iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** XII **Month of publication:** December 2018

DOI:

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: 6.887
Volume 6 Issue XII, Dec 2018- Available at www.ijraset.com

Proof-of-Work Vs Proof-of-Stake: A Comparative Analysis and an Approach to Blockchain Consensus Mechanism

Husneara Sheikh[1], Rahima Meer Azmathullah[2], Faiza Rizwan[3]
Department of Computer Science, [1]Prince Sattam Bin Abdalaziz University

Abstract: Blockchain is a pioneering technology which has brought huge popularity for new virtual currencies where in transactions are recorded after being verified. The transactions are then verified by many clients or "validators," to solve the reliability issue among several nodes implemented in digital currency's peer-to-peer network. Though there are different alternate consensus algorithms available, the most commonly implemented algorithm are Proof of Work (PoW) algorithm and the Proof of Stake (PoS) algorithm. In this paper, we present a comparative study of distinctive consensus algorithms that are currently applied in modern blockchain. This analysis focus on the consensus mechanism, reward of the validator who invests time to mine or verifies the block, and the available security risks available within the algorithm. Also, we will discuss the difference in basic characteristics and cryptocurrencies used in an algorithm. Finally, we will conclude future trends for consensus algorithms used in blockchain.

Keywords: blockchain; PoW; consensus algorithms; cryptocurrency; DDoS

I. INTRODUCTION TO BLOCKCHAIN

The blockchain is a resourceful invention by Satoshi Nakamoto where the information keeping in the shared database which are easily verifiable and not specified to any single location. It is a decentralized technology and there is no way for the hacker to corrupt the information in any transaction connected to the process of identity verification.

Blockchain eliminates risks of data located centrally and has no single point of failure by various identical block across the network. Blockchain has been operable without failure since the invention of a cryptocurrency, Bitcoin, in 2008 on the basis of public and private “keys”. Satoshi Nakamoto has introduced *proof of work (PoW)* to build a distributed trustless consensus and resolve the double-spend problem. Blockchain technology is disrupting almost every industry for its improvement in efficiency and security.

There are two primary algorithms, PoW (Proof-of-work) and PoS (Proof-of-stake) through which Blockchain operates and are required to decide whether to invest in a cryptocurrency using some decisive factors. Some significant features to understand in Blockchain include speed, applications as well as the consensus algorithms. In this paper, we will compare to know about; PoW (Proof-of-work), POS (Proof-of-stake).

II. UNDERSTANDING PoW AND PoS CONSENSUS ALGORITHM

PoW: Proof-of-Work or PoW, is the original consensus algorithm in a Blockchain networks, where user sends a digital token to each other, verifies the transactions and create new blocks to the chain. In this algorithm, all miners or validators participate to validate and confirm the transactions carefully on the network to get rewarded. All the verified transactions in the network is collected into blocks by the distributed ledger and arranged accordingly.

This process is called mining. Proof of work is a protocol that prevents cyber threat as in distributed denial-of-service attack (DDoS) which intends to drain computer resources by sending numerous false requests.

A. How does PoW work?

The miner or validator has to perform complex mathematical calculation to find digital coins. The successfully verified transactions are then stored in the new block and thus create a new group of blocks in blockchain, a public distributed ledger. There are two important aspects of mining; one is to check the validity of a transaction, and another is to create new cryptocurrency mined by the rewarded validators for their previous work. The miner will be rewarded with new cryptocurrency if they resolve the task first and this way, it interests new more miners. Furthermore, the mining process enhances the network computing power and computation to make a coin to escalate, which makes the mining process for the coin more difficult and expensive for the single miner.

Following occurrences happen while creating a transaction:

1) All transactions are stored in a block.
2) Miners validate the transactions in each block.
3) Miners/validators resolve mathematical problem called proof-of-work
4) The miner/validator is rewarded as first winner who resolves transaction running in each block.
5) Finally, the public blockchain is created with validated transactions.

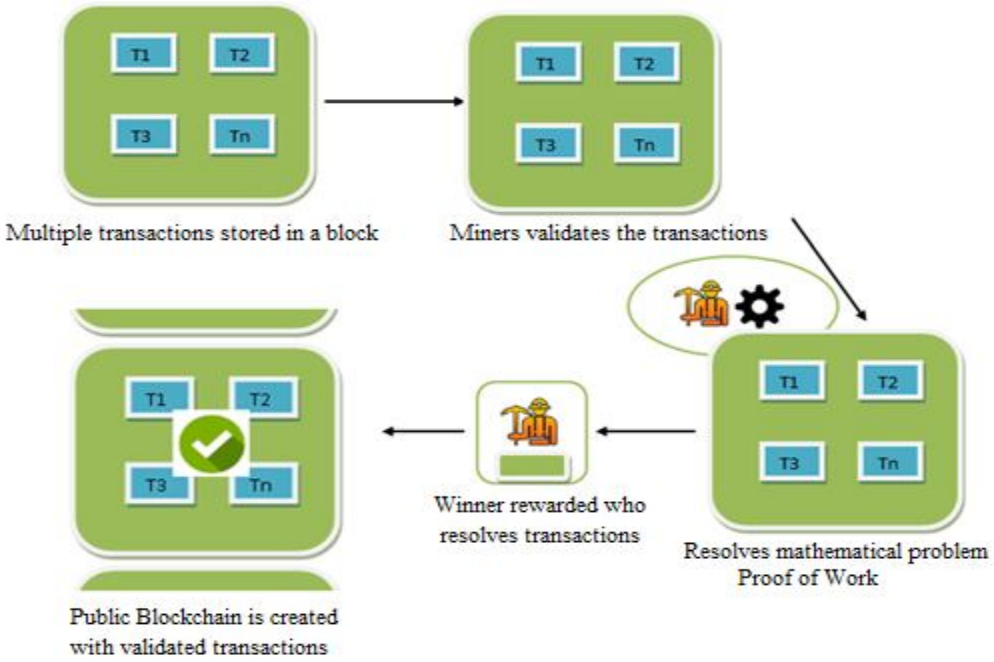


Fig. 1. Validation of Transaction Process

This mathematical computation or much CPU function is asymmetric and the work required is complex. Mining follows inverse hashing, where it finds number (nonce) so that the hash algorithm of block information is to be more lesser than the provided threshold (complexity). The threshold concludes the effort, computations, and energy required for mining to create a new block. That also makes the miner to be efficient for mining. This update occurs almost every 14 days, and a new block is generated in every 10 minutes. Miners put all the effort and get rewarded to make the node and blockchain more secure in the network. Proof-of-work is more complex computational process to prevent modification of the old blocks in blockchain.

a) *PoS:* Proof-of-stake is another consensus algorithm which possesses same motive as proof-of-work except the process to validate transactions in the distributed network. Proof-of-stake depends on its wealth called stake. A stake is a sum of currency locked up for some definite time period. Unlike proof-of-work, there is no reward of cryptocurrency unit for validating and confirming transaction within a block, instead, miners achieve transaction fees for the achieved task as reward. PoS works based on stake and emphasizes on number of cryptocurrencies in the blockchain to create new blocks rather than spending too many resources, energy or computational power as in PoW.

B. How does PoS work?

Proof-of-Stake is indirectly proportional to the network size and number of people staking the digital currency. If there is many people staking the coin then there will be fewer rewards. Furthermore, if the users have the possession of more cryptocurrencies for a longer period, achieve more transaction fees as reward, however, the process should be shared in the network so that the control of the coin is prevented from one person. This concept works similarly as in banks fixed deposit wherein the customer earns more interest for keeping significant amount of money for a longer period.

In PoS, the selection of a creator depends on the wealth, which is the number of coins or stake. Here, the user who validates the transaction and adds new block is called as forger. The forger puts their coins at stake to create a new block and validates the transactions to add a new block. They can also lose their stake and authority for further proceedings, if validator confirms any fraud transaction.

Here, it is required to select the forger to forge the next block. Following is the proper way to select the forger:

1) Randomized Selection- The user having the lowest hash value and the size of their stake will get the opportunity to select the next block.

2) Coin Age-Based Selection- The age of coin selects the forger.

III. COMPARISONS

A. Comparing PoW and PoS Consensus Algorithm

The proof-of-work and proof-of-stake are widely used consensus algorithm in blockchain technology. For example, bitcoin is commonly used cryptocurrency for proof-of-work and ethereum is switched for proof of stake algorithm.

1) *Impact of Blockchain Consensus:* The two important aspects of blockchain technology are decentralization and immutable record. Every cryptoasset has consensus mechanism. This mechanism ensures verified information in the ledger and protects from DDoS attack among the nodes. Also, it ensures next blocks added into the blockchain is secured from double-spending (spending same digital currency twice) and is equipped with the latest valid transactions on the network. This mechanism also prevents the network from interruption through continuous forking.

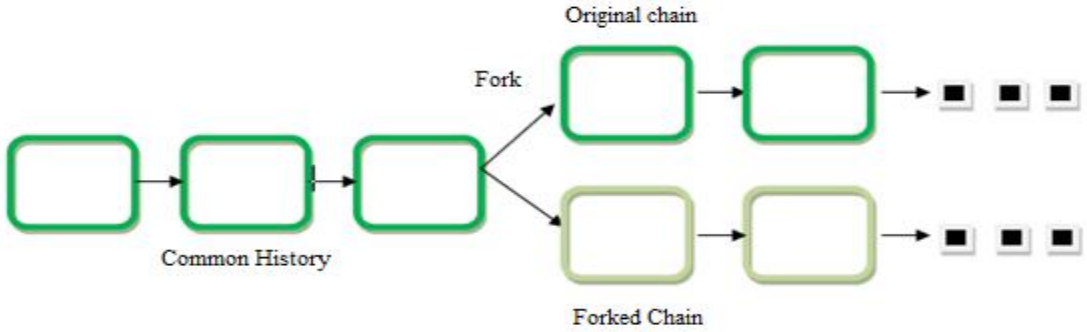


Fig. 2. Forking Process

We have different consensus mechanisms available with same perspective but different in their process. The main difference between all the consensus mechanisms are the way they represent and reward for the transaction verification.

2) *PoW algorithm:* The Proof of Work was invented by Markus Jacobson in 1999. All blockchain transactions are collected in groups called as mempool, where miners verify every transactions. Bitcoin users' requests transaction, which is then verified by the miner and add it to the next block using cryptographic hash value of the previous block. The hash value of the previous block is hidden for which miner has to keep trying a number after another. Once the miner finds the hash of the previous block, he declares it to the network to verify and create a new block. The first miner will be rewarded with bitcoin once he resolves this mathematical problem using massive computing power.

The miners have to resolve various problems with following characteristics:

a) Asymmetric problems are tricky to decipher but the resolution is easily approved by the network.

b) The puzzles with no skill involved, they require brute force, which needs massive computation energy.

c) The parameters are timely updated; the mining will become more complex if it exceeds average block time.

3) *PoS algorithm:* PoS algorithm has a different way of processing than PoW. In this case, set of nodes stake their own digital coins for transaction confirmation. The staker can have a better opportunity to own the transaction validation if the amount and the deposit time of the stake are longer. In PoS, mining is not required as done in PoW, instead the digital currencies are already created in the network avoiding loss of computation power and complex work. Also, the validators can add blocks more frequently if they have more stakes in the blockchain. The participant or validator will be selected based on the number of stake they possess. PoS implemented a technology called 'sharding'. It is the process of storing horizontal part of network in separate groups of nodes. The limitation of PoS depends on its monopoly and 'Nothing at Stake'. Monopoly is the main disadvantage of PoS algorithms by the major stakeholders of the network.

In case of 'Nothing at stake' there is more conflict occur if there are multiple unique chain in the blockchain, there can also have more forks which can create more confusion. Such problems does not occur in PoW algorithm.

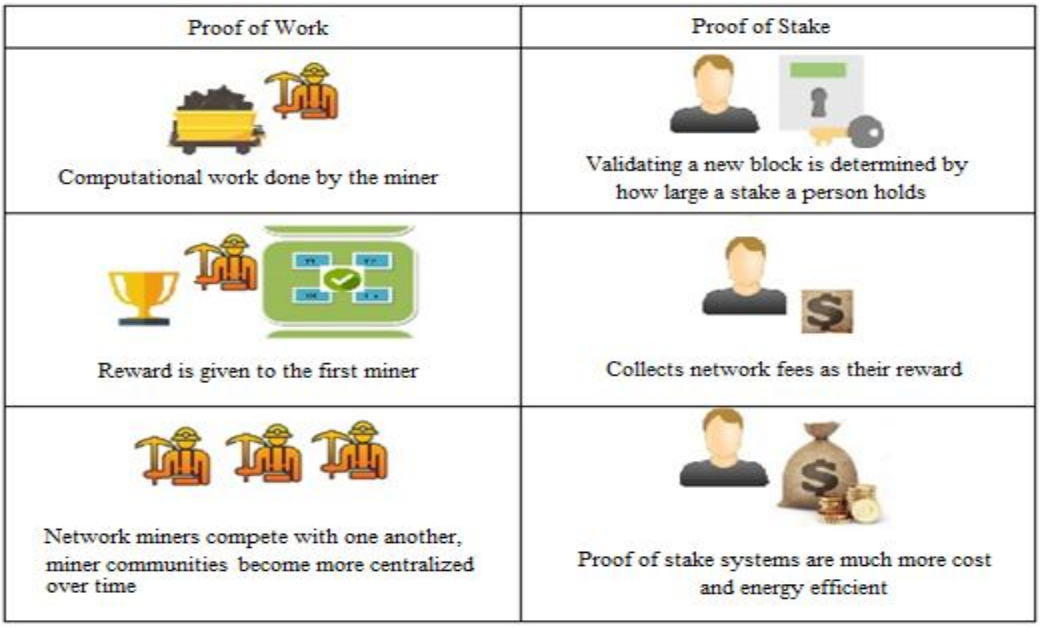


Fig. 3 PoW Vs. PoS

B. Comparing Characteristics of Consensus Algorithm

TABLE I
Property: Crypto Currency

PoW	PoS
BTC, ETH, Bitcoin Cash, Bitcoin SV, Litecoin, Monero, Zcash, Decreed and more.	BlackCoin, Peercoin, Nxt Coin, NEO, PIVX, Reddcoin, QTUM, OkCash, NAV Coin, Stratis and more.

TABLE II
Property: Immutability

PoW	PoS
It is the best immutable consensus method. It takes 10 minutes for every block to mine. Once 144 blocks (one 24 hour day) are mined, it becomes hard & costly to alter the data in a block and it makes concrete data after mining 1000 blocks (one week).	No Immutability. Proof-of-Stake instantly creates a block by saving time to select a new block signer.

TABLE III
Property: Cost, Energy And Resources

PoW	PoS
This algorithm demands massive energy. PoW network is very expensive. Application Specific Integrated Circuits (ASICS) machines are required for mining which is not feasible to afford to work.	This algorithm is not energy demanding. The process costs negligible due to less power consumption. Expensive advanced computer equipment is not required.

TABLE IV Property: Centralization

PoW	PoS
Centralization is a major threat for PoW. The mining work is widely popular for significant operations.	Proof-of-Stake systems possibly offers a reasonable resolution. The volume of the network can be occupied by a participant depend on the stake they invest.

TABLE V Property: Reward

PoW	PoS
The miner gets the rewards if they are capable of doing work.	It rewards validators or stakers based on the amount and duration they keep their stake.

C. Comparing Consensus Mechanism Concerning Security

Proof of Stake is uncertain for security risks as it is recent and not much experienced or accepted as Proof of work. Proof of work mechanism is considered more secure regarding double-spending where continuous forking is discouraged by the miners as it makes network unstable. While forking, miners have to decide whether to follow original blockchain or adjust to forked blockchain. To maintain both the blockchain, miners distribute their computational resources to both original and forked block chain. On the contrary, Proof-of-Stake called this problem as 'nothing at stake' problem. Here, validator receives a duplicate copy of stake on forked blockchain, and he can claim double transaction fee as reward after signing out from both the split blockchain. To solve this problem, this consensus required to enforce a deposit locked for certain periods. Casper is a protocol which encourages proof-of-stake system for the validators to participate with minimum deposition. The deposition could be removed in case the protocol finds any violation by the validator while constant forking.

D. Comparing Consensus Mechanism Concerning Vulnerability

There are standard Consensus Protocol Conditions that make the blockchain more secure to overcome vulnerabilities:

1) The user should transmit the block to the network instantly instead of holding.
2) Consensus protocol should resolve constant forking in blockchain.
3) The user should not build the block from the top of intermediary chains.

TABLE I
Vulnerabilities

1) Vulnerabilities	2) Consensus	3) Description
4) Selfish mining attack	5) PoW	6) The attacker determine mined blocks and devastates the resources of other miners.
7) Bribe Attack	8) PoS	9) The attacker secretly builds an alternative chain and gain confirmations after the transaction. The transaction is reversed considering a new blockchain.
10) 51% Attack	11) PoW, PoS	12) The attackers control the majority of mining power preventing other miners from completing blocks.
	13) PoW System	14) High cost and need to achieve 50%+ computation power in the network.
	15) PoS System	16) Cost is comparatively lower and need to achieve 50%+ currency in the network.

IV. FUTURE OF BLOCKCHAIN: PoW or PoS

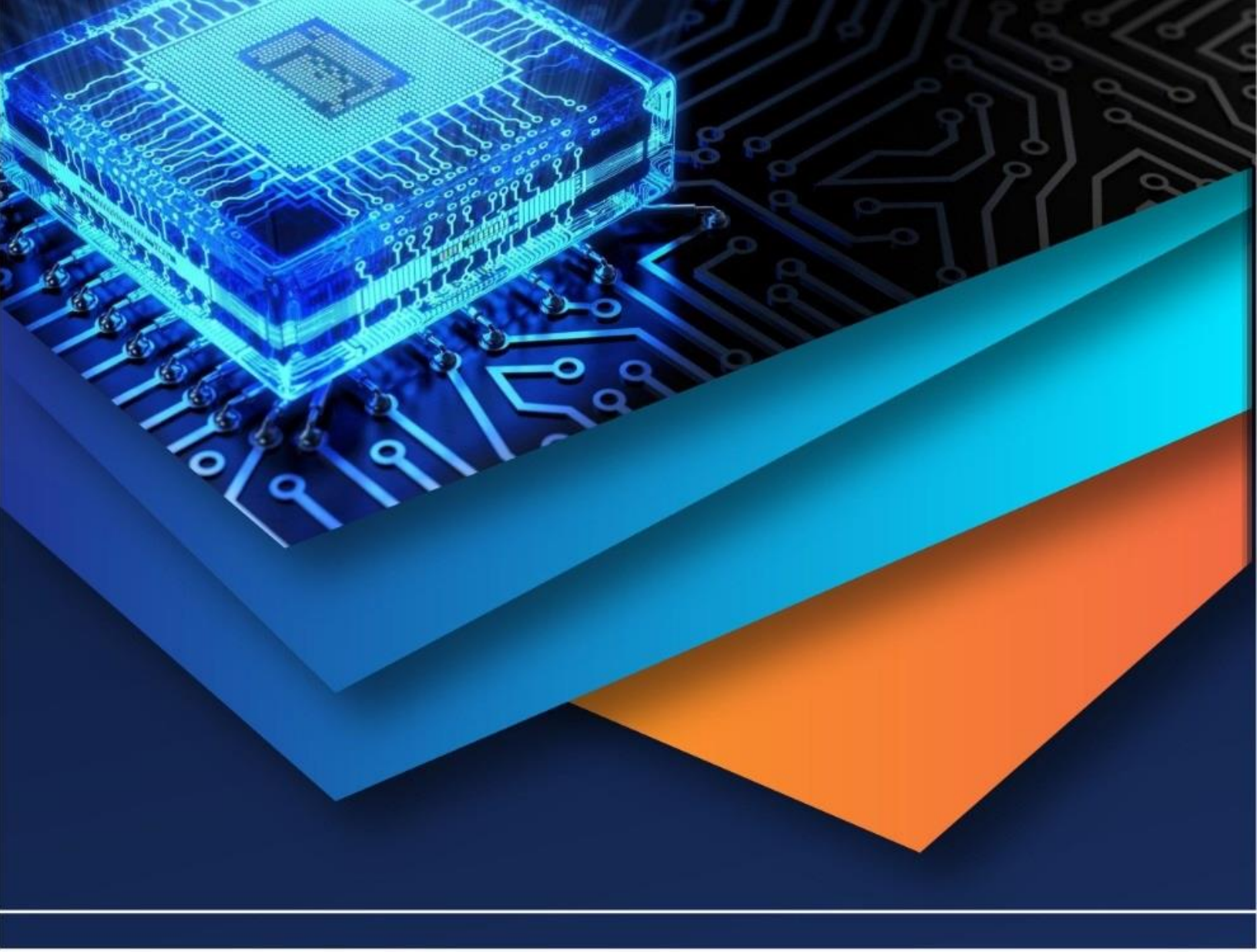
The popular cryptocurrency, Ethereum, has brought evolution for PoS over PoW. Ethereum is most important blockchain platform for application developers. The popularity of PoS algorithm will depend on the successful rate of Ethereum cryptocurrency. PoS and PoW are completely different process to achieve a single goal of validating transactions via various consensuses. The future among the two algorithms depend on the problem it addresses. The decision for the safety of the blockchain networks will be decided by the crypto society based on the capability the algorithms and only time will declare the most acceptable blockchain consensus algorithm for the future.

V. CONCLUSION

PoW and PoS are the most recent and implemented blockchain consensus mechanism. PoW is strongly verified and implemented in various cryptocurrency schemes. The blockchain implies PoW algorithm can hardly encounters with DDoS attacks on any technologies. However, the huge energy consumption, expensive computational power, rising centralization, and small transaction throughput will make it difficult to adopt in the future. On the contrary, PoS system does not consumption of computing power is lesser and the reward depends on the amount and the duration of keeping the stake longer. The PoS algorithm presents a scalable blockchain with major transaction throughput, however, it is not much securer than the decentralized PoW algorithm. The blockchain has been made more secure concerning attacks if there is rise in number of coins. The coin becomes more expensive preventing to take possession and buy huge amount of coins. In PoS, the protocol called Casper prevents from invalid transactions performed by staker. The protocol instantly removes the staker to validate the chain if found guilty and also stops for further staking. Though these consensus algorithms have a major role in cryptocurrency transaction, however, their differences in an approach becomes a controversial subject. The comparisons among consensuses algorithms prove its competitive nature for adoption.

REFERENCES

[1] Andrew Tar, Proof-of-Work, Explained. 17 Jan 2018. https://cointelegraph.com/explained/proof-of-work-explained
[2] Aleksandr Bulkin, Explaining blockchain—how proof of work enables trustless consensus. 03 May 2016. https://keepingstock.net/explaining-blockchain-how-proof-of-work-enables-trustless-consensus-2abed27f0845
[3] What is Blockchain Technology? A Step-by-Step Guide For Beginners. 13 Sep 2018. https://blockgeeks.com/guides/what-is-blockchain-technology/
[4] Georgios Konstantopoulos, Understanding Blockchain Fundamentals, Part 2: Proof of Work & Proof of Stake. 08 Dec 2017. https://medium.com/loom-network/understanding-blockchain-fundamentals-part-2-proof-of-work-proof-of-stake-b6ae907c7edb
[5] Ketalyse.io, **Blockchain Basics—PoW vs. Pos vs. PoI.** https://cryptodigestnews.com/blockchain-basics-pow-vs-pos-vs-poi-10a9b7c67d51
[6] Proof of Work vs Proof of Stake: Basic Mining Guide. https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/
[7] Toshendra, POI VS POW VS POS. 16 APRIL 2018. https://www.recordskeeper.co/blog/poi-vs-pow-vs-pos/
[8] Inferno Tower, **Why PoS is Better than PoW. 09 Feb 2017.** https://decentralize.today/why-pos-is-better-than-pow-2dc3cd9881a7
[9] Robert Greenfield, Vulnerability: Proof of Work vs. Proof of Stake. 24 Aug 2017. https://medium.com/@robertgreenfieldiv/vulnerability-proof-of-work-vs-proof-of-stake-f0c44807d18c
[10] Toshendra Kumar Sharma, HOW EXACTLY IS PROOF-OF-STAKE IMPLEMENTED? 28 JAN 2018. https://www.blockchain-council.org/blockchain/exactly-proof-stake-implemented/
[11] Turner Schumann, Consensus Mechanisms Explained: PoW vs. PoS. 5 April 2018. ttps://hackernoon.com/consensus-mechanisms-explained-pow-vs-pos-89951c66ae10
[12] edChain, POW vs. PoS: a comparison of two blockchain consensus algorithms. 12 June 2018. https://medium.com/@EdChain/pow-vs-pos-a-comparison-of-two-blockchain-consensus-algorithms-f3effdae55f5



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY