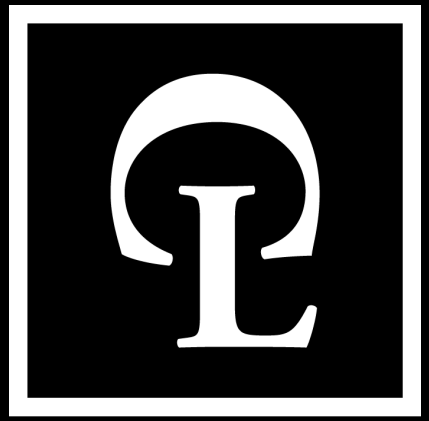



# Introduction to **Cryptium Labs** –

By Awa Sun Yin **@awasunyin**

# I. Proof-of-Stake will be an alternative to Proof-of-Work

# II. There will be many chains, and one ecosystem

# Cryptium Labs

Validation

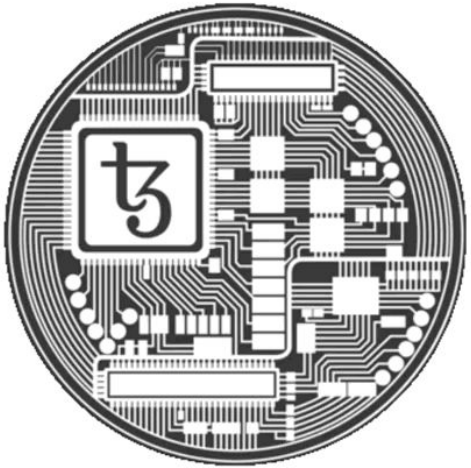
Development
Research

Community

# Cryptium Labs

Infrastructure operator for Proof-of-Stake (PoS) public blockchains

## Supported Networks



### Tezos (XTZ)

The Self-Amending Crypto-Ledger

Validating since July 2018

Networks Projects About

# Projects

Cryptium Labs' open-source projects


Bäckerei

Automated Rewards Payment Manager for Tezos Bakers Written in Haskell

View Code Read Article

Why GitHub? Business Explore Marketplace Pricing Search

## Cryptium Labs

Secure and highly available cryptographic keys for on-demand signatures.

Decentralised https://cryptium.ch hello@cryptium.ch

Repositories 2 People 0 Projects 0

**Grow your team on GitHub**

GitHub is home to over 28 million developers working together. Join them to grow your development teams, manage permissions, and collaborate on projects.

Sign up

Pinned repositories

**library**

This repository is used as an open library for the blockchain community. We include letters, papers, analysis, blogposts, etc, for anyone to use.

★ 13 3

**backerei**

Automated Rewards Payment Manager for Tezos Bakers Written in Haskell

Haskell ★ 21 3

Find a repository... Type: All Language: All

**library**

This repository is used as an open library for the blockchain community. We include letters, papers, analysis, blogposts, etc, for anyone to use.

blockchain consensus proof-of-stake cryptoeconomics tezos

★ 13 3 Updated 5 hours ago

Top langu

Haskell

Most use

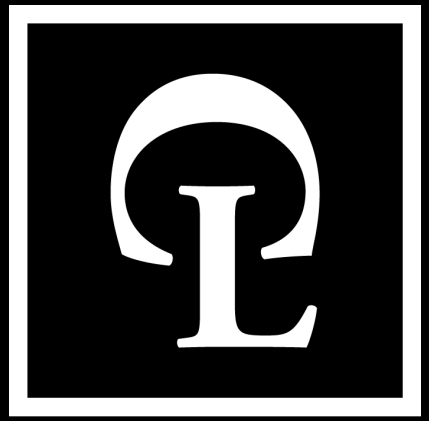
proof-of


ESPAÑOL CHINESE | OFFICIAL WEBSITE

Latest


## Half-Baked is Always Better than Double-Baked — ...

Many of you have seen on Reddit or




# Introduction to **Proof-of-Stake Algorithms**

# 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 electricity 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

- 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** |
| --- | --- | --- | --- |
| 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)

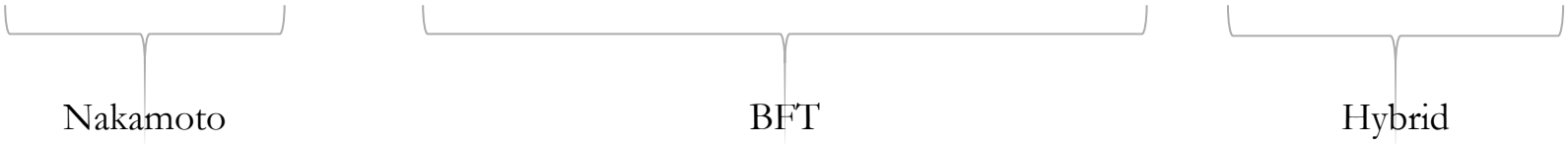
e.g. Cosmos Hub

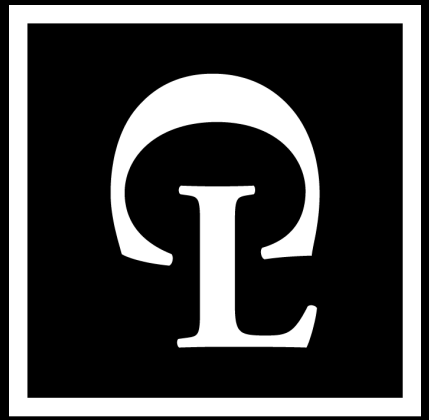
**Nominated** PoS (NPoS)

e.g. Polkadot

**Casper**

e.g. Ethereum






# Liquid Proof-of-Stake (LPoS)

**Bakers**

Tezos token holders who operate a validating node and participate in consensus

**Delegators**

Tezos token holders who participate indirectly in consensus by delegating their baking rights to bakers

# Bakers: What are they?

- Are in charge of maintaining the Tezos network active by producing blocks and endorsements
- Must have a minimum of 10,000 XTZ in self-bond
- Solo-bakers & Public Baking Services
- Are incentivised to operate **secure** validating nodes
- Have voting power for protocol upgrades

# Bakers: What are the Rewards?

- 64 XTZ / baked block
- 1 or 2 XTZ / endorsed block
- Transaction fees
- Every 10,000 XTZ = 1 Roll
- More rolls → Higher chance to receive baking and endorsement slots

# Bakers: What are the Risks?

- Safety-Faults:
  - Double-baked block: -512 XTZ/block
  - Double-endorsed block: -64 XTZ
  - - rewards and fees locked in the security deposits
- Liveness: Missing rewards
- Overdelegation: How to increase the self-bond?

# Bakers: Double-Baking Examples

tzscan The Tezos Block Explorer

Mainnet | Zeronet | Alphanet | Search by address : Transaction / Block / Account / Level | Go

Home | Blocks | Operations | Accounts | Protocols | Stats | Charts | Community | Misc | Lang(en)

Double Bakings Evidence 91

Rows: 20 « 1 2 3 4 5 »

| 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 |

# Delegators: Who are they?

- They own XTZ
- They do not want to operate a baker
- They are incentivised to at least delegate to bakers, so they can receive rewards
- They must trust the baker they choose to delegate to
- They can change bakers anytime
- They generate delegation smart contracts (and maintain custody)

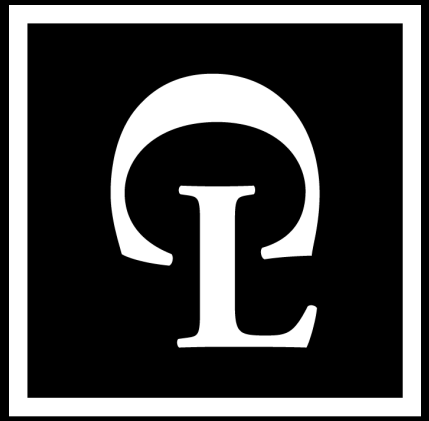
# Delegators: Risks and Rewards

- Delegations are not at stake but they must **trust** that their bakers will pay the rewards correctly and on time
- Opportunity cost when not switching quick enough when a baker closes
- Receive a portion of the rewards generated by the baker
- Normally pay a % in service fees to the baker

# Solo-baking vs Public Baker vs Delegating

| **Average Rewards for 1 Cycle** | **10,000 XTZ** | **100,000 XTZ** | **1,000,000 XTZ** |
|---|---|---|---|
| Solo-Baking | 7.9778 | 79.7780 | 797.7796 |
| Public Baker * | 16.71 | 168.52 | 1683.76 |
| Delegating * | 6.89 | 68.89 | 688.85 |

* 10% fee
** 50% revenue share
Find the detailed numbers and calculations here: https://medium.com/cryptium




# The Role of Tezos (XTZ) Token Holders

# 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