K.4 Consensus Platforms

Return to DIDO Consensus

Table 1: Crossreference os DIDO Platforms with Alogrithms.

Consensus Algorithm	Platform Examples	Pros	Cons	Type
Cellular Automaton Consensus	*Theoretical*			
Delegated Byzantine Fault Tolerance (dBFT)	NEO	• Generating a new block on the chain takes between 15 and 20 seconds. • The transaction throughput is close to 1,000 TPS. NEO hopes to reach 100,000 TPS, which would allow the network to support large-scale commercial applications. • No expenditure of energy needed (unlike the Proof-of-Work consensus algorithm). • Total finality for transactions after their confirmation. • There are no forks on the NEO blockchain. https://coinrivet.com/delegated-byzantine-fault-tolerance-dbft-explained/	• As delegates need to operate under real identities to be elected, there's no anonymity on the blockchain. • The mechanism requires regulated blockchains, which includes a certain level of centralisation (exactly what blockchains like Bitcoin and Ethereum are trying to achieve). https://coinrivet.com/delegated-byzantine-fault-tolerance-dbft-explained/	
Delegated Proof of Stake (DPoS)	Steem, EOS, BitShares, Steemit, Lisk, Ark	• Scalability and speed: It provides faster processing of transactions than PoW and PoS. This is probably the most meaningful advantage: DPoS makes sense for many applications that require a high level of scalability. • Better distribution of rewards: Theoretically, people will elect only those delegates who give them the most rewards, so everyone, including a casual user, benefits. (This democratization is another aspect supporters cite when noting that DPoS is more decentralized than either PoS or PoW.) • Real-time voting security: Voters can immediately detect malicious actions, and the malicious delegate can be voted out of the system. • Energy efficiency: DPoS consumes significantly less energy than PoW. • Less hardware: Participants don't need costly, specialized equipment. A regular computer is powerful enough. • An incentive to "behave": Block producers — delegates — can be voted out at any time, so the potential for loss of income and reputation provides a hedge against bad behavior. • Flexibility: Because DPoS unlinks the election of block producers from the block production itself, it allows for a more creative and flexible approach to solving problems with either, in isolation, a recent Coinmonks piece explains. It provides a foundation for implementing "interesting governance models in blockchain applications." https://www.verypossible.com/insights/pros-and-cons-of-the-delegated-proof-of-stake-consensus-model	• It's easier to organize an attack: Because fewer people are in charge of keeping the network alive, it's easier to organize a "51 percent" attack. • The rich may get richer: People's vote strength is determined by how many tokens they have, which means that people who own more tokens will influence the network more than people who own very few. • Apathy can kill: Without a large number of engaged users, the system will not function as intended. (That's a bit like any democracy or democratic republic.) • Delegates could form cartels: Delegates can organize into cartels by concentrating the role of validation in a smaller number of hands. This not only makes it less decentralized, but it also makes it less resilient. • This notion that DPoS is not truly decentralized may be the most notable criticism of all. Yes, DPoS is less centralized than some other consensus protocols; nevertheless, power is still concentrated in the hands of a handful of users. DPoS sacrifices decentralization for scalability, critics say. https://www.verypossible.com/insights/pros-and-cons-of-the-delegated-proof-of-stake-consensus-model	Collaborative Consensus
Directed Acyclical Graphs (DAGs)	Iota, HashGraph, Byteball, RaiBlocks/Nano, Obyte	• Highly scalable due to their non-linear structure. • Fast. • Energy-efficient. • Finality is achieved instantly. Webpage: SAINI	• Smart contracts implementation can only be done by use of oracles. Webpage: SAINI	
Fast Probabilistic Consensus (FPC)	*Theoretical*			
Leased Proof of Stake (LPoS)	Waves	• Validate With Less Stake - In a PoS network, the validators are picked based on their stake. That may challenge the fairness of the system where some nodes are chosen repeatedly. With LPoS, you can boost your chances of being picked by accepting a lease from other users. • Earn with Fewer Tokens- LPoS allows minor token holders to earn by leasing their limited tokens to full node owners. Token holders get a percentage from the profit generated by the full node. • Control Over Funds - Leased tokens are locked in the leaser's wallet. They can neither be traded nor transferred. While the leaser can't spend the locked funds, they can decide to stop the lease and make the leased money available for spending. • Fewer Energy Consumptions - A lease transaction can be activated using a phone. A handful of nodes can now do the process that requires multiple nodes with high computing power with the support of phone users. • Higher Processing Speed - LPoS-based systems are fast and efficient since a few nodes are involved in validating a transaction at a given time. LPoS is an excellent alternative to Bitcoin's PoW that makes 4.6 transactions per second. https://www.mycointainer.com/insight/a-complete-guide-to-leased-proof-of-stake-lpos/	• Possible Cartel Formations - Malicious activities can be orchestrated on the LPoS, where members lease to a single full node. This node will always be in front of the validators' pool, giving it an advantage over other nodes. • New Technology Shortcomings - LPoS is still a new technology whose vulnerabilities are not yet fully exposed to help users make sound decisions. It is subject to weaknesses of any new technology such as doubt and lack of regulations that affect adoption. https://www.mycointainer.com/insight/a-complete-guide-to-leased-proof-of-stake-lpos/	
Practical Byzantine Fault Tolerance (pBFT)	Stellar, Ripple, Hyperledger Fabric	Energy efficiency : pBFT can achieve distributed consensus without carrying out complex mathematical computations(like in PoW). Zilliqa employs pBFT in combination with PoW-like complex computations round for every 100th block. • Transaction finality : The transactions do not require multiple confirmations(like in case of PoW mechanism in Bitcoin where every node individually verifies all the transactions before adding the new block to the blockchain; confirmations can take between 10-60 minutes depending upon how many entities confirm the new block) after they have been finalized and agreed upon. • Low reward variance : Every node in the network takes part in responding to the request by the client and hence every node can be incentivized leading to low variance in rewarding the nodes that help in decision making. https://www.geeksforgeeks.org/practical-byzantine-fault-tolerancepbft/	There are two categories of failures that are considered. One is fail-stop(in which the node fails and stops operating) and other is arbitrary-node failure. Some of the arbitrary node failures are given below : • Failure to return a result • Respond with an incorrect result • Respond with a deliberately misleading result • Respond with a different result to different parts of the system https://www.geeksforgeeks.org/practical-byzantine-fault-tolerancepbft/	
Proof of Activity (PoA)	Espers and Decred			Collaborative Consensus
Proof of Authority (PoAuth)	Parity PoA	• High throughput; scalable • No mining mechanism like in PoW, PoA uses identity as the sole verification of the authority to validate, • PoA is suited for both private networks and public networks • PoA only allows non-consecutive block approval from any one validator, meaning that the risk of serious damage is minimized. https://tokens-economy.gitbook.io/consensus/chain-based-hybrid-models/proof-of-authority-poa	• By identifying validators it is a centralized system' https://tokens-economy.gitbook.io/consensus/chain-based-hybrid-models/proof-of-authority-poa	Centralized Consensus
Proof of Burn (PoB)	Slimcoin, TGCoin (Third Generation Coin)	• More sustainable. Reduced power consumption. • No need for mining hardware. Coin burns are virtual mining rigs. • Coin burns reduce the circulating supply (market scarcity). • Encourages long-term commitment by the miners. • Coin distribution/mining tends to be less centralized. https://academy.binance.com/en/articles/proof-of-burn-explained	• Some say that PoB is not really eco-friendly because the Bitcoins being burned are generated through PoW mining, which requires lots of resources. • Not proven to work on larger scales. More testing is needed to confirm its efficiency and security. • The verification of the work done by miners tends to be delayed. It is not as fast as in Proof of Work blockchains. • The process of burning a coin is not always transparent or easily verifiable by the average user. https://academy.binance.com/en/articles/proof-of-burn-explained	
Proof of Capacity (PoC)	Burstcoin and SpaceMint, IPFS	• Similar to PoW but uses space instead of computation. Thus much environmental friendly. • Can be used for malware detection, by determining whether the L1 cache of a processor is empty (e.g., has enough space to evaluate the PoSpace routine without cache misses) or contains a routine that resisted being evicted. • Can be used for anti-spam measures and denial of service attack prevention. • PoC can use any regular hard drives including those with Android-based systems. • It is reportedly up to 30-times more energy efficient than the ASIC-based mining of the bitcoin cryptocurrency. • There is no need for dedicated hardware or constant upgrading of hard drives. • Mining data can be easily wiped off and the drive can be reused for any other data storage purpose. https://www.investopedia.com/terms/p/proof-capacity-cryptocurrency.asp	• Not many developers have adopted the system. • It is possible for malware to affect mining activities. • Widespread adoption of PoC could start an "arms race" to produce higher capacity hard drives. https://www.investopedia.com/terms/p/proof-capacity-cryptocurrency.asp	Collaborative Consensus
Proof of Elapsed Time (PoET)	Hyperledger Sawtooth, Resource-Efficient Mining (REM)	PoET is a substantial improvement in the efficiency of proof of work systems. Simultaneously, it also provides a great solution to the "Random Leader Selection Problem" without being resource-intensive or requiring complex staking mechanics and incentive structures necessary with proof of stake consensus. • PoET is also an excellent consensus mechanism for permissioned networks, which is why it is the go-to consensus mechanism for Hyperledger Sawtooth. On top of that, it scales efficiently and can be used as a "plug and play" model for testing environments with Hyperledger Sawtooth. https://blockonomi.com/proof-of-elapsed-time-consensus/	• Software Guard Extensions (SGX) is a lauded and innovative technology, but recent developments are clearly a cause for concern regarding its use with PoET consensus. Intel will likely be able to fix the issue regarding the critical vulnerability, but the disadvantage here is the obvious and necessary reliance on specialized hardware's security. • Not only that, but Software Guard Extensions (SGX) is manufactured entirely by Intel, so the reliance on the consensus model extends to Intel as a company, a third party. The notion of such a reliance runs against the new paradigm that cryptocurrencies are attempting to achieve with blockchain networks, the removal of trust in intermediaries. https://blockonomi.com/proof-of-elapsed-time-consensus/	

Consensus Algorithm	Platform Examples	Pros	Cons	Type
Proof of Importance (PoI)	NEM	• NEM is overall improved by writing the code completely from scratch in Java: It can handle 3000 transactions per second, while only 3 to 4 transactions can be processed per second in Bitcoin. • Introduces "namespace": Namespace is like a Domain Name System (DNS) that can be used to create a unique place and subdomains for businesses. • Use the new Proof of Importance(PoI) algorithm: Compared with Proof of Work depending totally on hardware mining abilities, this algorithm takes into account how many transactions are made and the total token amount in an address. This incentivizes coin holders to carry out transactions, which helps the growth of the network in the long term. • Have a special messaging feature. No XEM needs to be sent in order for a message to be sent. The transaction fee of sending a message is also calculated in a different way(low cost compared to traditional messages that can be added in a block). For unencrypted messages, it charges 1 XEM for every 32 characters while the price for encrypted messages varies. • Has its own wallet (the Nano wallet, simply click and download). It can be set up quite simple and fast(uses your browser window to open the wallet), but still not that user-friendly for the general public. (A quick demo video) • Everyone having 10000 XEM can start mining(called "delegated harvesting"): This incentivizes regular users to contribute to the network. All these harvests can be done within the Nano Wallet. Only a normal computer is needed to start mining. https://medium.com/taipei-ethereum-meetup/pros-cons-of-the-top-10-cryptocurrencies-in-market-cap-you-need-to-know-ii-ad35e4a43c37	• The official website is still not easily understandable for standard users. Mass adoption is less likely to happen if people are not well educated with NEM's features. • As Ethereum is widely accepted and has no significant drawbacks now, it is hard to see people switching to NEM. The number of users is something to concern about.(I personally will stick to Ethereum for development, but will keep an eye on NEM.) https://medium.com/taipei-ethereum-meetup/pros-cons-of-the-top-10-cryptocurrencies-in-market-cap-you-need-to-know-ii-ad35e4a43c37	
Proof of Stake (PoS)	Ethereum, Dash, Peercoin, Decred, Reddcoin, PivX, NEO Project, Zcoin, Tezos	• Energy efficient • Low barrier to entry (no expensive investment in hardware is required) • PoS cryptocurrencies are generally faster than PoW cryptocurrencies https://coincodex.com/article/7142/what-is-proof-of-stake/	• Unproven in terms of long-term sustainability • Users who wold a large amount of coins can have an outsized influence on the consensus process https://coincodex.com/article/7142/what-is-proof-of-stake/	Competitive Consensus
Proof of Weight (PoW)	Algorand, Filecoin, Chia	• Energy efficient.Webpage: SAINI • Highly Customisable and scalable.Webpage: SAINI	• Incentivization can be hard.Webpage: SAINI	Competitive Consensus
Proof of Work (PoW)	Bitcoin, Litecoin, ZCash, Primecoin, Monero, Vertcoin	• Proof of work models make blockchain networks more difficult and costly to attack. • Proof of work models reward miners with both a block reward and a share of transaction fees. • Proof of work models often results in more decentralized networks. • Less opportunity for 51% attack • Better Security https://blockdaemon.com/blog/proof-of-work-vs-proof-of-stake-whats-the-difference/	• Require access to significant (and increasing) computational power, much of which is wasted each time an equation is solved. • Demand excessive energy consumption, leading to increased costs and environmental impacts. • Result in long-term disincentives to mining as newly minted cryptocurrencies near the cap. • Centralization of Miners https://blockdaemon.com/blog/proof-of-work-vs-proof-of-stake-whats-the-difference/	Competitive Consensus

☐ [char] Do general review of this page
☐ [char] Decide if it's worthwhile to fix the unordered lists so they look better in pdfexport