LIMITATIONS OF PROOF OF STAKE ALGORITHM IN BLOCKCHAIN: A REVIEW

Yenatfanta Shifferaw [1] and Surafel Lemma[2]

School of Electrical and Computer Engineering, Addis Ababa Institute of Technology, Addis Ababa University, Addis Ababa, Ethiopia
Corresponding Author's Email yenatshif@gmail.com

ABSTRACT

Blockchain is a new technology that has emerged to provide solutions to various sectors including health, insurance, advertising and many more. Despite the benefits, the technology has its own challenges with respect to the architecture and the consensus protocols involved. Proof of stake (PoS) is one type of consensus protocol by which a decision is made in order to handle transactions inside the blockchain technology. PoS concept states that a person can mine or validate block transactions according to how many coins the person holds. This work is aimed at studying the pros and cons of PoS and its proposed variations, and come up with recommendations to handle the drawbacks that currently exist in these algorithms. A detailed exploration has been carried out to understand the issues behind proof of stake protocol and the consensus algorithms that tried to address those issues. Consequently, four research gaps were identified. These gaps are less decentralized blockchain, vulnerable to 51% attack, not tested for security and performance, and problem of another issue being raised when trying to solve one. Most of the previously developed algorithms are based on proposing variation to the PoS working principle and trying to handle a particular limitation of PoS. Through careful analysis, specific and assumed best options on how to go about in addressing each of the four research gaps are laid down as future directions. This includes bringing hybrid implementation of different capability based consensus algorithms; generating, maintaining and testing traceability links on the system frequently; implementing merged mining of capability based consensus algorithm on a blockchain with a higher hash rate and through bringing more participants to the platform and making the committee of participant's mobility dynamic.

Keywords: block chain, consensus algorithms, proof of stake

INTRODUCTION

A blockchain is a growing list of records, called blocks that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data [1]. The process of creating new block on the chain is called mining and the nodes which create the new blocks are called miners. These miners are in turn rewarded for their efforts to create new blocks. There are three critical concepts behind the technology [2]. Digital assets are distributed instead of transferred, the asset is decentralized, allowing full real-time access and a transparent ledger (record) of changes preserves integrity of the document, which creates trust in the asset. Though blockchain has evolved to many levels since inception, there are broad categories in which blockchains can be classified majorly [3]. These are public, private and consortium blockchains. Public

block chain is a permission less ledger and can be used by anyone who has access to the internet and who is eligible to download it. Private block chain is the one which is shared only among the trusted participants. The rules of a private blockchain can be changed according to different levels of permissions, exposure, number of members, authorization etc. Consortium blockchain can be considered as a sub category of private blockchain. The main difference between consortium and private blockchain is that consortium blockchains are governed by a group rather than a single entity.

A key aspect of blockchain technology is determining which user publishes the next block. This is solved through implementing one of many possible consensus mechanisms [4]. The general category being compute-intensive, capability and voting based mechanisms. Compute-intensive based consensus protocols are energy-hungry mining algorithms. The miner needs to invest in huge amount of power in order to generate blocks. Capability based consensus protocols select a miner based on various factors such as the amount of cryptocurrency owned by that miner, the contribution of the miner to the community, the trust the network has on the miner, or the amount of storage owned by the miner. Voting based consensus protocols use a voting system to elect a miner for generating a block, eliminating the issue of high energy consumption and wealth dominance. All in all, due to the enormous benefits of the technology, today many sectors are looking for ways to integrate blockchain into their infrastructures. However the focus of this work is on proof of stake (PoS) which is the pioneer from capability based consensus mechanisms [4]. This is because PoS is more affordable for less developed countries and can further be applied for supply chain traceability, property ownership or digital payments. But before applying it for such sensitive purposes, the limitations of the mechanism and how they have been addressed before should be studied. The reason being, incorrect implementations can cause significant security issues. Consequently, the gaps involved in those solutions should be identified so that better alternatives can be suggested as future directions.

In light of this, we conducted a detailed exploration to understand the issues behind PoS protocol and the consensus algorithms that tried to address those issues. Accordingly, four research gaps were identified. These gaps are generating less decentralized blockchain, vulnerability to 51% attack, not being tested for security and performance, and problem with another issue being raised when trying to solve one.

The previously developed mechanisms base their concept on PoS by adding some other factors besides the stake in order to select the specific miners. Therefore the mechanisms tried to handle one particular limitation of the PoS. In this work, through careful analysis, recommendations on how to go about in addressing each of the four research gaps are laid down as future directions. These include bringing hybrid implementation of different capability based consensus algorithms; generating, maintaining and testing traceability links on the system frequently; implementing merged mining of capability based consensus algorithm on a blockchain with a higher hashrate and through bringing more participants to the platform and making the participant's mobility dynamic. The main contributions of this work are:

- Provide substantial information on proof of stake and its limitations
- Propose way forward for further improvement on the proof of stake mechanism

- Details alternatives and opportunities to apply PoS locally on record handling and supply chain systems

The rest of the paper is organized as follows. Sections 'Proof of Stake (PoS)' and 'Limitations of PoS' discuss PoS in detail highlighting the variants of PoS and their limitations. The efforts made in the state of the art to address the limitations of PoS are presented in Section 'Addressing the Issues of Proof of Stake', while the gaps in the state of the art are discussed in Section 'Research gaps in the State of the Art'. Section 'Future direction' outlines the future directions that could be used to address the gaps identified in the state of the art. Finally, Section 'Conclusions' concludes the paper.

PROOF OF STAKE (PoS)

PoS was proposed in 2011, as an alternate consensus protocol, which was later used by the crypto currency Peer coin (also known as PPcoin) in 2012 [5] in order to eliminate the competitive approach of Proof of Work (PoW) consensus protocol consuming a high amount of energy. PoS is designed for permissioned public distributed ledger and works on economically bonded puzzle solutions. In PoS, as there are no new coins generated, there is no block reward and the miner, which adds a new block of transactions to the blockchain, only takes the transaction fee. In addition, the miner for a particular block is chosen in a way that depends on its economic stake in the network with other factors combined [6].

Forger/Miner selection methods

The miners in PoS are called forgers and the mining process is referred to as forging. At the beginning of a forging round, each forger deposits a certain amount of owned crypto currency coins in the network as stake. The deposit is used by the protocol to select the next forger in the network.

There are two forger selection methods [4]:

1) Coin-age selection based on the number of days the coins are held at stake; and,

2) Randomized block selection based on the calculation of a hit value 25 using the forger's private key.

Coin age selection method

In the coin age selection method [5], a forger having the maximum value of coin age is selected to forge the block. Coin age is calculated by multiplying the total number of coins that are being staked by a forger and the total number of days the stake is held as shown in Equation 1. For example, 30 coins held for 10 days will have coin age of 300 coin days. In order to participate in the process of forging, the coins must be staked for minimum of 30 days. The stake holding duration is involved in order to avoid repetitive selection of a forger having more number of coins and to make the process semi-random. However, it may occur that a malicious user increases the probability of forging a block by holding the stake for a long period of time. To prevent this situation the stake holding period is capped at the maximum of 90 days by the protocol. Once a block is created by a forger, the coin-age value of the coins staked by that forger becomes zero.

$$Coinage = coinsstaked * Numberofdaysstakeheld \quad (1)$$

Peer coin uses a coin age parameter as part of its mining probability algorithm. In the peer coin system, the longer your peer coins have been stationary in your account (to a maximum of 90 days), the more power (coin age) they have to mint a block. The act of minting a block requires the consumption of

coin age value, and the network determines consensus by selecting the chain with the largest total consumed coin age.

There's a time lag in accepting a newly created block after it has been produced. This time lag may lead to another miner solving for the same exact block. This leads to a temporary mix-up on the blockchain network, as the nodes try to decide which block of the two newly identified blocks it wants to accept. In such a situation, the block with the larger stake gets accepted into the blockchain. The other block, with a smaller stake, is discarded from getting added to the blockchain and is termed as an orphan block.

When peercoin blocks are orphaned, the consumed coin age is released back to the blocks originating account [5]. As a result, the cost to attack the peercoin network is low, since attackers can keep attempting to generate blocks (referred to as grinding stake) until they succeed. Peercoin minimizes these and other risks by centrally broadcasting blockchain checkpoints several times a day, to freeze the blockchain and lock in transactions.

When blockchain checkpoints are broadcasted as many times as possible during the day, the nodes in the network will always have up to date information on the status of the blockchain. This will make it harder for attackers and malicious users to generate invalid blocks and add them to the chain. In addition, the transactions are not moved and are locked until they are verified and known by the nodes existing in the network.

Randomized block selection method

In the randomized block selection method [7], a forger having a specific hit value is selected for forging the next block. In order to calculate the hit value, each forger encrypts the hash of the previous block using its private key. The encrypted value is hashed and the first 8-bytes of the hashed output are stored as hit value. The use of a private key in the calculation generates a unique hit value for each forger in the network. The forger having the hit value below a target value is selected for the process of forging. The target value (T) is calculated using Equation 2. To make the selection based on the capability of the miner, the calculation of the target value involves the amount of coins staked by the miner. Consequently, the target value of each forger in the network is different and the value is higher for a forger having more coins at stake. When a forger holds more coins, the target value becomes high which provides an opportunity for the hit value to be less and the forger to be selected. Moreover, to make the target value non-deterministic, the calculation involves the time elapsed from the last block forged changing the target value every second.

$$T = T_b - S - B_e \quad (2)$$

Where T_b is the base target value calculated by multiplying the previous block's target value and the amount of time that was required to forge that block, S is the time elapsed since the last block forged and B_e are the coins at stake.

In scenarios, where more than one forger is having the same hit value below the target value, additional criteria which is based on the cumulative block difficulty D_{cb} value is used to discriminate and select a forger.

The cumulative difficulty mentioned is calculated using Equation 3. The forger who forges the block receives the transactions' fees of all the transactions in the block. There is no mining fee in PoS. If any forger tries to generate a malicious attack, the coins

at stake are lost as a way of discouraging the forgers to not perform such action.

$$D_{cb} = D_{pb} + \frac{2^{64}}{T_b} \quad (3)$$

Where D_{cb} is the cumulative difficulty, D_{pb} is the previous block's difficulty (the level of effort to create the previous block) and T_b is the base target value.

The PoS cryptocurrency known as Nxt uses a system where each coin in an account can be thought of as a tiny mining rig. The more tokens that are held in the account, the greater the chance that account will earn the right to generate a block. The total reward received as a result of block generation is the sum of the transaction fees located within the block. Since *Nxt* does not generate new tokens as a result of block creation, redistribution of Nxt occurs when block generators receive transaction fees. Subsequent blocks are generated based on verifiable, unique, and almost-unpredictable information from the preceding block. Blocks are linked by virtue of these connections, creating a chain of blocks (and transactions) that can be traced all the way back to the genesis block. Block generation time is targeted at 60 seconds, but variations in probabilities have resulted in an average block generation time of 80 seconds, with occasionally very long block intervals. If this specified time for generating a block is not met by the selected node, penalty is set for the delayed block submission and the process for selecting another node to generate the block continues.

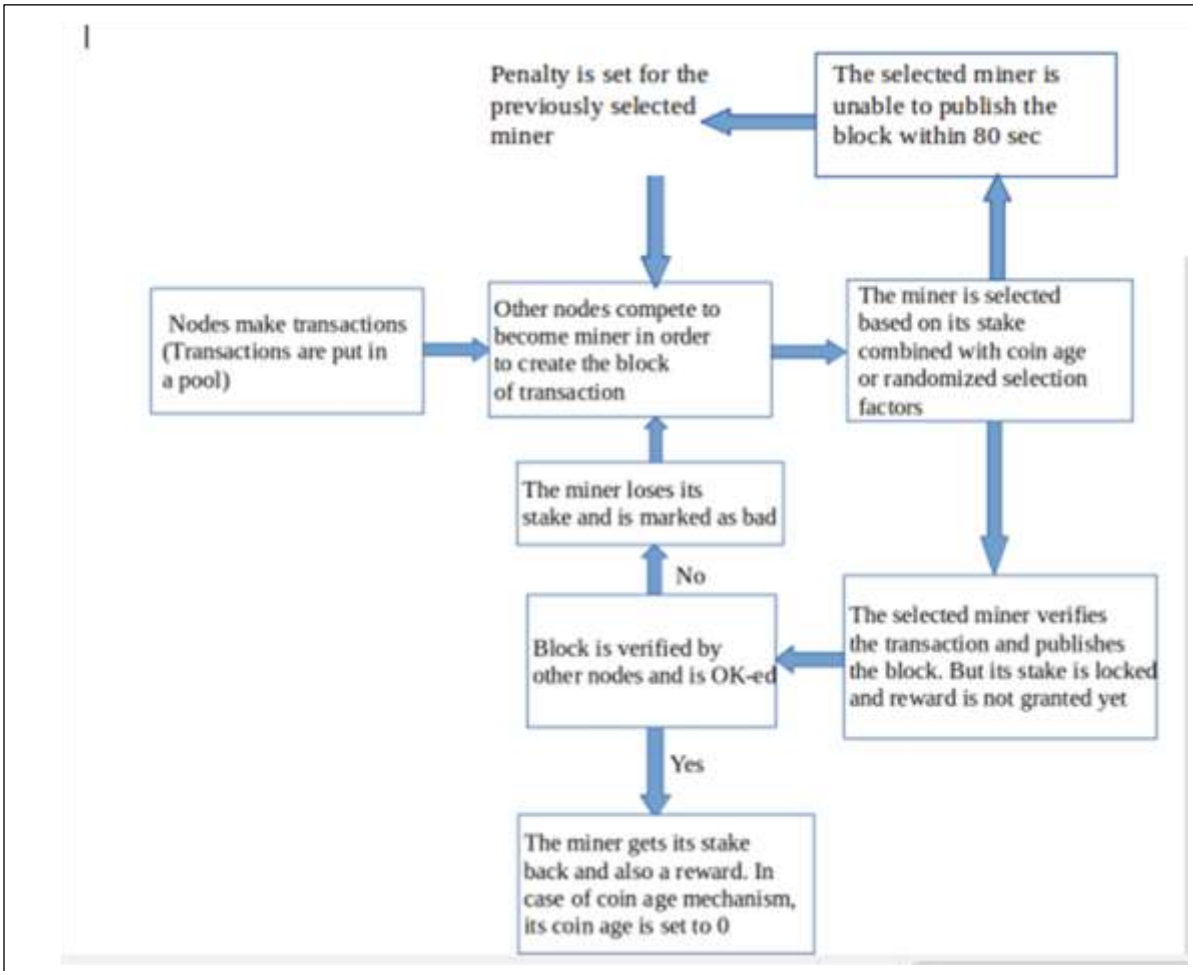

Figure 1: PoS based mechanism workflow

Generally, PoS involves transactions and selection of miners/forgers to validate the transactions. This mechanism is shown in Figure 1.

Variants of Proof of Stake

PoS comes in many variants from minimum to significant changes on the base protocol [6]. The most apparent fashion in which the consensus mechanisms differ is what strategy they implement to decide which node should be eligible to add the next block.

Leased Proof-of-Stake (LPoS)

LPoS [6] is an enhanced version of PoS. In a regular PoS system, each node that holds a certain amount of crypto currency is eligible to add the next block to the blockchain but in the LPoS system, specifically on the waves platform, users can lease their balance to full nodes. With LPoS, the user will have the ability to lease waves from the wallet to different contractors which can pay a percentage as a reward. The larger the amount that is leased to a full node, the higher the chances of that full node being selected to produce the next block. If that full node is selected to produce the next block, the leaser will then receive a percentage of the transaction fee that is collected by the full node.

Delegated Proof-of-Stake (DpoS)

DPoS [8] introduced another party besides the validators into the PoS system, which are called delegate. The delegates are the token holders. Since the beginning, there will be a certain fixed amount of validators/miners selected to forge new blocks into blockchain. Delegates will then vote on which validator to forge the next block. The voting weight is determined by the amount of coin staked. The validator that wins the voting will proceed and create a new block, then the reward will be shared and distributed to the delegates.

Masternode Proof of Stake

In masternode PoS, nodes become masternodes when meeting an amount of stake which is set as minimum. Masternodes are significantly invested with their large amount of stake. Therefore, they are considered more trustworthy than a regular node that exists in a Proof of Stake consensus mechanism. Masternode PoS is usually paired with regular proof of stake or PoW when processing transactions [9].

The aim behind creating such variants is to have an extra and various ways of selecting validators still without diverging from the basic principle of PoS.

Safety features in PoS

The following are included as safety features in PoS so as to keep the system secured.

Penalties for attackers: Some protocols using Proof of Stake include penalties for blockchain attackers. According to this protocol, a malicious validator can lose his entire stake if the network is attacked. Another penalty is in the form of loss in the value of the crypto currency involved, which in turn means loss in the net worth of the attacker.

Barriers to 51% stake: Another safety feature is that it is very difficult for a single entity to purchase a 51% stake in one go. Demand for the coin is bound to push up the price, making it a very costly option.

LIMITATIONS OF PoS

Some of the drawbacks that PoS consensus mechanism exhibits are the following.

Favors the rich

PoS algorithm allows users to stake their holdings as a means to verify the consensus. While investors cannot trade these staked assets, they earn proportionate returns for their investment. Consequently, the larger someone's staked holdings, the larger their return will be. In essence, this enables investors who already retain substantial holdings in a particular crypto currency to gain more shares. Having such staking invariably leads to greater centralization and the rich getting richer.

Reduces transaction flow in the network

Depending on the application, the transaction can be the transfer of a financial value or the execution of a smart contract. Therefore, when we say reduced transaction flow, we mean small movement of the digital currency. In PoS, since it is used as a stake to mine more blocks and get more profit, the miners would prefer to hold on to their stakes instead of moving them as transactions.

Encourages malicious users

This occurs because, in PoS, the staked coins are returned back to the nodes which have not been selected as miners. This limitation was not that frequent in PoW since the computational power used by the miner is non-retrievable [4]. However, in recent years more malicious users are observed in POW (e.g., in Ethereum Classic and Bitcoin gold [20]). Miners can form groups known as mining pools and each miner in a pool uses its capacity, and the mining reward is divided among the miners based on their mining contribution. If a mining pool owns more than 50% of the network's computing power, then it is likely that those miners would be able to prevent the validation of proposed transactions, and consequently stop the transactions between users. This will in turn give rise to the problem of 51% attack.

ADDRESSING THE ISSUES OF PoS

Various consensus protocols have been proposed in order to address different aspects of the drawbacks of PoS which were described in Section ‘Limitations of PoS’.

Rich getting richer

To address the problem of rich getting richer, the following algorithms have been proposed.

Delegated PoS (DPoS)

In order to solve the issue of rich getting richer in the PoS, a protocol called Delegated proof of stake (DPoS) [8] was proposed by Larimer. DPoS selects the forgers based on election rather than on the amount of staked coins owned. Unlike PoS, which follows direct democracy, it works on the concept of representative democracy. It boosts better distribution of reward as people tend to vote for the delegate (could be a casual user not necessarily rich) who will give back most rewards to them, thus favors decentralization. However, this protocol does not consider the case where each node votes for itself and has not been tested yet for its performance and protection against security threats.

Proof of Space (PoSpace)

Dziembowski et al [10] proposed proof of space (PoSpace) also known as proof of capacity where a miner having enough disk space wins the right to generate the next block in the chain. It generates all the random solutions, also called plots, using Shabal algorithm in advance and store it on the hard drive. This stage is called plotting and it may take days or even weeks

depending on the storage capacity of your drive. Then on the next stage, miners match their solutions to the most recent puzzle and the node with the fastest solution gets to mine the next block. Although this protocol consumes less energy and does not favor the rich, it can be prone to malware attacks as the plot of hashes stored in the hard disk can be easily attacked and tampered. Moreover, the miner does not burn any energy or coins in order to mine the block, encouraging malicious users to generate invalid block.

Proof of Believability (PoBelievability)

PoBelievability [11] was proposed in 2017. In this algorithm, the role of a miner is performed by a validator, where the validator with the highest believable score is selected for the generation of a block. Being developed by the Internet of Services Token (IOST) team in 2018, it implements a new sub-token called servi, which is awarded to good actors and cannot be traded. It serves to create a “believability score" of a particular node and verify it. Other factors that influence this process include IOST balance, the number of positive reviews of the node, and previous behaviors. Moreover, the validators are selected both randomly and algorithmically, so that the proven validators may participate along with the new ones.

Proof of believability avoids rich getting richer because the miner is not selected only based on the amount of coin he holds but based on believability score which is a combination of different factors. These are the amount of tokens, positive review and previous behaviors. This makes it not depend solely on the amount of coins. However, it has not been evaluated for security and privacy issues.

Proof of Elapsed Time (PoET)

PoET [12] was developed by Intel in 2016 to solve the issues of rich getting richer and centralization of the network, using trusted execution environment (TEE) along with Intel's software guard extensions (SGX). In PoET, each validator is assigned a wait time T for block construction which is assigned and monitored by the protocol. The first validator, who finishes the waiting time, creates and publishes the requested block on the network. The protocol works as the hybrid of first come first served and random lottery fashion. PoET requires the use of specialized SGX hardware developed by Intel. The dependency on specific hardware makes Intel as the controlling authority and thus the system less decentralized.

Reduced transaction flow

The following algorithms are proposed to address the reduced transaction flow problem.

Proof of Importance (PoI)

The crypto currency platform NEM introduced PoI [13] to address the issue of reduced transaction flow existing in the PoS protocol where the miners do not perform transactions in order to increase their chances of mining. Instead of considering only nodes' balances to determine the next winning node for solving the next block, it takes into account factors including a node's reputation and the number of transactions to or from that node. Therefore, this method of consensus considers productive network activity of nodes which is more efficient than only nodes' balances. PoI also discourages malicious users from mining invalid blocks as the miner is selected based on the recent transactions and the transacting parties. However, if a group of malicious attackers performs transactions amongst

themselves, then the network security might be compromised. In addition, PoI implicitly favors the rich as the calculation of the importance score is based on the number of vested tokens, and the number and size of recent transactions.

Proof of Stake Velocity (PoSV)

PoSV [14] was proposed by Ren in 2014 to promote more active network participation, which is necessary for an economy to grow. This is done by using an exponential growing function for the coin age calculation as compared to linear function used by PoS. PoSV is designed to encourage both ownership (stake) and activity (velocity). Due to the exponential decay in the growth rate of coin age, the newly accumulated coins will dominate the stale coins encouraging the stake holders to actively move their stake by transacting with counter parties. But if the counter parties exchange crypto currency with each other just for the purpose of reinitializing the age of the coin, then the economy will not benefit from this financial flow. Moreover, the protocol still favors the rich since it encourages higher stake.

Malicious users

The following algorithms are proposed to tackle the issue with malicious users which disrupt the functioning of the technology and the service it provides.

Proof of Burn (PoB)

To address the issue of high energy consumption in PoW and the problem of retrievable staked coins encouraging malicious users in PoS, Ian Stewart proposed Proof of Burn (PoB) in 2014. In PoB [15], the miners need to burn the coins by sending them to an irretrievable address, known as eater address. However, PoB favors the rich because the probability of a miner to be selected is higher if he burns more coins. The algorithm has not also been tested for its performance.

Proof of Authority (PoAuthority)

PoAuthority [16], a reputation-based consensus protocol was proposed in 2017 where the reputation or identity of the miner is at stake instead of coins. The identity is staked by a group of validators (authorities) that are pre-approved to validate transactions and blocks within the respective network. The group of validators is usually supposed to remain fairly small (25 or less) in order to ensure efficiency and manageable security of the network. But this algorithm makes the blockchain network less decentralized as the mining is performed by the fixed group of validators. Moreover, it has not been tested for its performance and protection against security threats.

Proof of History (PoH)

PoH was proposed in 2017 by Yakovenko [4]. It uses SHA-256 hashing algorithm that runs over itself continuously with the output being the next input. The node that verifies the transaction is called leader and it is selected based on the amount of stake the node holds. The leader runs the hash function for a random starting value, and passes the output as the input for the same function again. The leader records the output of the function every time and the corresponding counter value indicating the iteration. When a transaction takes place in the network, the leader verifies and combines it with the current hash output. This combination is then used as the next input and the counter value, the transaction and the hash output are recorded in the ledger. In this way, the transaction is recorded to have happened before and after a particular counter value.

The ledger state is then passed to the verifiers who verify the transaction validity and recalculate the hash output for all the counter values. However, PoH favors the rich for the selection of the leader making the process deterministic and centralized.

Proof of Activity (PoA)

PoA is a hybrid of PoW and PoS, and attempts to bring the best of both [17]. In PoA, the mining process starts, in the first phase as a standard PoW process with various miners trying to outpace each other with higher computing power to find a new block. When a new block is found (mined), the system switches to PoS, with the newly found block containing only a header and the miner's reward address. In the second phase, PoA selects N validators referred to as stakeholders based on the number of coins they have by using the PoS algorithm. Each selected stakeholder verifies and signs the block, and broadcasts it into the network. The more crypto coins a validator owns, the more chances the validator has for being selected as a signer. This mechanism suffers from the issue of high energy consumption as in PoW and it favors the rich as in PoS.

RESEARCH GAPS IN THE STATE OF THE ART

When looking at all the algorithms that have been implemented to solve the limitations of Proof of Stake, there are gaps in how the mechanisms handle the service to function correctly. These gaps are:

Raising another issue when solving one

This research gap occurs because of the fact that the previously proposed mechanisms only aimed at solving one of the three issues that exist in proof of stake, which in turn gave opportunity for the other issues to still exist and new issues to arise. For instance, in order to avoid the rich getting richer problem, Proof of Space provides capacity as a stake and not coins which in turn encourages malicious users to generate invalid blocks since the miner does not burn any energy or coins in order to mine the block.

Making the blockchain network less decentralized

The low degree of decentralization results from the fact that the applied consensus mechanisms require each node to agree on a certain state to reach total finality before a new transaction is committed to the distributed ledger. If a node owns some amount of stake in the network, then it means the node owns that much vote in the network. Given that most of the stakes in the network are not uniformly distributed, then those nodes that have more stakes exhibit more authority in the network and can influence the networks consensus which could easily lead to less decentralization.

Not being tested for performance or protection against security threats

A developed system needs to undergo performance testing using various metrics. It should also be provided with protection against threats. One of performance metrics is 'Throughput' which is calculated as the number of requests the system can process in unit time. The other metrics is 'Latency' which is evaluated as the time required processing a transaction from its initiation to final confirmation. On the other hand, security threats could be software flaws or malwares that can range anywhere from malicious crypto mining software to code that could shut down a company's servers. Crypto jacking is a type of malware which, simply put, is unauthorized and often unnoticeable takeover of a computer's resources to mine crypto currency. Although

crypto jackers don't directly steal money from their victims, the malware they inject causes performance issues, increases electricity usage, and opens the door for other hostile codes. Some of the proposed consensus mechanisms lack performance test and protection against security attacks.

Vulnerable to 51% attack

A 51% attack on a blockchain refers to a miner or a group of miners trying to control more than 50% of a network's mining power, computing power or hash rate. People in control of such mining power can block new transactions from taking place or being con_rmed. Whenever a transaction is carried out on a blockchain, be it by Bitcoin or any other crypto currency, it is usually put in a pool of unconfirmed transactions. Miners in return are allowed to select transactions from the pool to form a block of transactions. To be able to initiate such an attack one would need to spend an enormous amount of money to acquire mining hardware capable of competing with the rest of the network. However a bug in the code of a blockchain could in some cases open the door for a miner to produce new blocks at a much faster rate thus be in a position to initiate a 51% attack. In fact, an attack was performed in April 2018 on the Verge (XVG) blockchain. In this specific case, the attacker found a bug in the code of the verge blockchain protocol that allowed him to produce new blocks at an extremely fast pace [18].

FUTURE DIRECTION

From the research gaps mentioned in Section ‘Research gaps in the state of the art’, there can be a number of ways that can be undertaken so as to provide some kind of solutions or workarounds. Here, we will discuss some recommendations for each of the research gaps.

For the first problem of "Raising another issue when solving one", the way forward can be to have an implementation of hybrid algorithms. The focus can be on integrating some of the algorithms existing within the category of capability based consensus algorithms rather than on combining compute-intensive with capability based or voting based protocols. It will help to come up with a solution that could address all the three limitations of proof of stake or two of them at the same time. This can be achieved by first understanding the specific problems that each of the algorithms address. Afterwards, selecting one from each, the mathematical logic and implementation of those algorithms, their structure or architecture will be studied in depth.

Through this, one's implementation can be incorporated with the other with no conflicts arising or security concept being compromised. Putting into consideration the working platform of each algorithm and pulling out the rules that best describes the protocol or pinpoints its strongest capability, it can be possible to come up with a strong and efficient protocol. It needs deep investigation into each algorithm but as a first footstep: Proof of Believability, Proof of Importance and Proof of burn can be further studied and integrated to address the issues behind Proof of Stake.

When looking into the second issue of "Making the blockchain network less decentralized", despite envisioned decentralization; the high cost of mining has led to considerable centralization of consensus in practice. In order to share the risk of spending resources and the problem of failing to win the competition, groups of miners form mining pools. This resulted in just a few mining pools validating most transactions. Although, in practice achieving consensus is more centralized than it was envisioned, a certain degree of

decentralization is still retained. In order to make the network more decentralized, we can incorporate a consensus algorithm for instance Proof of Believability (PoB).

In PoB mechanism, the entry barrier to becoming a candidate is lower than other networks; therefore more community members are able to participate. At the same time, the committee members will have increased variation with higher frequency. The committee's mobility is very dynamic, and the degree of decentralization is much higher than others, thereby achieving better community autonomy while also guaranteeing higher security.

In order to address the third issue of "Not being tested for performance or protection against security threats", in blockchain, security issues range anywhere from malicious crypto mining software to code that could shut down a company's servers. This can be solved to some extent through applying software traceability links which makes it easier to track and verify vulnerabilities for product integrity. Software traceability is the ability to inter-relate any uniquely identifiable software artifact to any other, maintain required links over time and test their performance. Usually the apps built on top of the blockchains are still susceptible to bugs. Therefore, it's important that they need to undergo rigorous testing and review. This is where traceability links come in handy. Traceability links are important factors for the reuse, testing and maintenance of software system components. The tracelinks can be applied on the software artifacts based on user requirements, which can then be visualized periodically on a dashboard and in turn can give a better chance of identifying threats. Additionally, any reputable application should have redundant security measures in place. The number of requests the system can handle should be measured. If there's an issue with the performance value, action should be taken to check whether there are mysterious programs running or for any presence of security loopholes.

For the fourth issue of "Vulnerable to 51% attack", generally, 51% attacks are one of the most recognized blockchain security issues. In 2018, several notable crypto currencies, such as ZenCash, Verge, and Ethereum Classic were victim to 51% attacks [19]. Overall, attackers walked away with over USD 20 million due to this blockchain security issue. Most of the time, the pools vulnerable to these kind of attacks are small pools or the ones implementing proof of work consensus mechanisms. As a solution, being vigilant of mining pools, implementing merged mining on a blockchain with a higher hashrate, or switching to a different consensus mechanism are all viable options [19]. All the options seem possible but the merged

Table 1: Proposed Future directions

No	Gaps	Future direction
1.	Raising another issue when solving one	Implementation of hybrid capability based consensus mechanism
2.	Making the blockchain network less decentralized	Incorporate Proof of Believability algorithm and have more community members
3.	Not being tested for performance or protection against security threats	Applying Software traceability links and perform scheduled checking
4.	Vulnerable to 51% attack	Using merged mining of capability based consensus algorithms through allowing different crypto currencies to be combined

mining could yield a better result and be more appealing especially for smaller pools. Merged mining is a mechanism that allows different crypto currencies, which use the same algorithm, to be mined together. The benefit is that every hash the miner does, contributes to the total hash rate of both (all) merged currencies, and as a result they are all more secure. The big advantages of merged mining are greatly reducing the investment costs for miners since they won't need to buy brand new equipment. Miners can also earn extra rewards by maintaining the secondary chain. The other advantage is crypto currencies with lower hashrate can gain additional hashing power by piggybacking off a crypto currency with higher hashrate and thus eliminate the problem of 51% attacks. Currently, merged mining is performed on blockchains that are implemented based on PoW mechanism. However, here it is stated as a future direction to be applied in PoS implemented blockchains. It can be carried out in such a way that an encrypted puzzle is provided and if a miner successfully solves it, the corresponding block and the solution are combined and put into their respective blockchains.

In Table 1, each of the identified research gaps and their corresponding proposed future directions are summarized.

CONCLUSIONS

Blockchain technology was introduced over a decade ago with the intention of carrying out digital transactions without the need for third party. This technology has been applied to different sectors other than finance which include health, agriculture, advertising and many more. Through this, various architectures and consensus algorithms have been proposed to produce a specific kind of blockchain system. Generally, the structure of blockchain system falls into these three categories: public, private and consortium while each of them is being used for specific purposes. The consensus protocols include compute-intensive, capability based and voting based. A deep dive into the implementation and limitations of Proof of Stake consensus mechanism, which is the pioneer of capability based protocol, has been done. This is because Proof of Stake is more affordable for less developed countries and can further be applied for supply chain traceability, property record system and other sensitive and critical areas. This work has highlighted the consensus algorithms which are proposed considering the main drawbacks of proof of stake algorithm. It can be noted that the algorithms implemented to solve one of the issues from the three limitations identified, i.e., rich getting richer, reduced transaction flow, and malicious users, usually end up with the other issue still being present and untouched.

As it has been identified in this work, there are four main research gaps that exist currently in the state of the art which are raising another issue when solving one, making the blockchain network less decentralized, not being tested for performance or protection against security threats, and vulnerable to 51% attack. Recommendations are laid down in order to address these gaps which include implementation of hybrid capability based consensus mechanism, incorporate Proof of Believability algorithm and have more community members, applying software traceability links and checking them frequently, and using merged mining through allowing different crypto currencies to be combined respectively.

Overall, putting into consideration the blockchain platform and its specific applications, the directions stated above

could be used as one of the possible ways through which one can try to address the aforementioned issues.

REFERENCES

[1] Michael Nofer and Oliver Hinz. Blockchain, Springer-*Business & Information Systems Engineering*, 2017.

[2] Michael Crosby, Nachiappan, Pradan Pattanayak, Sanjeev Verma and Vignesh Kalyanaraman. Blockchain technology: Beyond bitcoin, Applied Innovation Review (AIR), 2016.

[3] Andreev, R. A.; Andreeva, P.A.; Krotov, L. N.; and Krotova, E. L., Review of blockchain technology: Types of blockchain and their application, Intelligent Systems in Manufacturing, 2018.

[4] Leila Ismail and Huned Materwala. A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions, Symmetry 11 (10), 2019.

[5] Sunny King and Scott Nadal. Ppcoin: peer-to-peer crypto-currency with proof-of-stake. 2018.

[6] Abdul Wahab and Waqas Mahmood. Survey of consensus protocols. Social Science Research Network, 1(1), 2018.

[7] Nxt whitepaper. https://nxtdocs.jelurida.com/Nxt_Whitepaper.(Accessed: April 2020).

[8] Bitshares. Delegated proof-of-stake consensus. https://bitshares.org/technology/delegated-proof-of-stake-consensus/.(Accessed: April 2020).

[9] Top Staking. Different types of proof of stake and staking. https://medium.com/@topstaking/different-types-of-proof-of-stake-and-staking-e2a718a0084c.(Accessed: April 2020).

[10] Stefan Dziembowski, Sebastian Faust, Vladimir Kolmogorov, and Krzysztof Pietrzak. Proofs of space. Springer-Annual Cryptology Conference,10 (1), 2015.

[11] Iost-official. Proof of believability. https://github.com/iost-official/Documents/blob/master/Technical_White_Paper/EN/Tech_white_paper_EN.md (Accessed: May 2020).

[12] Rick Echevarria. The second coming of blockchain. https://software.intel.com/en-us/blogs/2017/02/14/the-second-coming-of-blockchain.(Accessed: May 2020).

[13] NEM: technical reference. https://nem.io/wp-content/themes/nem/files/NEM_techRef.pdf.(Accessed: May 2020).

[14] Lerry Ren. Proof of stake velocity: Building the social currency of the digital age. Self-published, reddcoin.com, 10(1), 2014.

[15] Kostis Karantia, Aggelos Kiayias, and Dionysis Zindros. Proof-of-burn, International Association for Cryptologic Research, 2019.

[16] Stefano De Angelis, Leonardo Aniello, Roberto Baldoni, Federico Lombardi, Andrea Margheri, and Vladimiro Sassone. Pbft vs proof-of-authority: applying the cap theorem to permissioned block chain, 2018.

[17] Zhiqiang Liu, ShuyangTang, Sherman S.M.Chow, Zhen Liu and Yu Long. Fork-free hybrid consensus with flexible proof-of-activity, 2019.

[18] Jimi S. Blockchain explained: how a 51% attack works (double spend attack). https://blog.goodaudience.com/what-is-a-51-attack-or-double-spend-attack-aa108db63474.(Accessed: June 2020).

[19] Ledgerops Top five blockchain security issues in 2019. https://ledgerops.com/blog/2019-03-28-top-five-blockchain-security-issues-in-2019/.(Accessed: June 2020)

[20] MIT Technology Review, Once hailed as unshakable, block chains are now getting hacked. https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/.(Accessed: January 2021).