International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue II, Feb 2019- Available at www.ijraset.com

An Analysis of Consensus Algorithms for the Blockchain Technology

Deven A. Gol[1]
[1]*Department of Information Technology, G H Patel College of Engineering and Technology, Anand-388320, Gujrat*

Abstract: ***Cryptocurrencies have seen a massive surge in popularity and behind these new virtual currencies is an innovative technology called the block chain: a distributed digital ledger in which cryptocurrency transactions are recorded after having been verified.***
The transactions within a ledger are verified by multiple clients or "validators," within the cryptocurrency's peer-to-peer network using one of many varied consensus algorithms for resolving the problem of reliability in a network involving multiple unreliable nodes.
The most widely used consensus algorithms are the Proof of Work (PoW) algorithm and the Proof of Stake (PoS) algorithm; however, there are also other consensus algorithms which utilize alternative implementations of PoW and PoS, as well as other hybrid implementations and some altogether new consensus strategies.
In this paper, we perform a comparative analysis of typical consensus algorithms and some of their contemporaries that are currently in use in modern blockchains. Our analysis focuses on the algorithmic steps taken by each consensus algorithm, the scalability of the algorithm, the method the algorithm rewards validators for their time spent verifying blocks, and the security risks present within the algorithm. Finally, we present our conclusion and some possible future trends for consensus algorithms used in block chains.
Keywords: Block Chain, POW, POS, PBFT, POET etc.

I. INTRODUCTION

A blockchain is associate open, distributed ledger that may record transactions between 2 parties expeditiously and during a permanent, verifiable manner [1]. the foremost notable implementation of 1 being Bitcoin's, created in 2008 by an individual or cluster operating underneath the anonym "Satoshi Nakamoto" [2].
In keeping with the first Bitcoin whitepaper, the goal of this new technology was to modify the creation of a "peer-to-peer version of electronic money [which] would permit on-line payments to be sent directly from one party to a different while not researching an institution." In Bitcoin's implementation, this is often achieved by timestamping each dealing inside aforesaid peer-to-peer (P2P) network associated hashing them into an ever-growing chain of dealing blocks.
This hashing is accomplished by validators (i.e., "miners") that area unit peers within the network that participate within the creation of recent blocks [3].
Forward no individual or cluster of validators controls over twenty fifth of the computing power wont to hash these blocks, all transactions inside the chain area unit trustworthy as valid.
As there will be a probably unlimited range of validators in any given P2P network, agreement algorithms should be used for there to be any cooperation between them.
The foremost wide adopted of those is that the Proof of work (POW) algorithmic program enforced by Bitcoin; but, there are a unit various different suggests that by that a network will achieve agreement, like the algorithms which will be overviewed additional during this paper.
This paper is organized as follows: first, downside of reaching agreement during a distributed system is explained briefly. Afterwards, the agreement systems utilized by the highest cryptocurrencies (ranked by current market share) is overviewed. The various algorithmic programs area unit compared with the Proof of work algorithm in terms of measurability and energy potency. [10] Theoretical systems that propose interesting solutions to current agreement issues area unit mentioned and evaluated supported their feasibilities in terms of implementation.
Finally, the restrictions of the analysis conducted inside this paper area unit mentioned and avenues for additional analysis area unit provided.

II. THE CONSENSUS ALGORITHMS

Blockchain consensus models are methods to create uniformity and fairness in the current era of digital world. The consensus systems used for this agreement is called a consensus theorem.
These Blockchain consensus models consist of some particular objectives, such as: [24]

A. Coming to an agreement: The mechanism gathers all the agreements from the group as much as it can.
B. Collaboration: Every one of the group aims toward a better agreement that results in the groups' interests as a whole.
C. Co-operation: Every individual will work as a team and put their own interests aside.
D. Equal Rights: Every single participant has the same value in voting. This means that every person's vote is important.
E. Participation: Everyone inside the network needs to participate in the voting. No one will be left out or can stay out without a vote.
F. Activity: every member of the group is equally active. There is no one with more responsibility in the group.

III. DIFFERENT TYPES OF CONSENSUS ALGORITHMS ARE EXPLAINED AS PER BELOW

A. Proof Of Work

Proof of work is the first Blockchain calculations presented in the blockchain organize. Numerous blockchain Technologies utilizes this Blockchain accord models to affirm the majority of their exchanges and produce applicable squares to the system chain. The decentralization record framework gathers all the data identified with the squares. Anyway one needs to take extraordinary consideration of the considerable number of exchanges squares. [1] This duty falls upon all the individual hubs called mineworkers and the procedure they use to keep up it is called mining. The focal guideline behind this innovation is to take care of complex numerical issues and effectively give out arrangements. These numerical issues require a great deal of computational power, in the first place. For instance, Hash Function or realizing how to discover the yield without the info. Another is that whole number factorization, and it additionally covers visit confounds.
This happens when the server feels like it has a DDoS assault and to discover it out the accord frameworks requires a great deal of count. It's the place the diggers proved to be useful. The response to the entire issue with the scientific condition is known as the hash. Anyway proof of work has certain confinements. The system appears to grow a great deal, and with this, it needs loads of computational power. This procedure is expanding the general affectability of the framework. [14]

B. Proof Of Stake

Proof of stake is an accord calculation blockchain that bargains with the principle disadvantages of the confirmation of work calculation. In this one, each square gets approved before the system adds another square to the blockchain record. There is a tad of Twist in this one. Mineworkers can join the mining procedure utilizing their coins to stake. The Proof of stake is another sort of idea where each individual can mine or even approve new squares just dependent on their coin ownership. Along these lines, in this situation the more coins you have, the better your odds are. In this agreement calculation, the minors get recently picked. In spite of the fact that the procedure is totally arbitrary, still only one out of every odd minor can take an interest in the staking. Every one of the diggers of the system are arbitrarily picked. In the event that you have a particular measure of coins put away already in your wallet, at that point you will be fit the bill to be a hub on the system. In the wake of being a hub, on the off chance that you need to be fit the bill for being a digger you should store a specific measure of coin, after that there will be a casting a ballot framework for picking the validators. At the point when it's everything done, the mineworkers will stake the base sum required for the unique wallet staking. The procedure is very straightforward truly. New squares will get made corresponding to the quantity of coins' dependent on the wallet. For instance, on the off chance that you possess 10% of the considerable number of coins, at that point you get the chance to mine 10% new squares. There are numerous blockchain advances that utilization an assortment of Proof of stake accord calculation. In any case, the majority of the calculations work the equivalent for mining new obstructs each mineworker will get a square reward just as an offer of the exchange expenses.

C. Practical Byzantine Fault Tolerance (PBFT)

PBFT primarily focuses on the state machine. It replicates the system however gets eliminate the most Byzantine general drawback. Well, the formula assumes from the beginning that there may well be attainable failures within the network and a few freelance nodes will malfunction at bound times. The formula is intended for asynchronous agreement systems Associate in Nursingd more optimized in an economical thanks to manage all the matter. Moreover, all the nodes within the system gets organized in a very

specific order. One node is chosen because the primary one, et al. work because the backup set up. However, all the nodes within the system add harmony and communicate with each other. The communication level is pretty high as a result of they require to verify each data found on the network. This gets eliminate the unreliable data drawback. However, with this new method, they're able to conclude if even one in every of the node gets compromised. All of the nodes reach Associate in nursing agreement through majority selection.

D. Simplified Byzantine Fault Tolerance (SBFT)

In SBFT, the system works in other way. First, a block generator can collect all the group action at a time and validate them when batching them along in a very new form of block. In easy terms, a block can gather all the transactions, batch them consequently into another block then finally validate all of them along. The generator applies bound rules that everyone the nodes follow to validate all the transactions. After that, a block signer can validate them and add their terribly own signature. That's why if any of the blocks miss even one in every of the keys then it'll get rejected.

E. Delegated Byzantine Fault Tolerance (DBFT)

There is no dialogue on the actual fact that Proof-of-Work and Proof-of-Stake are the foremost wide known agreement algorithms. Whereas plenty of the blockchain scheme follows these 2 common algorithms, some are attempting to impose newer and a lot of advanced agreement systems. Among these pioneer blockchain brands, NEO's name is certain to return. With the thriving growth within the last twelve months, modern is currently the flapjack within the business. The Chinese complete has shown quite the potential. And why wouldn't they? They're the artificer of the advanced agreement theorem – Delegated Byzantine Fault Tolerance (dBFT). [24]

F. Proof-Of-Activity

While individuals were debating the subject – Proof-of-Work vs. Proof-of-Stake, the creator of Litecoin.

Thus, the concept of a desirable hybrid came to the globe – Proof-of-Activity. It combines the simplest 2 options – additional secured against any attack and not a not power-hungry system.

G. Proof-Of-Importance

The Proof-of-Importance blockchain agreement protocol example came to be as a result of the far-famed name of NEM. The thought could be a development of the Proof-of-Stake. Although, NEM introduced a replacement plan – gather or vesting. The gather mechanism determines whether or not a node is eligible to be side to the blockchain or not. The additional you harvest on a node; the additional probabilities it gets to be side on the chain. Reciprocally for the gather, the node receives the dealing fees that the validator collects because the reward. It solves out the most important downside of Proof-of-Stake. In PoS, the richer gets cash extra money more cash compared to the validators having less money. For instance, if you own two hundredth of the cryptocurrency, you'll be able to mine two hundredth of all the blocks on the blockchain network. [24]

H. Proof-Of-Capacity

Proof-of-Capacity accord example is associate degree upgrade of the noted Proof-of-Work blockchain accord protocol. The essential characteristic of this one is that the "plotting" feature. You may need to devote your process power and disk drive storage even before you're commencing to mine. This terribly nature makes the system quicker the captive. The Proof-of-Capacity will produce a block in only four minutes whereas the Proof-of-Work takes 10 minutes to try and do constant. Moreover, it tries to tackle the hashing drawback of the captive system. A lot of solutions or plots you have got on your pc, the higher your likelihood is that to win the mining battle.

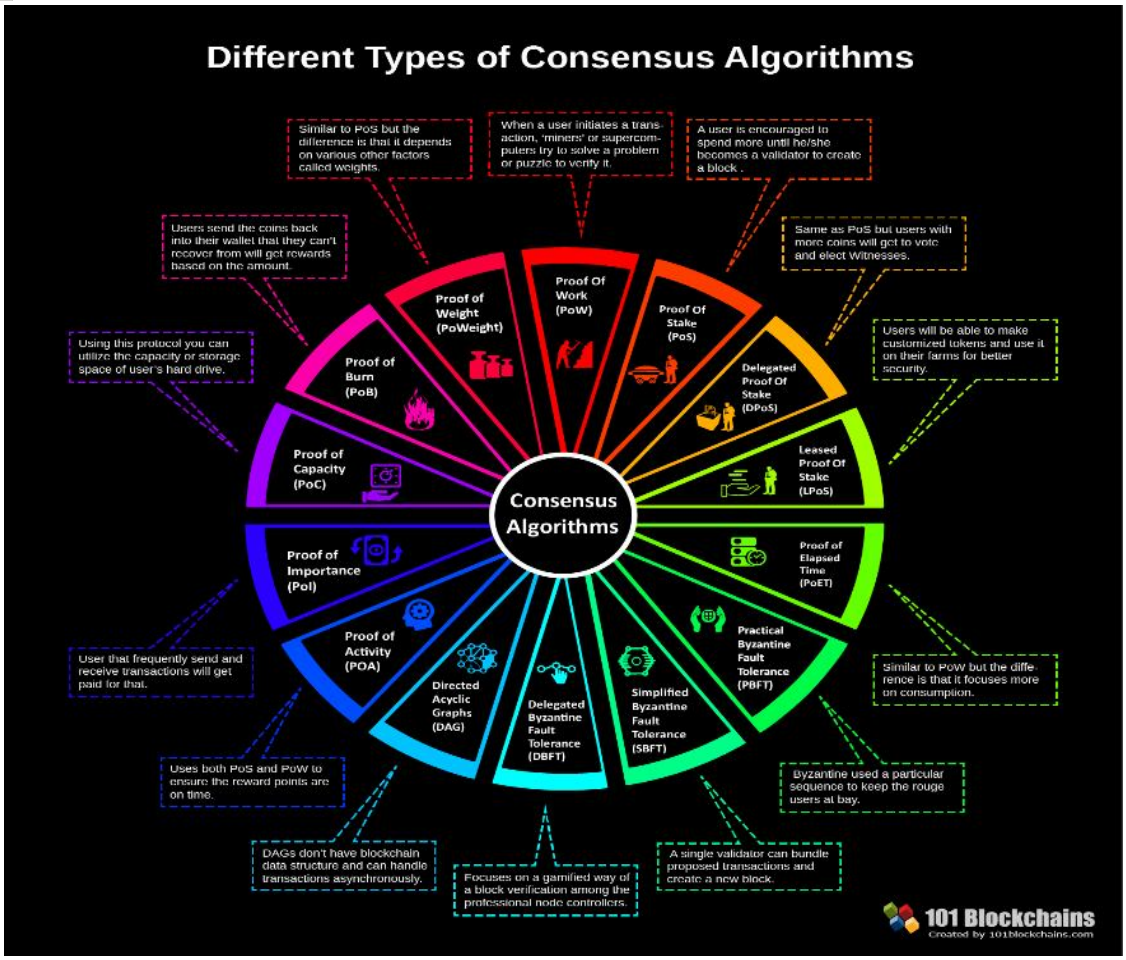

Fig 1: consensus Algorithm [24]

I. Proof-Of-Burn

This accord sequence is kind of spectacular. To safeguard the prisoner of war cryptocurrency, a little of the coins are burnt! The method happens because the miners send many coins to AN "Eater Address." The Eater Addresses cannot pay these coins on any purpose. [4] A ledger keeps track of the burnt coins creating them genuinely UN spendable. The user World Health Organization burnt the coins can get an award in addition. Yes, the burning may be a loss. However, the injury is temporary because the method can safeguard the coins within the long-standing time from the hackers and their cyber-attacks. Moreover, the burning method will increase the stakes of the choice coins. Such a situation will increase the possibility of a user to mine consecutive block in addition as will increase their rewards within the future. So, burning might be used as a mining privilege. The counterparty is a wonderful accord example of a cryptocurrency that uses this blockchain accord protocol.

J. Proof-Of-Weight

Proof-of-Weight blockchain agreement protocol is on the last position of our list of agreement algorithms. This can be an enormous upgrade of the Proof-of-Stake algorithmic rule. In Proof-of-Stake, the additional token you own, the higher your likelihood is to get more! This idea makes the system a touch biased.

Well, the Proof-of-Weight tries to resolve such biased nature of the PoS. Cryptocurrencies like Algorand, File coin, and Chia implement the PoW. The Proof-of-Weight considers another factors than owning additional tokens like in PoS. These factors get known because the "Weighted Factors." as an example, File coin considers the quantity of IPFS information that you just have and weights that issue. a number of the opposite factors embrace however not limit to Proof-of-Space-time and Proof-of-Reputation. The fundamental blessings of this method embrace customization and quantifiability. Though incentivizing may be an enormous challenge for this agreement algorithmic rule.

K. Proof Of Elapsed Time (Poet)

PoET is one in every of the most effective accord algorithms. This explicit algorithmic program is employed chiefly on permissioned blockchain network wherever you'll have to be compelled to get permission for accessing the network. These permissions networks got to choose the mining rights or balloting principles. To make positive that everything runs swimmingly the writer algorithms uses a selected maneuver for covering transparency into the total network. The accord algorithms additionally guarantee a secure login into the system, because the network needs identification before connection the miners. Needless to mention, this accord algorithmic program offers an opportunity to select the winner's mistreatment truthful means that solely. [2] Every individual on the network has got to look ahead to associate degree quantity of time; but, the point in time is completely random. The participant WHO has finished his/her justifiable share of waiting time can get to get on the ledger to make a replacement block. To justify these eventualities, the algorithmic program has got to contemplate 2 facts. Whether the winner truly selected the random range within the initial place? He or She might select a random short time and obtain the win initial. Did the individual extremely wait the particular time he/she were assigned? PoET depends on a special computer hardware demand. It's referred to as Intel package Guard Extension. This package Guard Extension helps to run distinctive codes at intervals the network. Writer uses this technique and makes positive the winning is solely truthful.

L. Leased Proof-Of-Stake (LPOS)

Another twist to the classic Proof of Stake is that the Leases proof of stake. The new agreement algorithmic rule blockchain was introduced to America by Waves platform. Similar to the other blockchain technology platform, waves additionally ensures to supply a stronger catch with a restricted quantity of power consumption. The original proof of stake had some limitations for staking. People with a restricted quantity of coins may never really participate within the staking ever. To keep up the network with success, solely some of a private with additional coins to supply is left behind. This method permits the system to form a centralized community among a decentralized platform, that is outwardly not the specified one.[5] In Leases proof of stake, the smallholders will finally get their likelihood of staking. They'll lease their coins to the network and take the have the benefit of there. After the introduction to the new Leases Proof of Stake, matters modified fully. the constraints of the previous system will currently get solved with none hassles. The most purpose of Waves platform was to assist out tiny time investors. People with a little range of coins in their case would ne'er get an opportunity to induce the advantages just like the huge fishes. This manner it all establishes the most theme of the agreement algorithms – transparency.

M. Directed Acyclic Graphs (DAG)

A lot of crypto-experts acknowledge Bitcoin because the blockchain 1.0 and Ethereum because the blockchain 2.0. However, these days, we tend to square measure seeing a replacement player within the market with even additional fashionable technology. Some also are locution that it's the blockchain 3.0. Whereas loads of contender's square measure fighting to urge the title of blockchain 3.0, NXT goes to be before the sport with the appliance of Directed Acyclic Graphs conjointly called the DAG. Except NXT, IOTA and IoT Chain conjointly adopts DAG to their system.

IV. CONCLUSION

It is that the agreement algorithms that build the character of the blockchain networks therefore versatile. [4] Yes, there's not one agreement algorithmic rule blockchain that may claim it to be excellent. However, that's the wonder of the technology we tend to guess – the constant modification for betterment. If these agreement algorithms weren't there, we'd still have to be compelled to depend upon the Proof-of-Work. Whether or not you prefer it or not, the POW quite threatens the decentralization and distributed nature of the blockchains. The whole plan of the blockchain technology is decentralization and a fight against the autarchy. It's time the people place a stop to the corrupted and faulty system. So all these algorithms work as per need by miners.

REFERENCES

[1] Iansiti and K. Lakhani, "The Truth About Blockchain", Harvard Business Review, 2018. [Online]. Available: https://hbr.org/2017/01/the-truth-about-blockchain. [Accessed: 04- Feb-2018].
[2] S. Nakamoto, "Bitcoin: A Peer-to-peer Electronic Cash System," 2008.
[3] G. Karame, E. Androulaki, Bitcoin and Blockchain Security, Norwood, MA: Artech House, 2016.
[4] L. Lamport, R. Shostak and M. Pease, "The Byzantine Generals Problem," ACM Transactions on Programming Languages and Systems, vol. 4, no. 3, pp. 382-401, 1982.
[5] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance and Proactive Recovery," ACM Transactions on Computer Systems, vol. 20, no. 4, pp. 398-461, 2002.

[6] M. Correia, G. Veronese and L. Lung, "Asynchronous Byzantine consensus with 2f+1 processes," Proc. 2010 ACM Symposium on Applied Computing - SAC '10, 2010.
[7] NEO White Paper. (2014). Available: http://docs.neo.org/en-us/.
[8] S. David, Y. Noah, B. Arthur, The Ripple Protocol Consensus Algorithm, Ripple Labs Inc, 2014.
[9] S. King, S. Nadal, "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake,"2012.
[10] P. Vasin, "BlackCoin's Proof-of-Stake Protocol v2," Blackcoin.co, 2016.
[11] Kiayias, A. Russell, B. David and R. Oliynykov, "Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol", Advances in Cryptology – CRYPTO 2017, pp. 357-388, 2017.
[12] D. Mazieres, "The Stellar Consensus Protocol: A Federated Model for Internet-Level Consensus," draft, Stellar Development Foundation, 2016.
[13] L.S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), 2017.
[14] D. Larimer, "DPOS Consensus Algorithm – The Missing Whitepaper," Steemit, 2018.
[15] EOS.IO Technical White Paper. Github. (2017).
[16] NEM Technical Reference, Version 1.2. 2018.
[17] Z. Theng, S.Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, , IEEE, pp. 557-564, 2017.
[18] J. Rubin and J. Holliman, "Oor: Stellar Consensus Protocol Implementation", p. 2, 2015.
[19] Eyal and E. Sirer, "Majority Is Not Enough: Bitcoin Mining Is Vulnerable", Financial Cryptography and Data Security, pp. 436- 454, 2014.
[20] Stellar Basics. "Ready for Faster, Cheaper Transactions?", Stellar Development Foundation.
[21] Raul. "Transactions Speeds: How Do Cryptocurrencies Stack Up To Visa or Paypal?", howmuch, 2018. [Online]. Available: https://howmuch.net/articles/crypto-transaction-speeds-compared. [Accessed: 13-Feb-2018].
[22] Bitcoin Energy Consumption Index. Digiconomist. (2018).
[23] https://www.newgenapps.com/blog/8-blockchain-consensus-mechanisms-and-benefits
[24] https://101blockchains.com/consensus-algorithms-blockchain/.