

Tech corner

When analyzing different protocols one often comes with the discussion of which Consensus Algorithm it uses. No consensus algorithm is perfect, but they each have their strengths. In the world of crypto, consensus algorithms exist to prevent *double spending*.

There are many different Consensus Algorithms and we will try to briefly explain the most used ones in today's crypto community.

Consensus Algorithms	Description	Pros	Cons	Protocols
POW (Poof-of-Work)	Is the first blockchain consensus algorithm. In PoW, miners solve hard, useless problems to create blocks. PoW runs on a system of "the longest chain wins." So assuming most miners are working on the same chain, that one will grow fastest will be the longest and most trustworthy.	It works	Slow throughput, energy inefficient	BTC, ETH (*), LTC
POS (Proof-of-stake)	The blocks aren't created by miners doing work, but by minters staking their tokens to "bet" on which blocks are valid. In the case of a fork, minters spend their tokens voting on which fork to support. Assuming most people vote on the correct fork, validators who voted on the wrong fork would "lose their stake" in the correct one.	Energy efficient, attacks more expensive, more d ecentralized	Nothing at stake	DCR
DPOS (Delegated Proof-of-Stake)	Token hodlers don't vote on the validity of the blocks themselves, but vote to elect delegates to do the validation on their behalf. There are generally between 21-100 elected delegates in a DPoS system. The delegates are shuffled periodically and given an order to deliver their blocks in. Having few	Cheap transactions, scalable, energy efficient	Partially centralized	EOS, Steemit, BitShares

	delegates allows them to organize themselves efficiently and create designated time slots for each delegate to publish their block. If delegates continually miss their blocks or publish invalid transactions, the stakers vote them out and replace them with a better delegate.			
POA (Proof-of-Authority)	Transactions are validated by approved accounts, kind of like the “admins” of the system. These accounts are the authority that other nodes receive their truth from. PoA has high throughput, and is optimized for private networks. You’re unlikely to see PoA running on a public chain due to its centralized nature.	High throughput, scalable	Centralized	POA Network
PoWeight (Proof-of-Weight)	Is a broad classification of consensus algorithms based around the Algorand consensus model. The general idea is that where in PoS, your percentage of tokens owned in the network represents your probability of “discovering” the next block, in a PoWeight system, some other relatively weighted value is used.	Customizable, scalable	Incentivation can be challenging	Filecoin
BFT (Byzantine Fault Tolerance)	There’s this classic problem is distributed computing that’s usually explained with Byzantine generals. The problem is that several Byzantine generals and their respective portions of the Byzantine army and have surrounded a city. They must decide in unison whether or	High throughput, low cost, scalable	Semi-trusted	XLM XRP Hyper-ledger

not to attack. If some generals attack without the others, their siege will end in tragedy. The generals are usually separated by distance and have to pass messages to communicate. Several cryptocurrency protocols use some version of BFT to come to consensus, each with their own pros and cons.

(*) ETH is in the process of changing from POW to POS in the coming months.