Nathan Minkwitz

Blockchain & MIS – MGMT 299 - 03

Dr. Hamid

05 May 2022

Final Exam – Prompt

Explain the below consensus algorithms in at least a couple of paragraphs. If there are some famous blockchains/cryptocurrencies that use these methods, please mention them (e.g. bitcoin uses proof of work). There might be some degrees of similarities between them, if you could, mention them, too.

proof of work, proof of stacking, Delegated Proof of Stake, proof of transfer, Proof of Elapsed Time (PoET), Proof of Burn, Proof of History (PoH), Proof of Capacity, Proof of Identity, Proof of Authority, Proof of Activity

Consensus Algorithms

geeksforgeeks

A Blockchain is a decentralized network that provides immutability, privacy, and transparency for all members of the network. Consensus algorithms are fundamental in Blockchain development and ensure that every transaction passed in the Blockchain is secured and verified.

The purpose of these consensus algorithms is to bring all nodes into agreement as there is minimal trust between the nodes in their distributed environment. They also have other objectives or requirements that promote agreement among all nodes, like mandatory participation and equality for all nodes.

These mechanisms ensure that every new block that is added to the Blockchain is the only version, and that is also verified by all the nodes in the Blockchain. Consensus protocols create reliable Blockchain networks and establish trust between anonymous users in a decentralized space.

Proof of Work (PoW)

geeksforgeeks, Investopedia

PoW was the first consensus protocol used for a Blockchain network development. It was later applied to Bitcoin and soon to the majority of other cryptocurrencies in circulation or in development. PoW involves a lot of effort and computing power to solve an arbitrary but easily verifiable answer to select the next miner to that gets to generate a new block in the blockchain. Because of PoW, cryptocurrency transactions can be processed person-to-person securely and without intermediaries. It help prevent malicious use of computing capabilities like sending spam emails or a denial-of-service (DoS) attack.

Once all nodes reach a consensus, it is relatively quick and simple to validate the new blocks transactions, organize them in chronological order, and then broadcast the new block to the rest of the network. The challenge in this process comes with solving the hard mathematical problem to connect the new block to the longest chain in the blockchain. After the miner finds the solution, it simultaneously announces it to the rest of the network and receives the mining reward. The more miners that belong to the network only speeds up this process of adding a new block thus the Bitcoin network regularly changes the difficulty level of mining a new block (Frankenfield, 2022).

Since the launch of Bitcoin in 2009, its block rewards have been halved and will continue until the number of coins in circulation reaches its maximum supply of $21 million. As of right now, miners have been receiving around 6.25 BTC for each new block which only takes about 10 minutes. Once bitcoin does reach its maximum supply there are speculations suggesting that miners will have to only rely on transaction fees given that there are no new blocks being mined (Hooda, 2019). Other Cryptocurrencies using PoW include Litecoin, Ethereum, Monero coin, and Dogecoin.

Proof of Staking (PoS)

geeksforgeeks, Investopedia

PoS is the most common alternative to PoW with ETH shifting to PoS consensus with its update. Instead of investing in expensive hardware to solve a complex PoW problem, PoS changes the way blocks are verified using the machines of coin owners. Coin owners (nodes on a network) offer their

coins up as collateral, or stake, to become the potential validators of a new block and earn the coin based on the amount staked. Then the validator selection algorithm selects a candidate, based on quantity staked in the coin combined with coin-age-based and random block selection algorithms.

“Proof-of-stake reduces the amount of computational work needed to verify blocks and transactions that keep the blockchain, and thus a cryptocurrency, secure” (Frankenfield, 2022). It is more energy efficient because the nodes are not competing to attach to a new block and there are not problems to be solved. PoW blockchains like bitcoin lead to a more centralized representation of a blockchain where joining the mining pool yields exponential reward. While PoS promotes decentralization with rewards that are proportional to the amount staked and thus there is no added advantage to joining the mining group. PoS is also considered to be safer than PoW with regards to the potential of an attack on the network because for someone to hack the network they would need to own 51% of the stakes.

There are some drawbacks to PoS especially because it is new technology and research continues to uncover flaws in the system. Another problem is that if validator candidates combine and own a large share of the cryptocurrency, there is a higher chance of being selected as validators.

Delegated Proof of Stake (DPoS)

Technopedia, Gemini

DPoS is a consensus algorithm in the blockchain that competes with PoW and PoS protocols as a way to verify transactions and promote blockchain organization. Users are able to delegate the production of new blocks in the blockchain to a certain number of delegates, also known as witnesses or block producers. Network participants decide which witnesses will validate the new blocks through a democratic voting process where votes are weighed by the quantity of tokens staked in platform crypto wallets. The voting process is continuous, and users can replace block producers is they are not behaving honestly and effectively.

Elected block producers receive the transaction fees from the newly validated block. That block producer then shares the reward with the rest of the users that pooled their tokens in the successful delegate’s staking pool. Rewards are shared based on the quantity of coins each user has staked. For example, if a user’s stake represents 5% of the total staking balance in a given delegates staking pool, that users receive 5% of the total block reward.

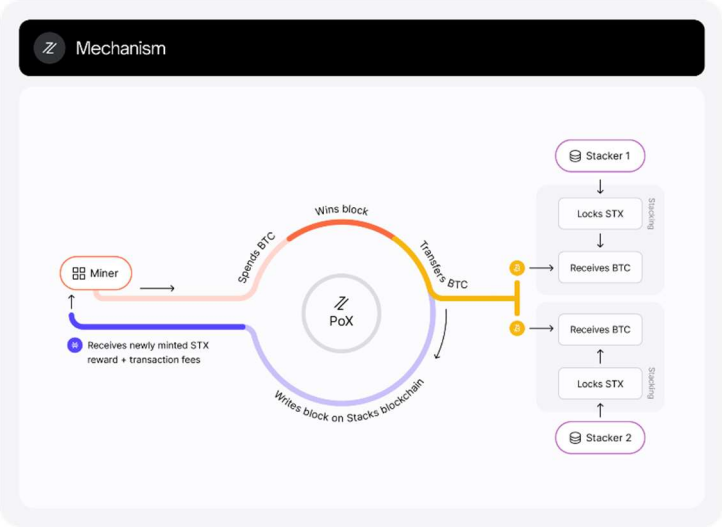
Those supporting DPoS state that it is a more democratic way of deciding who verifies the next block. It allows a more diverse group of people to participate in the verification process because of the fact that a new group of delegates are selected for each new block. Also, because it is a much smaller group of validators, usually ranging between 20 and 100 witnesses, they can reach a consensus much more efficiently than a traditional PoS system (Cryptopedia Staff, 2021).

Traditional PoS algorithms are random but weighted in favor of network participants that hold a large number of the network’s coins. DPoS allows all holders of a cryptocurrency to influence network decisions and thus makes it one of the most used variations of the original PoS model. Several major projects, like EOSIO and TRON, utilize DPoS. People against the DPoS protocol point out that it centralizes the decision-making processes around the richest few, “Some worry that a delegated proof of stake model will result in larger stakeholders forming cartels, which can lead to multiple types of bad market actions” (Techopedia, 2019).

Proof of Transfer (PoX)

Stacks.co – PoX, hackernoon

PoX is a new blockchain consensus protocol which connects two separate blockchains, i.e. BTC and STX. It is a mining capability that provides a new take on consensus and allows builders to leverage and extend BTC powers without modifying itself. PoX is an extension of the proof-of-burn mechanism, where miners compete by destroying a PoW currency from an established blockchain as a proxy for computing resources. Rather than burning the cryptocurrency, miners transfer the committed coins to other participants in the network who are 'Stacking'. As it can be seen in the diagram below, BTC transferred by the miners is then used to provide Stacking rewards to token holders for helping to secure a stable network.



There are many advantages to utilizing PoX with respect to both secure decentralized processes and sustainable practices. All STX transactions are settled on BTC which results in inherited BTC security for STX users. Other benefits include the fact that apps built on Stacks can interact with Bitcoin on-chain data so anyone can mine because no special hardware is required. This technology allows developers to benefit from BTC's properties without modifying BTC itself.

It is also a sustainable extension to the environmentally costly BTC mining processes. "The electricity expended to secure Bitcoins is reused by Stacks, allowing builders to create more value from energy already spent" (*Stacks features and possibilities* 2022). PoX reuses the energy already expended in BTC's PoW consensus mechanism. The STX PoX extension allows users to earn a BTC yield for aiding in securing the network and also provides new business model opportunities and funding models to developers.

Proof of Elapsed Time (PoET)

geeksforgeeks, Investopedia, Hyperledger

PoET is one of the fairest consensus algorithms and is widely used in permissioned Blockchain networks. Permissioned Blockchain networks require that every network participant to verify their identity before they are allowed to join the network. Unlike PoS and DPoS every validator on the network has an equal

chance to create their own block. So, all the nodes wait for a random period of time and add the proof of their wait in the block that they create, and the created blocks are shared throughout the network for other participants to consider. The block from the winning validator node that gets appended to the blockchain is the one that has the least timer value in the proof part. There are also additional checks in the protocol that ensure nodes do not continually win the election by stopping nodes from getting the lowest timer value.

So, PoET must ensure two key factors to uphold the integrity of the algorithm. First, "It ensures that the participating nodes genuinely select a time that is indeed random and not a shorter duration chosen purposely by the participants to win. Second, it establishes that the winner has completed the waiting time" (Frankenfield, 2022).

The Linux Project along with IBM, Intel and SAP sponsored the Hyperledger Sawtooth project. It is an open-source enterprise level blockchain system that incorporates consensus algorithms like PoET. The project falls under the Hyperledger category which support "global enterprise blockchain project that offers the necessary framework, standards, guidelines, and tools to build open-source blockchains and related applications for use across various industries" (Frankenfield, 2022). These projects include variety of different implementable permissioned networks where nodes have an intrinsic interest in forming a consensus because they are not anonymous.

Proof of Burn (PoB)

Investopedia, medium

Proof of Burn is another consensus mechanism used to verify new blocks on a blockchain. It Is based on users destroying coins, hence the name "burn." It is implemented to avoid the possibility of any coin double spending. This consensus protocol gives block generation power to miners that deem trustworthy for destroying a predetermined number of coins.

When coins are burned, they are not physically destroyed but transferred to a specific account that is visible to all network users. Those coins stored in the public account are unusable without an owner. This can lead to an increase in value to a given coin because of the fact that the algorithm continually withdraws coins from the system and systematically creating scarcity of any coin.

In PoB, the miners invest a portion of their assets that will eventually be destroyed over a period of time to gain trust in the network and eventually validate a new block. The more coins destroyed by a miner proportionately increases the chance that the miner will be selected to verify the new block. To ensure that miners to not take on losses by burning their own coins, PoB networks offer a reward for each new block created (TheLuWizz, 2021). PoB is also economically friendly where it takes minimal energy to destroy coins. PoB networks are also very secure because there is a relatively large investment is required before a miner is authorized to validate a new block, similar to PoW (TheLuWizz, 2021).

Proof of History (PoH)

gitbook, Solana.com, medium

PoH is a sequence of computations that allows users to cryptographically verify the passage of time between two events. "Instead of trusting the timestamp on the transaction, you could prove that the

transaction occurred sometime before and after an event" (*Proof of History* 2019). PoH is a high frequency Verifiable Delay Function (VDF) which requires a certain number of steps in order and produces a unique output that can be "efficiently and publicly verified" (*Proof of History* 2019). PoH uses a cryptographically secure function to ensure that any output cannot be predicted from any given input. The function must also be run successfully and completely in order to yield the output. Other characteristics of the sequential function include that it is run on a single core, its previous output is the current iterations input, as well as the fact that it periodically records the current output and the number of iterations. "The recording of the state, index and data as it was appended into the sequences provides a timestamp that can guarantee that the data was created sometime before the next hash was generated in the sequence" (*Proof of History* 2019).

PoH answers questions like: How do you determine time when there is no single centralized clock? And how do you validate information without a central source of time? Solana solves the issue of needing to move and process transactions quickly through PoH by allowing "timestamps" to be built into the blockchain itself and further knowing the precise time of various activities. Other cryptocurrencies, like ETH, utilize outside sources to assign a "medium" timestamp for transactions which are validated in chronological order (Echter, 2021).

Proof of Capacity (PoC)

geeksforgeeks, Investopedia

PoC is a relatively new consensus algorithm allows miners in a network to use their available hard drive space to determine the mining rights and verify transactions. Many proponents of PoC believe that it is a sound alternative to other major consensus mechanisms and can offer many benefits. Therefore, many supporters of the capability are interested in implementing it into new projects. PoC is a modification of the PoW consensus mechanism because it is faster where it takes PoW about 10 minutes to produce a block while PoC only takes about 4 minutes.

The mining difficulty for validating a new block on the BTC blockchain has significantly increased over the years to the point where only the most powerful computers (ASIC) can solve the hash functions. For the miners that cannot solve the hash in the required amount of time, this means that all the energy invested will be for nothing. Thus, there is an increasing need for PoC because it allows for adequate network decentralization and low energy usage.

The 2 parts to PoC include hard drive plotting and block mining. Plotting is a long process that can take several weeks and is done with the Shabal hash which is a sluggish and hefty cryptocurrency. This makes it perfect for use in PoC cryptos like Burstcoin. "This is due to the fact that the precomputed hashes are stored while still being able to do smaller live verifications. Burst makes use of Shabal256, a 256-bit variant of Shabal. The Shabal hashes are precomputed and saved on a hard drive because they are difficult to calculate" (error_502, 2021).

The hard drive is computed where a list of all potential nonce values is constructed by hashing the data (hashing a miners account continually). Each nonce is made up of 8192 and are all coupled into "scoops" or groups of adjacent hashes. The next part of PoC is the actual mining part where the miners calculate the number of scoops. "For example, if a miner starts mining and creates scoop number 40, the miner would then go to nonce 1's scoop number 40 and utilize the data from that scoop to compute a deadline value" (citation). The miner does this for each nonce stored on the hard drive, calculates all the

deadlines and then chooses the nonce with the lowest deadline. Finally, the miner with the lowest deadline can receive the block reward if no other miner can within the deadline.

Proof of Identity (PoI)

allerin, cryptoslate.com

PoI compares the private key of a network participant with an authorized identity (public key). It is a piece of evidence using a network users private key that is attached to a particular transaction. This process closely resembles one of the learning modules from the Udemy course Blockchain Programming within our signatures class. Ultimately, using this class the user can detect a good signature, flag a bad one, and also flag a bad message through the same process of verifying identities by checking the public and private key pairs attached to a particular transaction. PoI promotes integrity and legitimacy of created data (Joshinav, 2019).

There are many applications to PoI consensus mechanisms. For example, integrating blockchain PoI within smart cities that currently use AI and IoT can solve previous issues concerning security of personal data (Joshinav, 2019). Based on cryptoslate.com there are a variety of cryptocurrencies that utilize PoI mechanisms like Syscoin, Civic, Metadium, and KILT Protocol.

Proof of Authority

blockonomi, allerin

Proof of Authority is a modification of the PoS consensus mechanism where there are not anonymous block producers. The most significant features of Proof of Authority include the low energy requirements and no communication is needed among nodes to reach consensus. Also maintaining the network is irrelevant to the number of nodes on in the network as they are predetermined. Network participants verify their identity through the correlation of their private and public key. Networks that utilize Proof of Authority select about 25 (or less) validators to generate new blocks. These users “stake their reputation on the network” and therefore are incentivized to preserve the integrity and longevity of the network (writer et al., 2018).

3 basic requirements to become a validator for a Proof of Authority network include those identities must be identified in a formal manner and can be cross referenced on some form of public ledger. Also, qualifying and becoming a validator must be difficult to ensure the integrity and longevity of the network. Lastly, there must be a consensus established regarding the decision about who the validators are.

Proof of Authority is currently operational in Ethereum’s Kovan Testnet as well as other well know cryptocurrencies such as Vechain and PulseChain utilize this consensus mechanism. Further the VeChainThor network strives to be an enterprise integratable public network “for the transparent flow of information and tracking, primarily in the supply chain and logistics realm” (writer et al., 2018).

Proof of Activity

allerin, Investopedia

Proof activity is a cross between PoW and PoS and ensures that all transactions on the network are authentic and that all the miners in the network reach a consensus. A proof of activity network works to combine the best aspects from each of the mechanisms like where the mining begins in PoW and then after switching to a PoW basis after mining the new block. Like how other PoW protocols work, mining begins with miners competing to validate the next block. After the new block it found, the system converts to a PoS state and "with the newly found block containing only a header and the miner's reward address" (Seth, 2022). Decred (DCR) is one of the most well-known blockchains actively using the Proof of Activity protocol.

PoW and PoS systems work to counter an attack where a group of network participants obtain control of over 50% of the networks mining computing power. Gaining this amount of control includes being able to "halt new transactions from getting confirmed, stop payments between various blockchain users, and even reverse the transactions completed in the past during their control of the network, allowing them to double-spend (allowing one or a group to reclaim spent coins) the cryptocurrency coins" (Seth, 2022). In Proof of Activity, it is impossible to predict the signing individual would be the owner of a future transaction and it also deters a group from collectively obtaining the majority of the networks computing power.

Works Cited

Cryptopedia Staff. (2021, December). *Proof of stake vs. Delegated Proof of Stake*. Gemini. Retrieved May 5, 2022, from https://www.gemini.com/cryptopedia/proof-of-stake-delegated-pos-dpos

Echter, B. (2021, November 30). *Proof of history: How Solana brings time to crypto*. Solana. Retrieved May 5, 2022, from https://solana.com/news/proof-of-history

error_502. (2021, July 13). *Proof of capacity*. GeeksforGeeks. Retrieved May 5, 2022, from https://www.geeksforgeeks.org/proof-of-capacity/

Frankenfield, J. (2022, February 8). *Proof of elapsed time (poet)*. Investopedia. Retrieved May 5, 2022, from https://www.investopedia.com/terms/p/proof-elapsed-time-cryptocurrency.asp#:~:text=Proof%20of%20elapsed%20time%20(PoET)%20is%20a%20consensus%20mechanism%20often,they%20are%20allowed%20to%20join.

Frankenfield, J. (2022, February 8). *What is Hyperledger?* Investopedia. Retrieved May 5, 2022, from https://www.investopedia.com/terms/h/hyperledger.asp

Frankenfield, J. (2022, March 18). *Proof-of-stake (POS)*. Investopedia. Retrieved May 5, 2022, from https://www.investopedia.com/terms/p/proof-stake-pos.asp

Frankenfield, J. (2022, May 2). *Proof of work (POW)*. Investopedia. Retrieved May 4, 2022, from https://www.investopedia.com/terms/p/proof-work.asp#:~:text=Proof%20of%20work%20(PoW)%20is,transactions%20and%20mining%20new%20tokens

Hooda, P. (2019, January 9). *Proof of work (POW) consensus*. GeeksforGeeks. Retrieved May 5, 2022, from https://www.geeksforgeeks.org/proof-of-work-pow-consensus/

Joshinav. (2019, April 2). *8 blockchain consensus mechanisms you should know about*. Application development. Retrieved May 5, 2022, from https://www.allerin.com/blog/8-blockchain-consensus-mechanisms-you-should-know-about

Joshinav. (2019, January 24). *Making Smart Cities 'Secure' with blockchain: Internet of things*. Application development. Retrieved May 5, 2022, from https://www.allerin.com/blog/making-smart-cities-secure-with-blockchain

Proof of History. Proof of History - consensus. (2019). Retrieved May 5, 2022, from https://tokens-economy.gitbook.io/consensus/chain-based-proof-of-capacity-space/proof-of-history#:~:text=Proof%20of%20History%20is%20a%20sequence%20of%20computation%20that%20can,executed%20to%20generate%20the%20output.

Seth, S. (2022, February 8). *Proof of activity*. Investopedia. Retrieved May 5, 2022, from https://www.investopedia.com/terms/p/proof-activity-cryptocurrency.asp#:~:text=Proof%2Dof%2Dactivity%20(PoA)%20is%20a%20blockchain%20consensus,miners%20arrive%20at%20a%20consensus.

Stacks features and possibilities. Stacks Features and Possibilities. (2022). Retrieved May 5, 2022, from https://www.stacks.co/learn/features#:~:text=Proof%20of%20Transfer%20(PoX)%20is,powers%20without%20modifying%20Bitcoin%20itself.

Techopedia. (2019, January 2). *What is delegated proof of stake (DPoS)? - definition from Techopedia*. Techopedia.com. Retrieved May 5, 2022, from https://www.techopedia.com/definition/33597/delegated-proof-of-stake-dpos#:~:text=Delegated%20proof%20of%20stake%20(DPoS)%20is%20a%20verification%20and%20consensus,transactions%20and%20promote%20blockchain%20organization.

TheLuWizz. (2021, November 2). *What is proof of Burn (POB)?* Medium. Retrieved May 5, 2022, from https://medium.datadriveninvestor.com/what-is-proof-of-burn-pob-e8f7e7dfbbfa

writer, A. B. C. B., Curran, A. B., & writer, B. (2018, July 5). *What is proof of authority consensus? (PoA) staking your identity*. Blockonomi. Retrieved May 5, 2022, from https://blockonomi.com/proof-of-authority/