iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VII **Month of publication:** July 2021

DOI: https://doi.org/10.22214/ijraset.2021.36425

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VII July 2021- Available at www.ijraset.com

Comparative Study of Proof of Work (PoW) and Delegated Proof of Stake (DPoS) Blockchain Consensus Algorithm

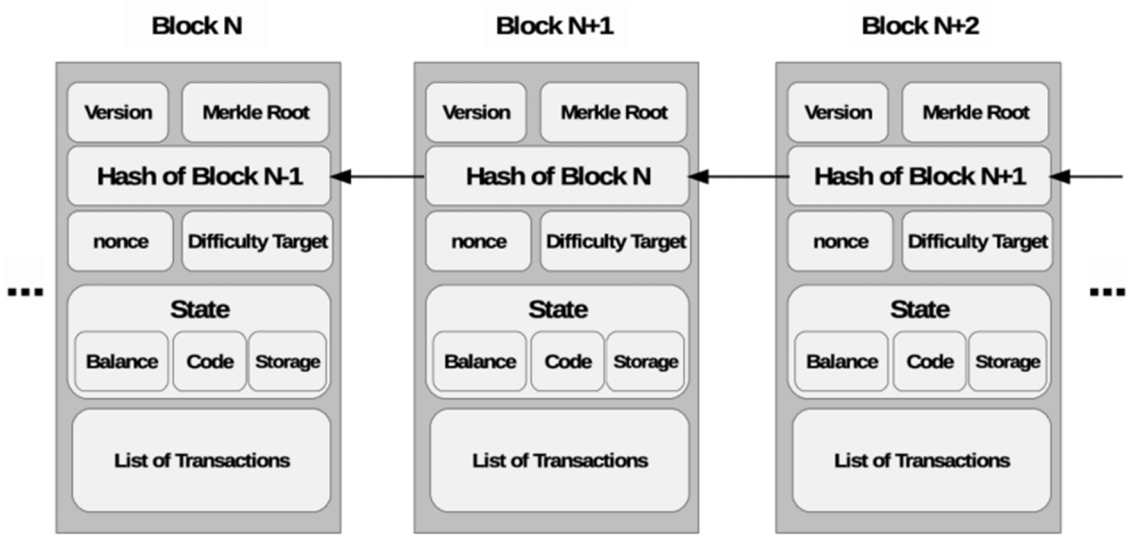
Nithish Kumar R
Electronics and Instrumentation Engineering Department, MIT Campus, Anna University, Chennai, India

Abstract: ***As opposed to the current system, that is controlled by a central authority, blockchain was invented by Satoshi Nakamoto in 2008 as a distributed ledger system. A major development in the technology came with the introduction of virtual cryptocurrencies where transactions were recorded and verified by miners or validators at various nodes in different locations. Since these transaction records are available to everyone, this solved the current problem of excessive double spending. In a decentralized system like blockchain, a reliable mechanism was necessary to verify the integrity of all transactions. This led to the introduction of a variety of consensus mechanisms. This paper presents the results of a comparative study between Proof of Work and Delegated Proof of Stake, both of which have been widely used in Blockchain projects recently. Based on the above, this study will primarily discuss a brief explanation of the workings of both algorithms, comparisons between them, and various factors impacting these algorithms from a crypto currency standpoint.***

Index Terms: Proof of Work (PoW), Delegated Proof of Stake (DPoS), Algorithm, Cryptocurrency, Bitcoin

I. BLOCKCHAIN INTRODUCTION

The blockchain is an ever-growing list of data consisting of transaction details or smart contracts, depending on the need. All the data in the blockchain are stored inside the blocks which is protected by the SHA256 cryptographic hashing. The blocks are made up of the index number, block data, hash of the block, and the previous block's hash, allowing them to connect and form a chain. Blockchain operates in a distributed peer-to-peer network, where every node in the network contains the same copy of the blockchain, and when a block is added to the chain it will be updated in every node, this acts as one of the biggest advantages of blockchain technology. In the event that a third party attempts to make changes to the chain or add a malicious block, the p2p network rejects the change thus making the whole system an immutable ledger. Blockchain, by virtue of being decentralized, prevents single points of failure, which is a problem associated with centralized databases.



©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VII July 2021- Available at www.ijraset.com

II. CRYPTOCURRENCY INTRODUCTION

One of the most popular implementations of blockchain is cryptocurrency, a digital currency in which every transaction is stored inside the block and is publicly available. Bitcoin is currently the most valued cryptocurrency, In the wake of bitcoin's success, multiple cryptocurrencies were introduced to the market through ICOs. In the case of bitcoins, the details about each transaction are stored inside the block, which the miners then add to the blockchain. Miners mine each block by solving complicated mathematical problems and if they are successful, they will be allowed to add the data into the blocks and for mining each block the system rewards them with the cryptocurrency.

III. CONSENSUS MECHANISM

The blockchain system is vulnerable to Byzantine Fault, thus the system was introduced to a number of consensus algorithms that are byzantine fault tolerant. Consensus algorithm is defined as the process of agreeing on a single value for a piece of data among processes or systems distributed across a network. There are multiple consensus algorithms present There is no one consensus mechanism that can be used by all blockchain networks because different outcomes need to be obtained for different applications. A variety of consensus algorithms are available to be used, such as Proof of work (PoW), Proof of stake (PoS), Proof of capacity (PoC), Delegated Proof of stake (DPoS), Practical Byzantine Fault Tolerance (PBFT), etc. Cryptocurrencies like Bitcoin and Litecoin typically use the Proof of Work (PoW) consensus mechanism as it is the most commonly used consensus algorithm.

IV. PROOF OF WORK

A proof of work (PoW) is a cryptographic proof in which the prover (one party) proves to the verifiers (another party) that then amount of computational effort has been expended. Proof of work was the original consensus algorithm implemented in the blockchain network when it was created by Satoshi Nakamoto. In order to confirm transactions and produce new blocks in the chain, proof of work is required. The process of PoW is based on miners competing against each other to complete transactions on the network. An open network exchanges digital tokens between its members. Unlike centralized ledgers, decentralized ledgers gather all transactions into blocks, which are handled by special nodes called miners. For mining a block, miners need to solve a mathematical equation or problem that requires a large amount of computing power. The PoW problem or mathematical equation has an answer called hash. Due to the network's increasing size, it faces increasingly complicated problems. As algorithms become more complex, they require a greater amount of computational power

V. DELEGATED PROOF OF STAKE (DPOS)

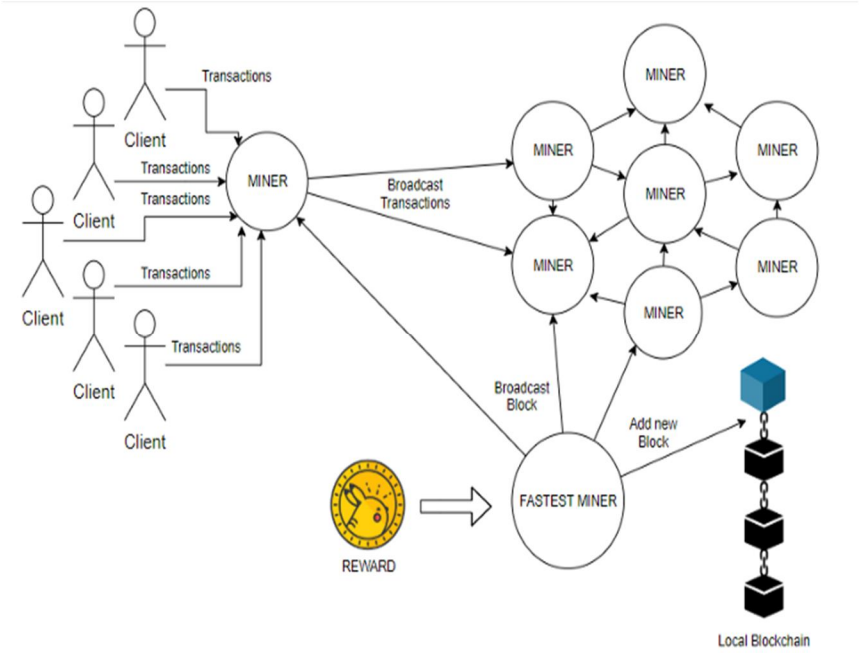
A delegated Proof-of-Stake consensus method was proposed by Daniel Larimer in 2014 to replace the Proof-Of-Work algorithm that Bitcoin and most other crypto currencies used at the time. Delegated Proof of stake (DPoS) is viewed as a democratic consensus algorithm. Block producers are selected by shareholders, and then they are tasked with verifying transactions and producing blocks. Voted delegates determine the fees that these witnesses receive through the transactions. This voting system allows the shareholders with the most coins to have the most votes, since every share has one vote. The voter can replace a delegate if they believe the delegate has been malicious.

VI. PROOF OF WORK (POW) WORKING

Proof of work is a document that is difficult to produce but easy for others to verify and which meets certain requirements. It is often necessary to perform a lot of trial and error before a valid proof of work can be generated because producing a proof of work is a random process with low probability. As a general rule of thumb, the miners are required to invest a large amount of computational power in finding a hash string that matches a set of constraints. In the case of Bitcoin then miners are supposed to identify a hash with a particular number of leading zeros, in the beginning, the number of leading zeros determine the difficulty of the block, and the difficulty of the block is constantly modified to limit the number of blocks found in a particular amount of time. By repeatedly changing a number call nonce, a miner can find the valid hash. Nonce is an integer value with 32 bits of memory with a range of 4 billion values. The miner will increment each nonce looking for the valid hash and the number of hashes the miner can check in a second is known as hashing power. In a PoW system, every single miner in the network will run the same algorithm to find the same block at the same time. Thus, this creates a competitive environment, and the miner who discovers the valid hash will be rewarded by the system, and then the miner can validate and submit transactions to be added to the block. Following this, the block will be added to the blockchain and the chain will be updated in each node present in the network.

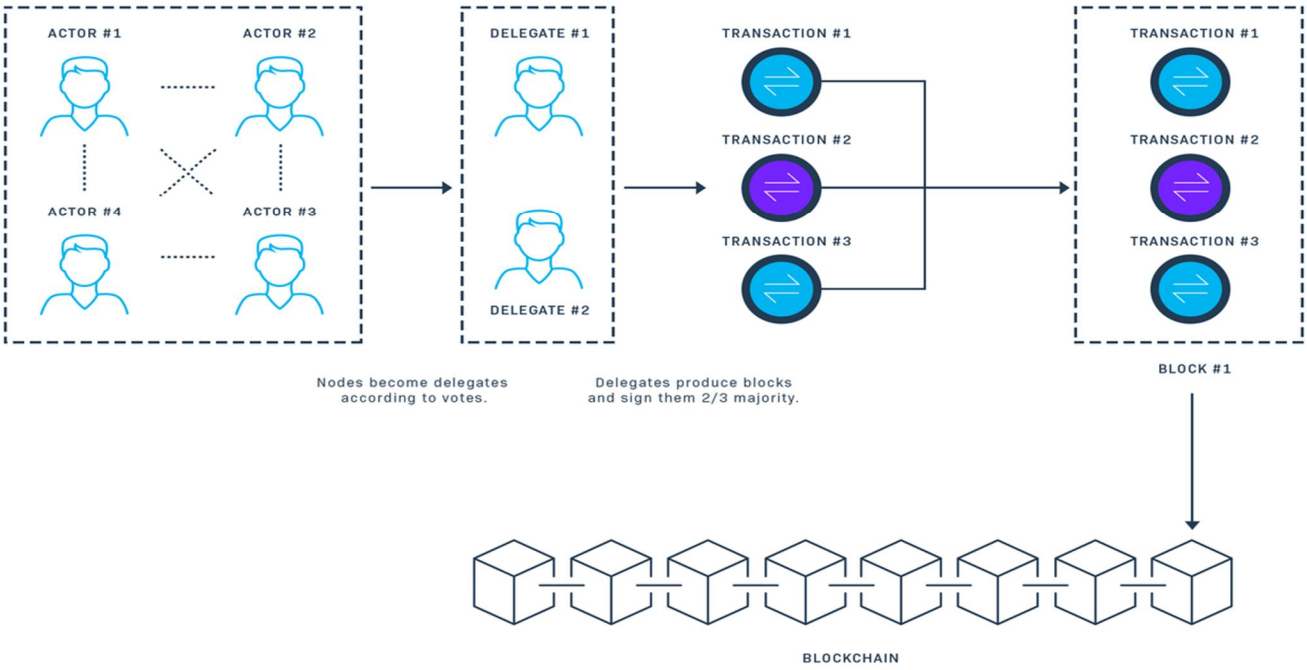
©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VII July 2021- Available at www.ijraset.com



VII. DELEGATED PROOF OF STAKE (DPOS) WORKING

DPoS allows users to vote on delegates by pooling their tokens into a staking pool and linking them to a specific delegate. Tokens are not physically moved to another wallet, but instead staked in staking pools through staking service providers. The block producers in this case are voted into power by the users of the network, who each get a certain number of votes based on how many tokens they own on the network. Delegates from the previous block may not automatically become delegates of the next, as only a limited number of delegates are selected for each block. The delegates elected by the network receive the transaction fees from the validated block, and that reward is then split with all the users who contributed tokens to the pool of the successful delegates. Stakes are based on the amount staked, and the more the users stake, the more shares they receive. Blocks are considered final when voted on by 2/3+1 of the block producers, if not, the longest chain rule is applied.



©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VII July 2021- Available at www.ijraset.com

VIII. COMPARISON

A. *Proof Of Work*

1) *Proof of Work (POW):* In Proof of work, miners try to find the valid hash with the help of powerful computational devices with high hashing power. The miner with the highest hash power is likely to find the valid hash more likely than every other miner since they are competing at the same time for the same blocks. This can cause the system to favor those with high capital for investment.
2) *Delegated Proof of Stake (DPOS):* Delegated Proof of Stake allows block producers to take turns producing blocks, each of them having a scheduled time slot when they are allowed to do so. The block producers and other peers are all informed about the production schedule. As transactions and votes are broadcasted, the block producer collects them into blocks. The creation of blocks is limited to one at a time, rather than multiple peers simultaneously.

B. *Energy Consumption*

3) *Proof of Work (POW):* This process involves a large number of miners using very powerful computing devices to mine the same block at the same time, which consumes a huge amount of energy across the world. The increasing difficulty of finding the new block also contributes to the inefficiency of the entire mining process.
4) *Proof of Work (POW):* In contrast to proof of work, delegated proof of stake operates on a schedule for each delegate to verify and add the block to the chain, this results in low energy consumption, thus making the system energy efficient.

C. *Speed*

1) *Proof of Work (POW):* Bitcoin is currently one of the biggest users of the proof of work algorithm, and currently, it takes around 10 minutes to mine a block, a delay caused by the algorithm's increasing difficulty. The slow speed also contributes to the high energy consumption of bitcoin mining.
2) *Delegated Proof of Work (DPOW):* With proper ordering of block producers waiting for their turn to mine a block, delegated proof of stake enables faster processing of transactions than proof of work. It takes approximately 3 seconds for a new block to be created in TRON, one of the cryptocurrencies using DPoS.

D. *Cost*

1) *Proof of Work (POW):* Proof of Work on bitcoin requires a powerful set of computational devices to mine a block. Mining was done using GPUs (graphics processing units) which became quite slow when difficulty increased over time, and the use of Application Specific Integrated Circuits (ASIC) improved this by making mining faster than CPUs, but in return increased the average cost of mining by folds, making small scale mining unprofitable.
2) *Delegated Proof of Work (DPOW):* Due to the low amount of Block Producers in the Delegated Proof of Stake system, there is no need for any competition among the block producers, therefore removing the need for any expensive computing devices. The result of this is a lower cost compared to other consensus algorithms.

E. *Reward System*

1) *Proof of Work (POW):* Proof of work systems encourage miners across the world to compete against each other to find the next block, and the miner who finds the block is rewarded for his work. Over time, the reward amount decreases as more blocks are mined.
2) *Delegated Proof of Work (DPOW):* In a Delegated Proof of stake System, the voters stake their coin and elect their block producer and the block producer is incentivized after adding a new block to the chain, in order to maintain the block producer, position the voters are compensated a particular amount of money decided by the block producer. If in any case, the block producer stops compensating the voter they can easily remove the Block producer from the position by voting for another delegate.

©IJRASET: All Rights are Reserved

F. Decentralization

1) *Proof of Work (POW):* The Proof of Work algorithm in Bitcoin was previously considered to be the most decentralized system because it gave everyone the chance to be a miner, but as more miners with large capital have been investing in mining farms, the probability is rising that the Proof of Work algorithm will favor centralized entities. There are currently about 12 bitcoin mining pools dominating the industry.
2) *Delegated Proof of Work (DPOW):* DPoS cannot be described as decentralized as PoW since it allows only a few people to create the blocks at a given time. Meanwhile, DPoS prevents the system from being manipulated by substantial miners, because the other voters could remove the person who staked the biggest amount and gained the key position.

G. Vulnerabilities

1) *Proof of Work (POW):* The proof of work algorithm is vulnerable to 51% attack, it is a scenario where a miner controls 51% of the total mining power in which case the miner can control the entire network decision. It is theoretically possible, however the cost involved in acquiring 51% mining power is too high in comparison to the amount of money a miner could gain from the process, making it practically inefficient.
2) *Delegated Proof of Work (DPOW):* There is a risk of Cartel formation in the delegated proof of stake system where a number of block producers join together and create a cartel that controls the network's overall block production system. Another scenario is when a lack of participation by the coin holders in the voting process, which can result in only a few people voting for the Block producers. This can generate a 51% attack.

H. Applications

1) *Proof of Work (POW):* The Proof of work algorithm is used by some of the most valuable cryptocurrencies like Bitcoin, Ethereum, Litecoin, Monero, etc.
2) *Delegated Proof of Work (DPOW):* The Delegated Proof of Work is used by EOS, TRON, Tezos, Lisk etc.

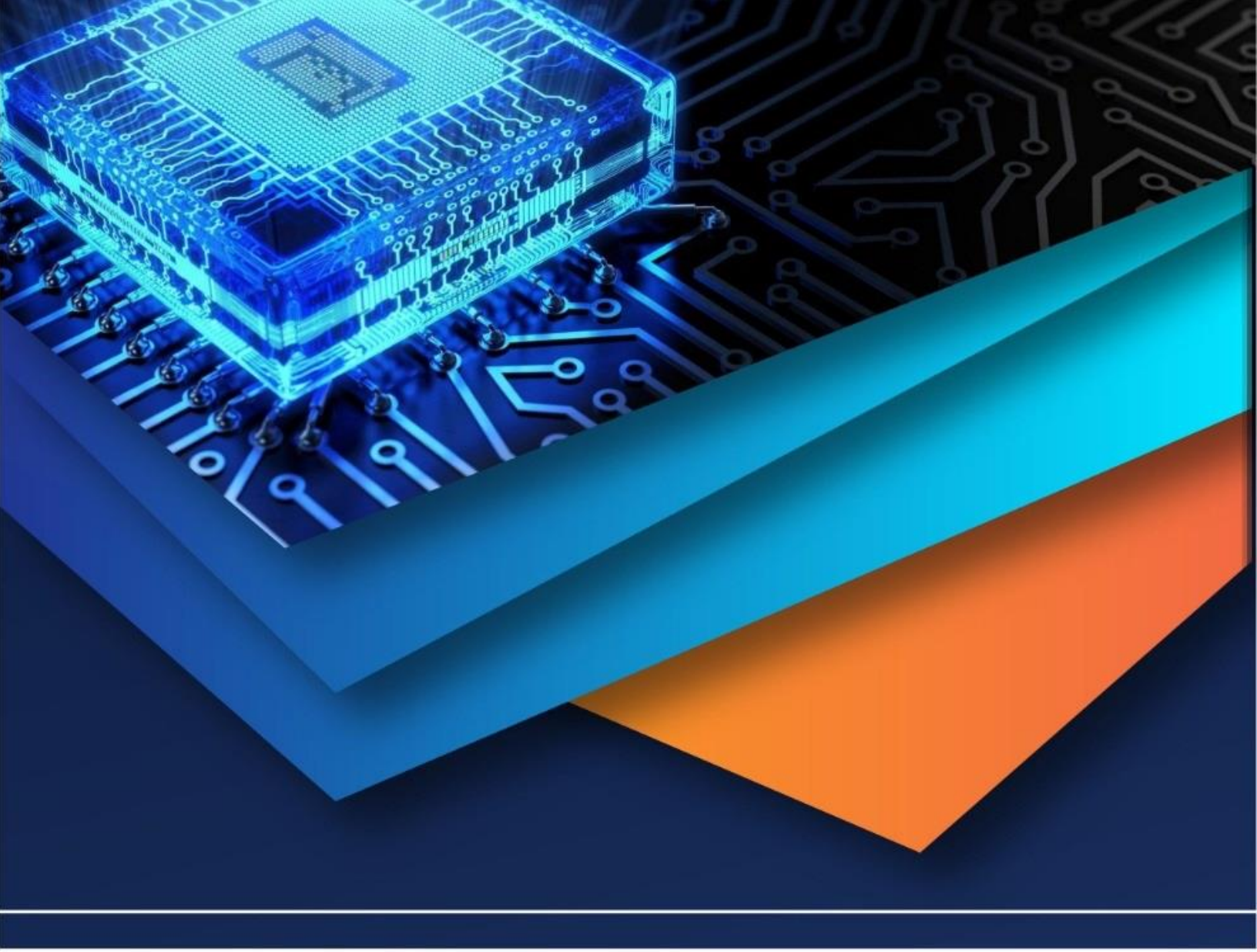
IX. CONCLUSION

While the PoW algorithm was the first implementation of a consensus algorithm on a blockchain network, the change of time has resulted in the need for modified consensus algorithms like DPoS and PoS There is a constant risk of forking in the Blockchain network due to two groups of nodes having a disagreement, which causes the chain to split into two separate chains. This is why an algorithm like DPoS is necessary. Consequently, the chain becomes unstable, which can lead to fewer people investing in it. DPoS systems are typically better because of their finality, in which the chain generated is the final chain and no further forking of the chain is permitted. However, DPoS is not considered a completely decentralized network, whereas PoW is. Due to its low energy consumption, DPoS is gaining popularity. However, PoW's energy consumption rate is increasing exponentially, which poses a serious environmental concern. Although neither algorithm is considered perfect, each has its advantages and disadvantages, and the PoW algorithm is considered the most secure and thus the perfect choice for high-value cryptocurrencies. A DPoS algorithm, on the other hand, is known for its high speed and scalability, making it a perfect candidate for developing decentralized applications (DApps). The development of Web 3.0 will rely heavily on both of these algorithms as people move toward decentralization in the future.

REFERENCES

[1] Andrew Tar, Jan 17, 2018, Proof-of-Work, Explained, https://cointelegraph.com/explained/proof-of-work-explained
[2] Blocktrades, 2020,The History of Delegated Proof-of-Stake (DPOS), Blocktrades, 2020. https://ecency.com/blockchain/@blocktrades/the-history-of-delegated-proof-of-stake-dpos
[3] Cryptopedia Staff, April 30, 2021,What Are Proof of Stake (PoS) and Delegated Proof of Stake (DPoS)?, https://www.gemini.com/cryptopedia/proof-of-stake-delegated-pos-dpos#section-delegated-proof-of-stake
[4] Binance, Nov 27,2018, Delegated Proof of Stake Explained, https://academy.binance.com/en/articles/delegated-proof-of-stake-explained
[5] Husneara Sheikh, Rahima Meer Azmathullah, Faiza Rizwan,Proof-of-Work Vs Proof-of-Stake: A Comparative Analysis and an Approach to Blockchain Consensus Mechanism, IJRASET, Volume 6 Issue XII, Dec 2018
[6] Kashish Khullar, Part 1: Implementing Blockchain and Cryptocurrency with PoW consensus algorithm, Oct 24,2018, https://medium.com/coinmonks/implementing-blockchain-and-cryptocurrency-with-pow-consensus-algorithm-part-1-545fb32be0c2
[7] Kirill Eremenko, How deoes Bitcoin/Blockchain Mining work?, May 3, 2018, https://medium.com/swlh/how-does-bitcoin-blockchain-mining-work-36db1c5cb55d
[8] Tokens 24, The Delegated Proof of Stake (DPOS) Explained, April 27, 2018, https://www.tokens24.com/cryptopedia/basics/delegated-proof-stake-dpos-explained
[9] Sivleen Kaur,Sheetal Chaturvedi,Aabha Sharma, Jayaprakash Kar, A Research Survey on Applications of Consensus Protocols in Blockchain, Volume 2021, Article ID 6693731, Jan 22, 2021, https://www.hindawi.com/journals/scn/2021/6693731/

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)