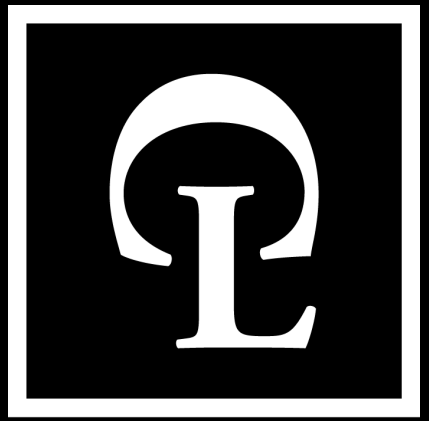


Variants of Proof-of-Stake & Importance of Building a **Strong Validator & Delegator Set –**

By Awa Sun Yin **@awasunyin**

About Me & Cryptium Labs

- Founder @ Cryptium Labs
- Main research topics: Consensus, Proof-of-Stake, and Security
- Network agnostic validator, supporting any *reasonable* protocol
- Development & Research
- Community Development (validators and delegators side)

Consensus Algorithm ≠ Proof-of-X

Consensus Alg.
Mechanisms that enable 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 *work* or heaviest 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

Nodes can cause and maintain forks at no cost

Example

- Present in PoS variants from commercial and academic projects
- Commercialised projects:
  - Delegated Proof-of-Stake (DPoS)
  - 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**
- Is it a plausible assumption?

Security of Your Application

The risk of using NASP protocols as infrastructure for your dApp

Variants of **Proof-of-Stake**

Liquid PoS (LPoS)	**Bonded** PoS (BPoS)	**Nominated** PoS (NPoS)	**Casper**
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

e.g. Ethereum

Nakamoto Consensus (Heaviest Chain Consensus)

BFT Consensus

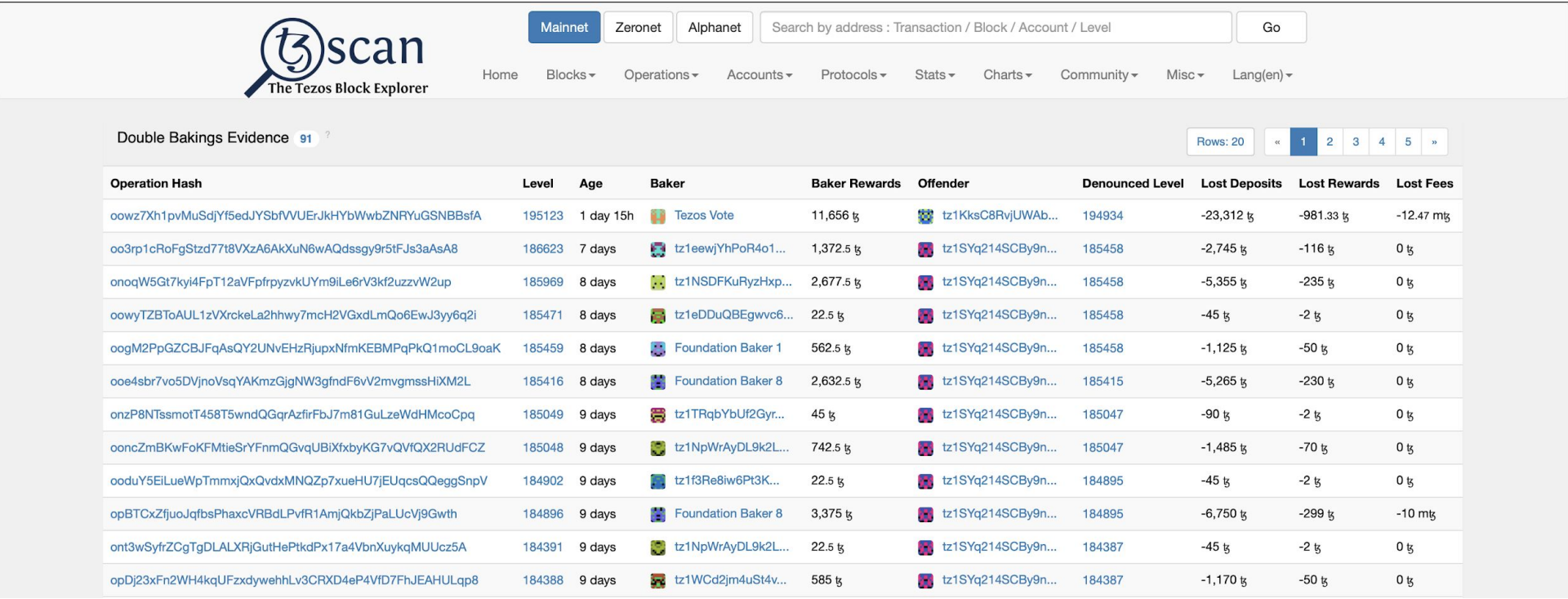
Hybrid Nakamoto + BFT Consensus

A Note on **Finality Gadgets**

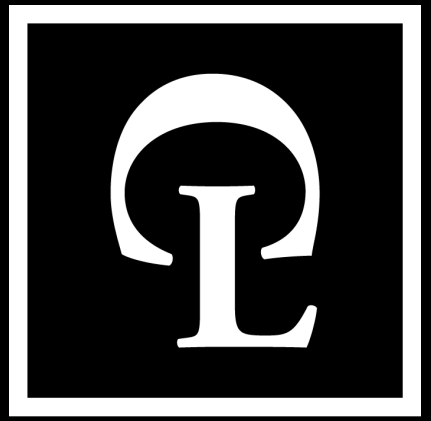
Beacon chain, layer on top of existing chain to enable finality

	LPoS (Tezos)	**BPoS (Cosmos)**
Consensus Mechanism?	Nakamoto Consensus	Tendermint Consensus
Who is allowed to participate?	10,000 XTZ self-bond	Top 100 by economic stake
How is leader elected?	Pseudorandom assignment of slots (based on staking balance)	Weighted Round-Robin
What is at stake?	*Bakers*' self-bond, reward, fees	Self-bond, delegation, rewards
What are the slashing conditions?	Double-baking (- 512 XTZ/slot) Double-endorsing (- 64 XTZ/slot)	Double-signing (- 50%) Liveness (- 1%)
What are the rewards?	Baking + fees Endorsements, denunciations	Validation rewards + fees
Annual Inflation %	~5.51%	~7-20%
How often does the validator set change?	Every cycle (2-3 natural days)	Recalculated at end of every block

Proof-of-Stake in Action



Operation Hash	Level	Age	Baker	Baker Rewards	Offender	Denounced Level	Lost Deposits	Lost Rewards	Lost Fees
oowz7Xh1pvMuSdjYf5edJYSbfVVUErJkHYbWwbZNRYuGSNBBsfA	195123	1 day 15h	Tezos Vote	11,656 ꜩ	tz1KksC8RvjUWAb...	194934	-23,312 ꜩ	-981.33 ꜩ	-12.47 mꜩ
oo3rp1cRoFgStzd77t8VXzA6AkXuN6wAQdssgy9r5tFJs3aAsA8	186623	7 days	tz1eewjYhPoR4o1...	1,372.5 ꜩ	tz1SYq214SCBy9n...	185458	-2,745 ꜩ	-116 ꜩ	0 ꜩ
onoqW5Gt7kyi4FpT12aVFpfrpyzvkUYm9iLe6rV3kf2uzzvW2up	185969	8 days	tz1NSDFKuRyzHxp...	2,677.5 ꜩ	tz1SYq214SCBy9n...	185458	-5,355 ꜩ	-235 ꜩ	0 ꜩ
oowyTZBToAUL1zVXrckeLa2hhwy7mcH2VGxdLmQo6EwJ3yy6q2i	185471	8 days	tz1eDDuQBEgwvc6...	22.5 ꜩ	tz1SYq214SCBy9n...	185458	-45 ꜩ	-2 ꜩ	0 ꜩ
oogM2PpGZCBJFqAsQY2UNvEHzRjupxNfmKEBMPqPkQ1moCL9oaK	185459	8 days	Foundation Baker 1	562.5 ꜩ	tz1SYq214SCBy9n...	185458	-1,125 ꜩ	-50 ꜩ	0 ꜩ
ooe4sbr7vo5DVjnoVsqYAKmzGjgNW3gfndF6vV2mvgmssHiXM2L	185416	8 days	Foundation Baker 8	2,632.5 ꜩ	tz1SYq214SCBy9n...	185415	-5,265 ꜩ	-230 ꜩ	0 ꜩ
onzP8NTssmotT458T5wndQGqrAzfirFbJ7m81GuLzeWdHMcoCpq	185049	9 days	tz1TRqbYbUf2Gyr...	45 ꜩ	tz1SYq214SCBy9n...	185047	-90 ꜩ	-2 ꜩ	0 ꜩ
ooncZmBKwFoKFMtieSrYFnmQGvqUBiXfxbyKG7vQVfQX2RUdFCZ	185048	9 days	tz1NpWrAyDL9k2L...	742.5 ꜩ	tz1SYq214SCBy9n...	185047	-1,485 ꜩ	-70 ꜩ	0 ꜩ
ooduY5EiLueWpTmmxjQxQvdxMNQZp7xueHU7jEUqcsQQeggSnpV	184902	9 days	tz1f3Re8iw6Pt3K...	22.5 ꜩ	tz1SYq214SCBy9n...	184895	-45 ꜩ	-2 ꜩ	0 ꜩ
opBTCxZfjuoJqfbsPhaxcVRBdLPvfR1AmjQkbZjPaLUcVj9Gwth	184896	9 days	Foundation Baker 8	3,375 ꜩ	tz1SYq214SCBy9n...	184895	-6,750 ꜩ	-299 ꜩ	-10 mꜩ
ont3wSyfrZCgTgDLALXRjGutHePtkdPx17a4VbnXuykqMUUcz5A	184391	9 days	tz1NpWrAyDL9k2L...	22.5 ꜩ	tz1SYq214SCBy9n...	184387	-45 ꜩ	-2 ꜩ	0 ꜩ
opDj23xFn2WH4kqUFzxdywehhLv3CRXD4eP4VfD7FhJEAHULqp8	184388	9 days	tz1WCd2jm4uSt4v...	585 ꜩ	tz1SYq214SCBy9n...	184387	-1,170 ꜩ	-50 ꜩ	0 ꜩ



The Role of Tezos Token Holders in PoS Networks

Validators

Token holders who operate a validating node and participate in consensus

Delegators

Token holders who participate indirectly in consensus by delegating their validating rights

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)

How to Reach Out

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