analysis of the main consensus protocols of blockchain" , ICT Express, 2020.
8. David A. Cook and Udo W. Pooch, "Accelerated time discrete event simulation in a distributed environment", International Journal of Systems Science, 1993.