Proof of Work vs. Proof of Stake in Cryptocurrency

Shijie Lin *

Department of Computer Science, University of Nevada, Las Vegas, Nevada, United State

* Corresponding author email: lins13@unlv.nevada.edu

Abstract. This research document demonstrates the understanding of two key elements: Proof of Work (PoW) and Proof of Stake (PoS) within cryptocurrency. Cryptocurrency is often misunderstood as just volatile and risky but many investors do not understand what it even is. What is proof of work (BTC)? What is proof of stake (ETH)? How are they similar and how are they different? Cryptocurrency is actually more relatable that originally imagined once a person understands digital currency, money, it's origins, and how they hold similar monetary value within their own wallets. Cryptocurrency in PoW involves complicated mathematical equation solving via mining from a large growing pool of miners. These miners receive rewards such as bitcoin/tokens/etc. from their mined hash blocks verified, and blocks added to the blockchain. Challenges are that there are many miners and there may be a computational limit per core of each PC to be able to mine since Bitcoin has increased its difficulty 70 billion times since it started. BTC or Bitcoin is still widely trusted due to its increasing difficulty to race to the finish line to finish the advanced math computations. Whereas within PoS this is not a race between the masses and advanced math computations, but a validator that generally has more put in their stake vs. gained by receiving the processing fees associated. ETH or Ethereum has shifted from PoW to PoS for its better energy efficiency in resources. It has employed many other additional checks from Casper to Gasper which is the combination of Casper (fork-choice algorithm), LMD-GHOST (heavest observed subtree), and finality which requires 2/3rd agreement as well as once a block is justified it is upgraded to a finalized block. the similarities between the two PoW and PoS are that they are consensus-driven algorithms. They are designed to reach an agreement between the systems in place before each block is placed in the blockchain. Additionally, they also have a shared public ledger that operates on a global if not international scale. With blockchains, there is always only one true version and this is relying on a network rather than a governing authority like a bank/government entity to provide security and to prevent fraudulent transactions. It is still widely contested which is better than these two well-known consensus algorithms and it is still widely contested. The best answer is suited on a per investor per business basis in terms of the willingness of taking a risk just like any investment. This document serves to help provide guidance in the understanding of cryptocurrency of two main consensus algorithms, its similarities, differences, and help identify see what a potential investor the reader may be.

Keywords: Proof of Stake; Proof of Work; Cryptocurrency; Ethereum; Bitcoin; Blockchain Algorithm.

1. Introduction

In 2008, Satoshi Nakamoto published the paper "Bitcoin: A Peer-to-Peer Electronic Cash", which established Bitcoin as the first truly decentralized cash system also known as cryptocurrency [1]. Later in 2009, he released the first Bitcoin-related software, and mining was formally established. As Bitcoin grew in popularity, alternatives like Bitcoin such as Ethereum emerged onto the digital cash market. The cryptocurrency was growing steadily since with a remarkable spike in 2017 where BTC reached 40K in USD cash value [2]. Bitcoin like other cryptocurrencies is on a global public ledger. They operate truely decentralized, meaning there is no governing authority. While there maybe millions of miners as of today, the system remains the same where only one block represents a part of the ledger and appended one at a time [3]. While there may be forks along the blockchain there is only one truely correct chain (i.e., the longest) and the rest will be orphaned. It is also up to the miners to check the ledger to validate its legitimacy prior to be added to the blockchain. With the birth of Bitcoin, it gave stemmed growth to many alternative cryptocurrencies such as Ethereum. Which will be addressed later within this document in further detail, but the most interesting factor of ETH was using Bitcoin's consensus algorithm of PoW and has chosen to progress to the new PoS consensus

algorithm. The purpose of this document is to assist a potential investor or one that may be curious to learn more about cryptocurrency, how it all works, features, differences, and how it continues to evolve our concept of digital currency.

2. Proof of Work and Proof of Stake

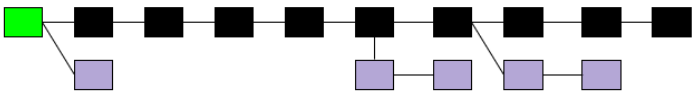
2.1 What Proof of Work is in Cryptocurrency

2.1.1 Definition

In cryptocurrencies, the Proof of Work (or PoW) is a decentralized proof method used to verify transactions [4]. Decentralization does not rely on a centralized authority, meaning is it not owned or controlled by any entity (i.e., government, bank, or the company itself) benefits of this is that PoW runs and is maintained by the participating users. For example, with the millions of users within BTC security is naturally strengthened as well as resistance to hacking (i.e. illegal data mining or fraudulent cryptocurrency trading) [5]. With decentralization, the participating members of the network expend more effort via mathematical puzzles as a means of encryption when verifying transactions. These puzzles will be addressed later in the section of algorithm, but for a simplicity the puzzles increase in complexity with each member competing to solve it. Proof of Work is a publicly recorded ledger that is distributed via "blockchain" to verify each transaction. For example, with regards to BTC, think of this ledger as a master record of all transactions completed with respect to PoW [6]. In reference to the blockchain, it is organized in a series of sequential blocks so when a user completes a transaction, it ensures no duplication occurs or trading with insufficient funds. Since the ledger is public, any transactions that are modified that do not go in line with the blockchain sequence would be quickly remedied. When a user wants to initiate a transaction, PoW's process produces the cryptographic hash when an input of any length is run through the hash function, an output of a fixed length is created. the data from the transaction is passed through a hash function and a secure hash is generated to be posted to the public ledger.

The verifier (Miner) needs to go through the hash function and compute the result to verify and actualize the transaction. The hash is a one-way function, so the transaction data cannot be derived by invert the result, but only by checking that the data generating the hash is the same as the original data [7]. With hash functions being a one-way function, it is not permutable thus collision-free. This mathematical function is essentially the Proof of "Work" in Bitcoin (i.e., similar to proving a proof in math). Even if the initiator of the transaction makes a small change to any part of the original data, the miner can compare the data result output from the hash function.

The proof of work is a series of checks and balances with more than one check potentially being performed to address the validity of the data output from the hash function; where a majority performing such checks will either confirm or reject the transaction. Each transaction is verified by a miner which represents a single vote based on a unique IP address. A proof of work is essentially a CPU with one vote. The longest chain represents the majority decision, while (if the majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains [8] (see Fig. 1).



Green is the start of the blockchain, **Black** are the mined honest blocks added to the blockchain, and **Purple** are

Fig 1. Longest Blockchain (in Black)

It will be very difficult for an attacker to tamper with the transactions. This is because the attacker would need to modify the previous and current blocks, and incoming blocks from other data miners.

This influx of blocks makes it increasingly if not nearly impossible for an attacker to keep modifying/altering the hash functions. This involves the algorithm which will be explained in a high-level overview in relation to Proof of Work in the next section.

2.1.2 Method of Proof of Work

2.1.2.1 How to Move Money from Personal Bank to Bitcoin

The process of purchasing crypto currency starts first with exchanging fiat money (money that is backed by the government as a medium of exchange). Fiat money is the same green dollar bills in everyone's wallet. Do not confuse this with the gold standard and representative money as they are backed by a commodity (i.e., gold bars or certificates for gold/silver). Keep in mind exchanging for cryptocurrency a fee will be incurred to process the transaction. The algorithm of Proof of Stake is not limited to one algorithm. In cryptocurrencies, the algorithm of Proof of Stake can be slightly different from one cryptocurrency to another. Even though the algorithms are different among them, they all have a common purpose, which is to achieve distributed consensus in the blockchain [9].

After a block is forged, the age is reset to zero and there is a specific amount of time before the node can forge another block for the blockchain. While this creates a delay in transaction time, the reasoning is to prevent controlling the consensus mechanism in place for blockchains (i.e. larger stake nodes taking over and controlling the blockchain). Also to ensure there is time to verify the validity of a block and that the node has not added any fraudulent blocks to the blockchain.

2.1.2.2 How the Validation Occurs

Validation occurs at the time of sign-up throught the bitcoin application or any other supporting applications that can sell bitcoin. This is were a potential buyer of cryptocurrency will go through a series of validation checks (i.e. identity verification). Validation of a personal photo government issued valid ID, drivers license, and/or passport. Which is also inclusive of banking information to link the account to the bank. This would often create the initial encryption keys from the bank to deposit into the Bitcoin wallet. At this time no purchase of Bitcoin has occurred, only a deposit like a gift card to use toward purchasing Bitcoin and/or any other cryptocurrency. This is the point where a potential investor can now purchase cryptocurrency and create their own starting block to be mined and validated with an end product of a blockchain [10].

2.1.3 Theory of Algorithm/ Methodology

This starts with a timestamp of when the transaction occurs and is recorded to the server by taking a hash along with other associated items such as IP address etc. This information is encrypted so the actual person making the transaction will not be at risk with having their personal information exposed [11]. This shows that the data has to have existed in order for the hash to have been created. While each hash has a block that connects to another has with another block before it (see Fig. 2) . A hash is a 256-bit number that has to start with a huge number of zeros (i.e. be a very small number).

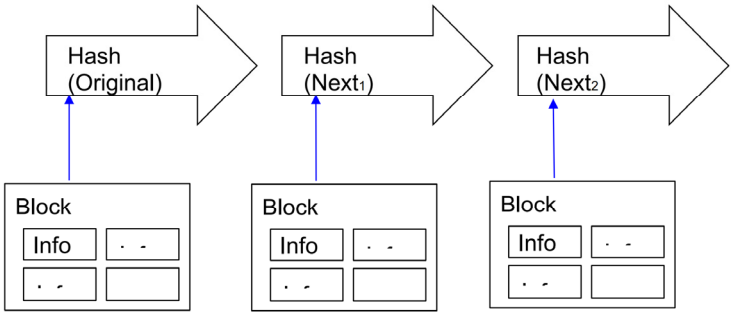


Fig 2. Timestamp Server & Blocks Being Added to each Hash

This is where the Proof of Work system will be implemented alongside the usage of the timestamp server on a peer-to-peer basis. Proof of work first scans for a value that when it is hashed the hash will begin with a number of zero bits. There is a certain required number of zero bits and the bits also

correlate to the average amount of time or work it will take to verify by executing the hash. In order for the time stamp network to work, the PoW increments a nonce until a value found gives back the required amount of zero bits (i.e. a sufficient amount of zeros). A nonce is a 32-bit random one-time whole number that is used to test. Miners use and discard millions of nounces every second until they can fulfill the requirement of the hash zero bits set by the network difficulty (see Fig. 3) .

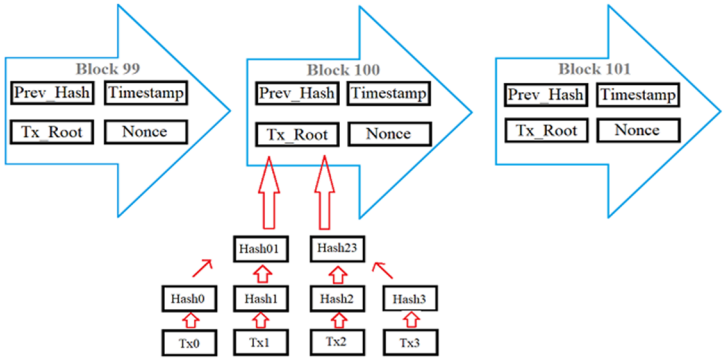


Fig 3. Building Blocks Associated with Nonces

Once the CPU has satisfied the computational requirements for PoW, the block created cannot be changed without re-doing all the work. As a result, if there were additional blocks chained after the first original block, the all the other blocks would require to be redone. The algorithm of PoW serves as the solution for consensus decision making. So like the voting system one CPU is equated to a single vote. Not to mistaken it by one IP one vote as an IP address can be compromised with an individual that is capable of allocating many IP addresses. The majority decision is based on the longest blockchain, which has the most amount of work invested. With the theory of honest nodes being able to grow the fastest and outpace any other forks in the blockchain.

2.1.4 Risk, Security and Speed of Transition

(1) Risk: If we have 51% attackers.

While it is possible for a 51% attacker situation to occur, it is improbable. The idea of 51% attackers is to take control of the majority of the network's “hash power” to control it. To accept fraudulent transactions and cancel ones they do not want to accept. However, this would require a significant amount of computers to mine, time and patience. As re-writing the history of the chain would be impossible, they either gain control of the processing power or try to double spend to stop other nodes from validating the transaction. Double spending is stealing as the attacker spends the coins and reverses the transactions to spend again thus spending twice. Normally this would not work as the transactions would have other nodes competing with the attacker to validate the transaction, but with control of the network it is possible to double spend. This would create a longer blockchain and blocks that were honest blocks then would be orphaned. While this is entirely possible with smaller less valued cryptocurrencies, the return value is insignificant as rewards mined (i.e. $0.0000001 reward). But when comparing the 51% attacker situation to larger cryptocurrencies like BTC, it is unlikely to occur. An attacker would need to compete against millions of miners and the amount of CPU processing cores would be astronomical to just compete in redoing the blocks within the blockchain and fending off honest blocks. Other solutions to fend against the 51% attack are: hard forks, chain crosslinks, and block delay penalty.

(2) Security: How to keep it secure

When a network is under attack, developers search for the offending block that would allow attacks to happen. The corrections that are made to the code from the attack result in what is known as a hard fork. These hard forks make it so that the new miners of the hash will now need to use the newly modified code and anyone mining with the old would be automatically booted from the network. Other prevention mechanisms using the hard fork method would be to introduce new codes for hard

forking. Cross-chain links from one blockchain to another blockchain will make weaker chains fixed. Regular recording of a smaller chain to a larger chain would as a means of proof that the blockchain is authentic and trustworthy (i.e. similar to getting a notary at a Bank). This form protects against attackers as these new nodes that have been notarized will not accept the removal or change of a previous notarized block [12]. Lastly, the block delay penalty is enforced to add an additional layer of security as it gives time for the developers to act. Typically, with attackers they try to double-spend coins (i.e., submitting a delayed chain of blocks). While it could occur accidentally in situations it would not be a chain of blocks, when minor attempts occur, they can be resolved via consensus. With major chains of blocks being delayed in submission it would pose large penalties towards the miner (i.e., assumed attacker). All this effort to keep cryptocurrency secure has drawbacks, which are ultimately higher levels of energy consumption and time needed [13].

(3) Speed of transition: energy used

While it has been covered that hard forking can be a security measure it should be understood by introducing new code, and having miners start again it will take more time and resources which delay the block formation to the blockchain. Similarly adding additional security features such as cross-chain where nodes are notarized and creates smaller blockchains to be unchangeable adds additional use of time and resources. As blockchain type notarizations reoccurs down the blockchain approximately every 10 minutes. Lastly block delay penalty, alongside with the first two additional layers of security the last one creates more time and resources being used but only in the event of a potential attack. Ultimately, PoW relies on its community to stay vigilant in the honest production of blocks for the blockchain within the network in terms of security.

2.2 What Proof of Stake is in Cryptocurrency

2.2.1 Definition

Proof of Stake is an alternative to the Proof of Work while it has the same overall mechanics in relation to the cybersecurity of cryptocurrency. PoS like PoW uses a blockchain mechanism to facilitate and validate transactions in digital assets on a blockchain. Blockchains like an accounting ledger is a digital ledger for recording public transactions in digital assets. Digital tokens are a way to represent value for online transactions (similar to a wire transfer of cash to another account or the UNLV cashiering collecting financial aid disbursements from a student's FAFSA account).

Mainly with Proof of Stake, there is a penalty system in place where the creator of the next block is chosen based on the amount of investments within cryptocurrency held by the specific user (or the Stake they have). Thus, if the user is attempting any type of fraudulent cryptocurrency mining they risk losing their investments (i.e. their stake) as a penalty. This could range from hundreds to thousands of dollars in penalties which encourages honest trading behavior and an easier way to track down systematically any person posing a risk to cryptocurrency cybersecurity swiftly. This does not mean everyone can be chosen to be a creator of the next block, as it weighs more heavily on the amount of stake placed as there is a simple convention of understanding that ownership of 1 cryptocurrency equates to 1 vote. Which means to have a higher majority vote, there is a higher investment and risk of a higher penalty that can be incurred. Thus, with the validation via Proof of Stake “validators” are randomly selected, there is no competition, and no paid rewards for completing a computational puzzle. PoS has this financial incentive for a forger node to avoid validating or initiating any potentially fraudulent transactions. Should fraudulent transactions be detected the forger node will lose some if not all of its stake and be blacklisted from being a potential validator in the future.

Proof of Stake holders are rewarded through other means such as additional ownership of tokens overtime via network-related fees, new-minted tokens, etc. Just to qualify as a validator for Proof of Stake they must be the first eligible based on an amount of coins and then for Ethereum specifically requires 32 ETH to be staked. For comparison purposes 32 ETH in cryptocurrency as of November 19, 2022 is worth approximately $38K USD (see Table 1). Proof of stake fundamentally shifts the

workload and energy consumption of verifying blocks to using the hardware of users that own cryptocurrency.

Table 1. Proof of Stake value of 32 ETH to USD Conversion Rate as of November 19, 2022 from Refinitiv Refinitiv

32 ETH (Ethereum)		USD $ US Dollar	Conversion Rate
32.00 ETH	↔	$38,480.00	$1,202.50 USD for 1 ETH

2.2.2 Theory of Agorithm/ Methodology

The process is the same in terms of initiating a transfer from one's bank account to say bitcoin to be a digital currency transaction ready for any potential investor. Validation of one's identity is also the same process to get a user ready before any person can hope to begin purchasing cryptocurrency.

While the term "algorithm" of PoS is used, it is not limited to a single process. The only commonality shared among all cryptocurrencies is that they all try to achieved distributed consensus of a block to add to the blockchain. With Proof of Stake, the block is not mined, but forged. Using ETH Ethereum for example it has only 117.5 million finite coins. While a cryptocurrency may start as PoW and transition to PoS just as ETH has done, there is a limit of coins.

PoS relies not on miners' resources and time, rather validators that stake capital in the form of cryptocurrency (i.e. ETH) in a form of a "smart contract." This staked ETH then will be collateral that could serve as a penalty should the validator conduct acts of dishonesty (i.e. dishonest block acceptance). This is because the validator assumes the responsibility for verifying the new blocks created over the network are honest blocks. Validators also may partake in creating new blocks to be validated in addition to validation of blocks. As it is assumed an investor will buy and/or sell cryptocurrency. After a block is forged, the age is reset to zero and there is a specific amount of time before the node can forge another block for the blockchain. While this creates a delay in transaction time, the reasoning is to prevent controlling the consensus mechanism in place for blockchains (i.e. larger stake nodes taking over and controlling the blockchain). Also to ensure there is time to verify the validity of a block and that the node has not added any fraudulent blocks to the blockchain.

Just as hash may have a required number of zero bits for PoW and 32-bits for nonces, PoS also has a required 32 slots for epochs. Epochs are simply a period of time that dictates when certain actions will occur like clockwork. Blockchain protocols like ETH utilize epochs to represent a set time for each validator within the committee to vote for or against a validity of a new block(s). While there is a level of pseudo-randomness selection for validators there is at least 128 validators that are assigned to slots [14]. Figure 4 demonstrates a smaller visual scale of what Proof of Stake in terms of knowing each step that happens prior to a new block being added to the blockchain.

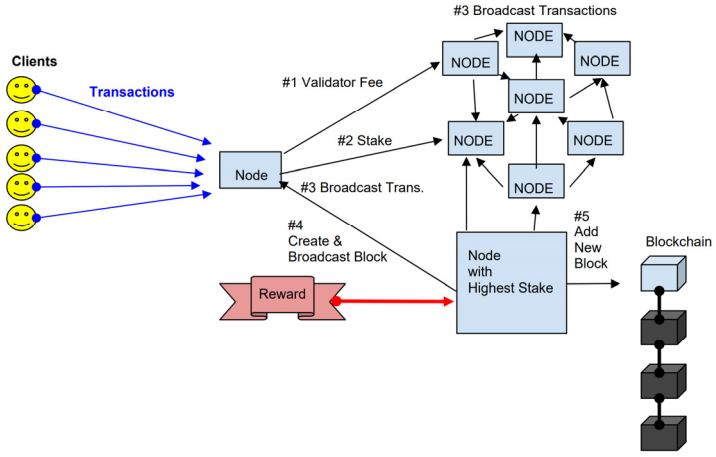


Fig 4. Proof of Stake Visual Methodology

2.2.3 Risk, Security, and Speed of Transition

(1) Risk: If we have 51% attackers

In the situation, there is a fraud attempt, with proof of stake the forger will generally lose more coins as they have staked more than the fees that could be gained. A majority stake within a network is commonly known as the "51% attack". A 51% attack would be required to successfully control a network to accept fraudulent transactions. This is impractical as it requires the attacker to have a higher investment of owning 51% of the finite number of coins in the cryptocurrency ecosystem. To own 51% of ETH cryptocurrency alone would be estimated in the billions. 117.5 million coins for ETH multiplied by 51% is roughly 59.9 million ETH coins and in USD translates to approximately 72 billion (see Table 2) Further discussed are the security protocols such as Gasper which is the union of Casper and GHOST that protect against such attacks.

Table 2. Estimate of 51% – ETH – in USD Conversion Rate as of November 19, 2022 from Refinitiv

ETH - Ethereum	↔	USD $ - US Dollar	Conversion
117,500,000 * 51% = 59,925,000 ETH coins For approximately 51% share		$72,059,812,500.00 USD	$1,202.50 USD for 1 ETH

(2) Security: How to keep it secure

The proof of stake algorithm has three fundamental features; a fixed finite number of coins that circulate the network at any given time. There is no possibility of creating new coins. Thus, with proof of stake a cryptocurrency ecosystem either has a finite set of coins to start or they start with the proof of work then switches after a certain set number of coins are attained. The transaction fees associated with creating a new block are given to the forger. Should the block be proven to be fraudulent the forger loses their transaction fee reward as well as their stake that is higher than the fees rewarded. The 51% attack can also be seen as a security feature as it is too time-consuming, costly, and would not yield profit relative to the money invested in the stake. However, there are specific security protocols called Gasper, which is the combination of two security separate security features of Casper and Ghost. Casper introduces finality where certain blocks cannot be reverted unless there is a critical failure to achieve consensus and/or is under attack where more than ⅓ of the total staked ether has been destroyed [4]. A block must pass two specific procedures to be finalized. The first step is ⅔ of the total staked ETH was voted for inclusion where then the block is "justified" and unlikely redone. The second step is that when the block is included in a finalized block it must be added to the main chain and not a side chain. Thus, it is unlikely to be redone without the attacker destroying millions of ETHS (i.e., billions of USD). Along with Casper, the Fork Choice algorithm is imposed to follow the chain that contains the greats distance from the genesis block (i.e. origin block). With the addition of the algorithm of GHOST, it emphasizes the Greedy Heaviest Observed Sub-Tree; sub-branches with the most activity. The adversary uses withheld blocks to displace an "honest chain" once it catches up with a sub-tree in the number of branched blocks. Essentially it looks like a wide tree that grows in width more than height. The result of this is that there can only be 2 blocks that enter the main blockchain permanently while others will be seemingly orphaned uncle blocks (uncle blocks within PoS can still have rewards collected unlike PoW).

These two in addition to introducing finality (one-way), it makes it even more difficult for attackers to try to obtain control over the network as well as being completely unprofitable with the high stakes and penalties they face. PoS arose as a means to fix the high resource consumption seen with PoW and lower the total transaction times needed to add a block to a chain. The sections below will entail how Proof of Stake is more efficient with less advanced mathematical computations.

(3) Speed of transition: energy used

Proof of Stake is more energy efficient since nodes are not competing against each other to add another block to the blockchain. Less energy also is consumed as there is no increasing difficulty level of advanced math being used. What generally happens is when there are more than enough

forgers that are producing a lot of hash values or blocks being forged, the network will increase the difficulty by lowering the threshold. What happens then is that the number of total legitimate hash values discovered is lower and thus the number of successful forged blocks will fall in number. However, the reverse is true when there are not enough forgers to create an acceptable rate of blocks found on the network, the threshold will increase to generate a greater number of valid hashes. Proof of Stake can dynamically adjust and create a controlled environment of hash validity rate to create a block to blockchain rate.

2.3 Compare ETH(Proof of Stake) with BTC(Proof of Work)

While both PoS and PoW are very similar as they require consensus to keep the blockchain secure. The main difference between them is that Proof of Stake requires significantly less work (i.e. energy) to validate blocks in the blockchain. This is because unlike Proof of Work; Proof of Stake does not have a large number of competitions to race to complete a validation of a transaction. This is due to the PoS selection draw system from the blockchain itself with a general consensus of having more stake than fees accessed to be selected as a potential validator. With PoW, the individual that successfully mines receives a small reward (i.e., bits, tokens, etc.) whereas PoS receive the ability to collect fees as their reward along with (i.e. bits, tokens, etc). This pseudo-random selection process considers factors such as the node's wealth, age of stake (or the age of the coins), and random block selection.

Another key difference is that PoS is forged and PoW is mined. This means that for PoS they are already "pre-mined" or essentially start with the Proof of Work method to then move to Proof of Stake. While for PoW there is an incentive for miners as they receive a reward for successfully mined blocks. With the method for PoS random block selection chooses potential validators based on the lowest hash value and highest stake. The age of the coin is determined by the number of days the coin has been staked by the number of coins being staked (i.e. days multiplied by the number of coins). Now that there is a general understanding of the similarities and differences in how these consensus algorithms work within digital currency a potential reader of this document can have a better grasp of what investor they maybe should they want to invest. There is a reason why digital currency is on the rise regardless of its known risk, just like any stock market – what the investor's willingness is in terms of the level of risk they will accept. With more understanding of how PoW and PoS work, they can ascertain which method of the two works best for them.

3. Conclusion

There are incentives for both Proof of Work and Proof of Stake; to identify which one has more incentive would be to know the investor. Both are considered decentralized as they do not have bank/government intervention. With PoW, there is an additional incentive for rewards to join a mining pool. Whereas in PoS the rewards are comparable to the amount of stake (i.e., money invested) and a mining pool does not benefit a potential investor. When seeing both in perspective, it is easy to see which of the Proof of Stake promotes true decentralization. However, the negatives of PoS can be that validators with large investments could potentially group together to have a higher likelihood to become the next validator of the blockchain. So, which one is better? It is still highly debatable between PoS and PoW, it would have to be per investor or per business perspective.

References

[1] Ciaian P, Rajcaniova M, Kancs A. The economics of BitCoin price formation[J]. Applied economics, 2016, 48(19): 1799-1815.

[2] Liu Y, Tsyvinski A. Risks and returns of cryptocurrency[J]. The Review of Financial Studies, 2021, 34(6): 2689-2727.

[3] Vranken H. Sustainability of bitcoin and blockchains[J]. Current opinion in environmental sustainability, 2017, 28: 1-9.

[4] Gervais A, Karame G O, Wüst K, et al. On the security and performance of proof of work blockchains[C]//Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. 2016: 3-16.

[5] Chen R, Tu I P, Chuang K E, et al. Endex: Degree of mining power decentralization for proof-of-work based blockchain systems[J]. IEEE Network, 2020, 34(6): 266-271.

[6] Kiayias A, Miller A, Zindros D. Non-interactive proofs of proof-of-work[C]//International Conference on Financial Cryptography and Data Security. Springer, Cham, 2020: 505-522.

[7] Grassi L, Khovratovich D, Rechberger C, et al. Poseidon: A New Hash Function for {Zero-Knowledge} Proof Systems[C]//30th USENIX Security Symposium (USENIX Security 21). 2021: 519-535.

[8] Cheng S, Lin S J. Mining strategies for completing the longest blockchain[J]. IEEE Access, 2019, 7: 173935-173943.

[9] Xiao Y, Zhang N, Lou W, et al. A survey of distributed consensus protocols for blockchain networks[J]. IEEE Communications Surveys & Tutorials, 2020, 22(2): 1432-1465.

[10] Jiménez I, Mora-Valencia A, Perote J. Risk quantification and validation for Bitcoin[J]. Operations Research Letters, 2020, 48(4): 534-541.

[11] Zhu X, Xu H, Zhao Z, et al. An Environmental Intrusion Detection Technology Based on WiFi[J]. Wireless Personal Communications, 2021, 119(2): 1425-1436.

[12] Zhang J, Liu Y, Zhang Z. Research on cross-chain technology architecture system based on blockchain [C]// International Conference in Communications, Signal Processing, and Systems. Springer, Singapore, 2019: 2609-2617.

[13] Hu Y, Manzoor A, Ekparinya P, et al. A delay-tolerant payment scheme based on the ethereum blockchain[J]. IEEE Access, 2019, 7: 33159-33172.

[14] Kiayias A, Russell A, David B, et al. Ouroboros: A provably secure proof-of-stake blockchain protocol [C] // Annual international cryptology conference. Springer, Cham, 2017: 357-388.