Variants of **Proof-of-Stake**, Importance of Building a Secure **Validator** & **Delegator** Set

By @awasunyin

CONTENTS

- Motivations
- Proof-of-X ≠ Consensus Algorithm
- "Nothing-at-stake problem"
- Chain-based PoS vs. BFT PoS
  - Examples of Chain-based PoS
  - Examples of BFT PoS
- The role of token holders

MOTIVATIONS

- First Proof-of-Stake networks appearing and many to come in 2019
- Test the protocols with real validator sets and token holders
- Will PoS achieve the goals that it promised?
  - E.g. substituting PoW a and increasing the scalability of blockchains? At what cost?
- Requires and encourages higher involvement of its token holders, as validators or delegators

Consensus Algorithm ≠ Proof-of-X

Consensus Alg.
Mechanisms that enable trust-less peers to agree on a specific state of values

Proof-of-X
Mechanisms that determine what peers are eligible to participate in consensus

Nakamoto Consensus

The chain with the largest pool of electricity or longest is the canonical one

Byzantine-Fault Tolerant Consensus

Latest block with more than 2/3 of the validator set's signatures

Proof-of-Work

Compete with other nodes to solve the computational puzzle or find the nonce for the next block

Proof-of-Stake

Allocate the required amount of value as a collateral, which can be lost when deviating from the protocol

The Nothing-At-Stake Problem

- Deviating from the protocol, by e.g. causing and maintaining multiple forks, *at no cost*
- Present in PoS variants from commercial and academic projects
- One of the most commercialised projects:
  - Delegated Proof-of-Stake
  - Used in e.g. Bitshares, EOS
- Assumes that if one of the active block producers (top 21 by votes) deviates, it will not get voted again

Variants of **Proof-of-Stake**

Liquid PoS (LPoS)	**Bonded** PoS (BPoS)	**Nominated** PoS (NPoS)	**Casper FFG**
e.g. Tezos	e.g. Cosmos Hub	e.g. Polkadot	e.g. Ethereum

Variants of **Proof-of-Stake**

Liquid PoS (LPoS)

e.g. Tezos

Bonded PoS (BPoS)

e.g. Cosmos Hub

Nominated PoS (NPoS)

e.g. Polkadot

Casper FFG

e.g. Ethereum

Nakamoto Consensus

BFT Consensus

Hybrid PoW + BFT PoS

	Liquid PoS (LPoS)
Consensus Mechanism?	Nakamoto Consensus
Who is allowed to participate?	10,000 XTZ self-bonded
How is leader elected?	Pseudorandom assignment of slots
What is at stake?	*Bakers'* self-bond, rewards
What are the slashing conditions?	Double-signing Double-baking
What are the rewards?	Baking + fees Endorsements
How often does the validator set change?	Every cycle (2-3 natural days)

	Liquid PoS (LPoS)	**Cosmos** PoS (BPoS)	**Nominated** PoS (NPoS)
Consensus Mechanism?	Nakamoto Consensus	Tendermint Consensus	Tendermint, HoneyBadgerBFT
Who is allowed to participate?	10,000 XTZ self-bonded	Top 100 by economic stake	Sufficiently high bond deposited
How is leader elected?	Pseudorandom assignment of slots	Weighted Round-Robin	- Every quarter
What is at stake?	*Bakers'* self-bond, rewards	Self-bond, delegation, rewards	Self-bond, rewards
What are the slashing conditions?	Double-signing Double-baking	Double-signing Liveness	Double-signing Liveness
What are the rewards?	Baking + fees Endorsements	Validation rewards + fees	Validation rewards + fees
How often does the validator set change?	Every cycle (2-3 natural days)	Recalculated at end of every block	-

	Liquid PoS (LPoS)	**Cosmos** PoS (BPoS)	**Nominated** PoS (NPoS)	**Casper FFG**
Consensus Mechanism?	Nakamoto Consensus	Tendermint Consensus	Tendermint, HoneyBadgerBFT	Hybrid Consensus
Who is allowed to participate?	10,000 XTZ self-bonded	Top 100 by economic stake	Sufficiently high bond deposited	Any (voting power proportional)
How is leader elected?	Pseudorandom assignment of slots	Weighted Round-Robin	- Every quarter	Round-Robin (?)
What is at stake?	*Bakers'* self-bond, rewards	Self-bond, delegation, rewards	Self-bond, rewards	The entirety of the self-bond
What are the slashing conditions?	Double-signing Double-baking	Double-signing Liveness	Double-signing Liveness	Double-signing Double-voting
What are the rewards?	Baking + fees Endorsements	Validation rewards + fees	Validation rewards + fees	- Finder fee
How often does the validator set change?	Every cycle (2-3 natural days)	Recalculated at end of every block	-	Dynamically (*Dynasties*)

The Role of Token Holders

- *Hodling* is economically discouraged
- PoS Networks introduce two new stakeholders into the ecosystem:
  - **Validators**: participate directly in consensus
  - **Delegators**: participate indirectly

- On-Chain Governance
  - In some networks only validators will have voting power proportional to their total stake
  - In others, delegators have the power to overwrite the vote of the validators

The **security** & **decentralisation** of these networks rely on the decisions of token holders, be it **by validating or delegating**

– *Letter to Current & Future Delegators* (Link)

Resources

- Larimer, D. (2014). Delegated proof-of-stake (dpos). Bitshare whitepaper.
- Goodman, L. M. (2014). Tezos—a self-amending crypto-ledger White paper. URL: https://www.tezos. com/static/papers/white_paper. pdf.
- Kwon, J. (2014). Tendermint: Consensus without mining. Draft v. 0.6, fall.
- Wood, G. (2016). Polkadot: Vision for a heterogeneous multi-chain framework. White Paper.
- Buchman, E., Kwon, J., & Milosevic, Z. (2018). The latest gossip on BFT consensus. arXiv preprint arXiv:1807.04938.
- Arluck, Jacob (2018). Liquid Proof-of-Stake. URL: https://medium.com/tezos/liquid-proof-of-stake-aec2f7ef1da7
- Cosmos latest testnet parameters: https://github.com/cosmos/cosmos-sdk/blob/develop/x/slashing/params.go#L61
- Buterin, V., & Griffith, V. (2017). Casper the friendly finality gadget. arXiv preprint arXiv:1710.09437.
- Dwork, C., Lynch, N., & Stockmeyer, L. (1988). Consensus in the presence of partial synchrony. Journal of the ACM (JACM), 35(2), 288-323.
- Brown-Cohen, J., Narayanan, A., Psomas, C. A., & Weinberg, S. M. (2018). Formal Barriers to Longest-Chain Proof-of-Stake Protocols. arXiv preprint arXiv:1809.06528.

How to Reach Out

- **Slides** will be available github.com/cryptiumlabs/library
- **Website**: cryptium.ch | tezos.cryptium.ch
- **Twitter**: @CryptiumLabs | @awasunyin
- **Email**: awa@cryptium.ch