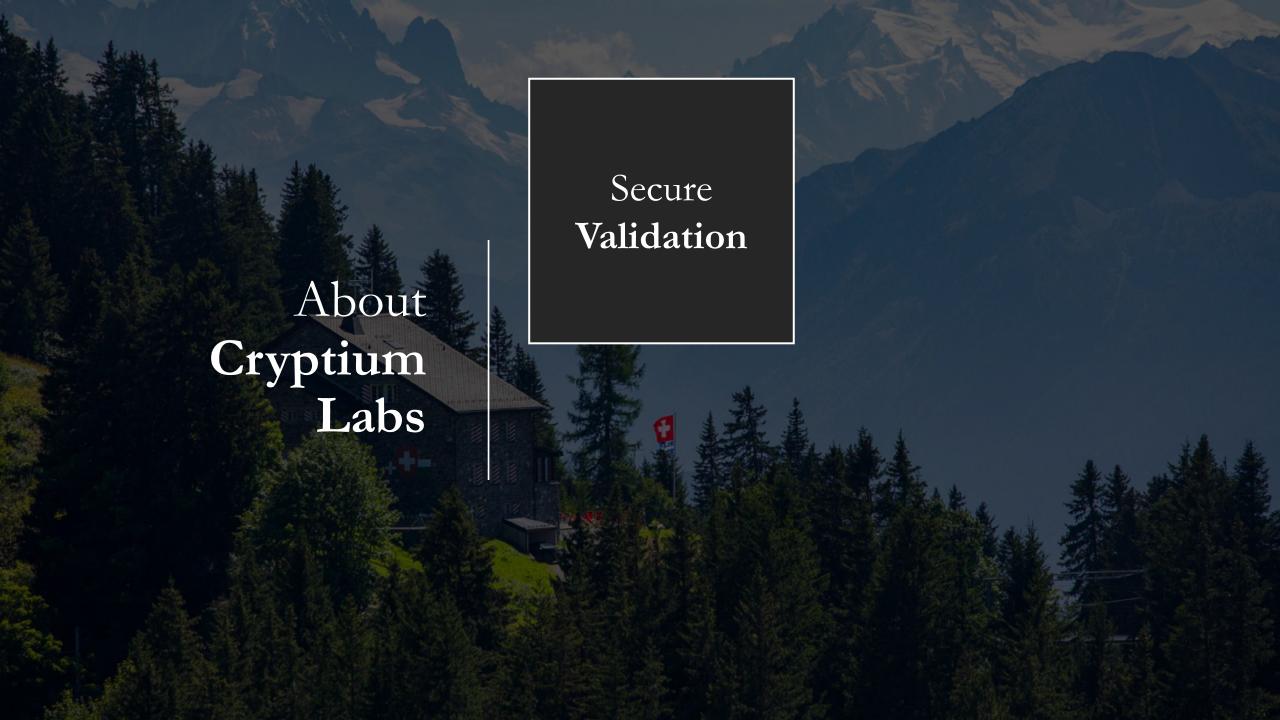
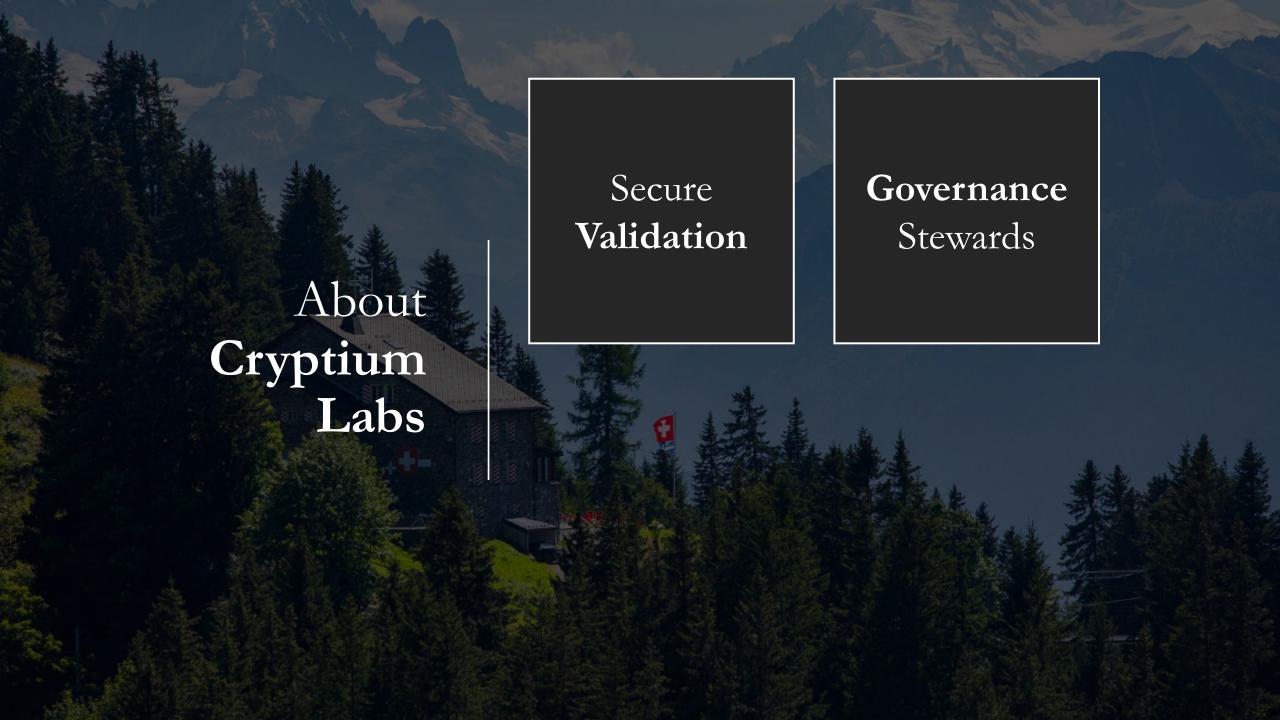


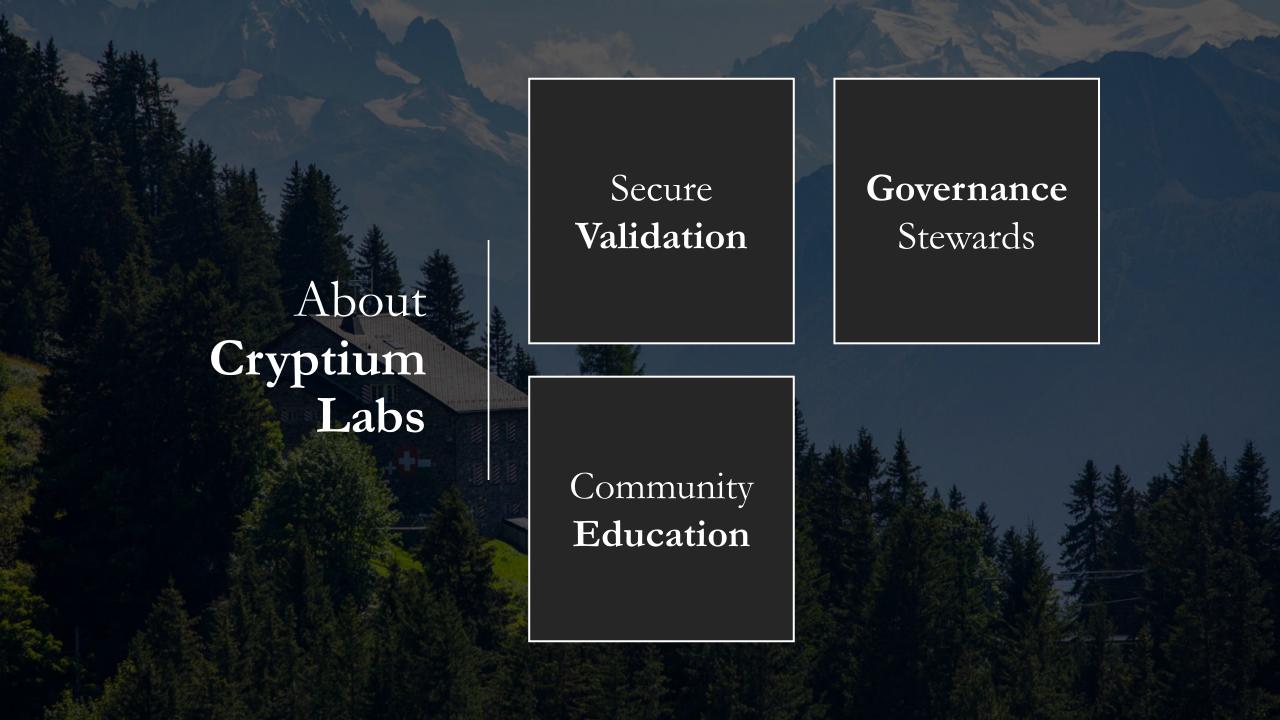
Salut, Paris!
A bit about myself...

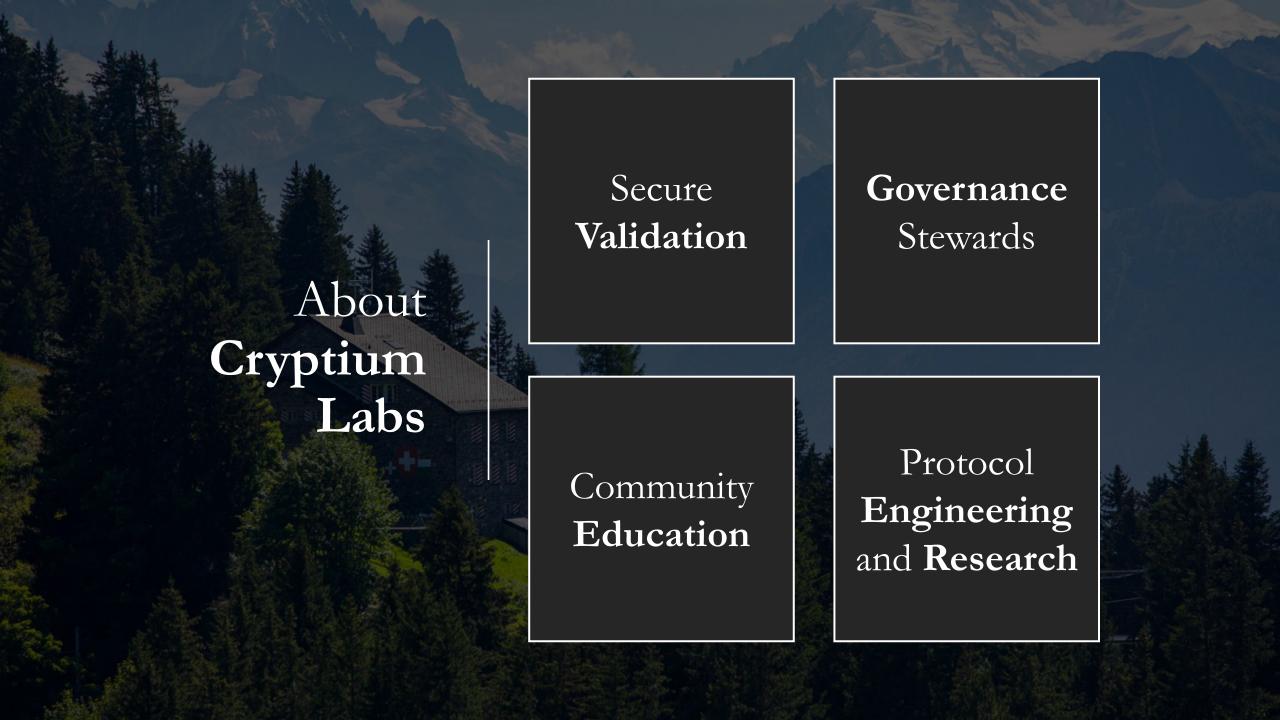
- Founder @Cryptium Labs
- Researcher @ Cosmos
- Data Scientist &Software Engineer@ Chainalysis

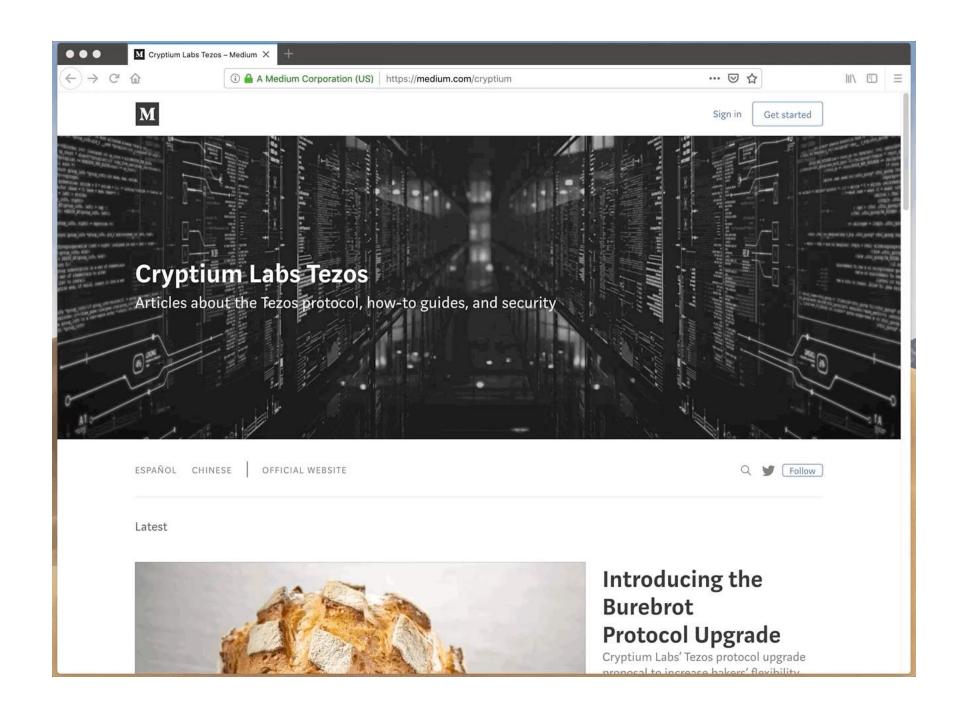
















AGENDA

1 RE-visiting Basic Concepts

2 Some Variants of PoS

A Comparison of Economic Mechanisms

5 Q&A

Mechanisms



Introduction & Variants of PoS

(a) awasunyin

1. Re-Visiting Basic Concepts

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 of NASP

- Present in PoS variants from commercial and academic projects
- Commercialised projects:
 - Delegated Proof-of-Stake (DPoS)
 - Used in e.g. EOS

- Assumes that if one of the active block producers (top 21 by votes)
 deviates, it will not get voted
 again
- Is it a fair assumption?

Security of Your Application

The risk of using NASP protocols as infrastructure for your dApp

Block Production # Finality

You might have one system for block production and an additional system for achieving finality

A Note on Finality Gadgets

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

2. Some Variants of PoS

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

Variants of **Proof-of-Stake**

Liquid PoS (LPoS)

e.g. Tezos

Nakamoto Consensus **Bonded** PoS

(BPoS)

e.g. Cosmos

Hub

BFT Consensus

Nominated

PoS (NPoS)

e.g. Polkadot

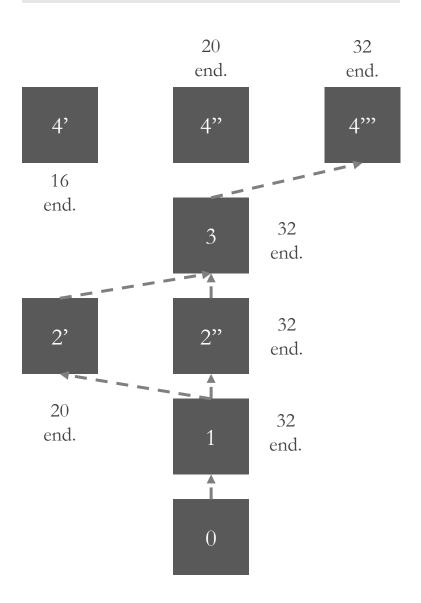
Casper FFG

e.g. Ethereum

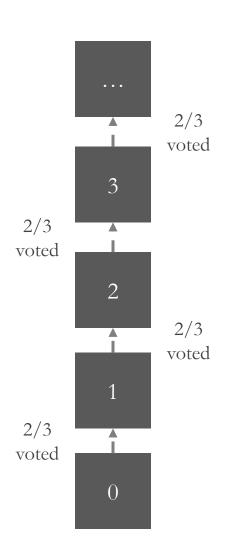
Hybrid Nakamoto + BFT Consensus

3. Comparing Consensus

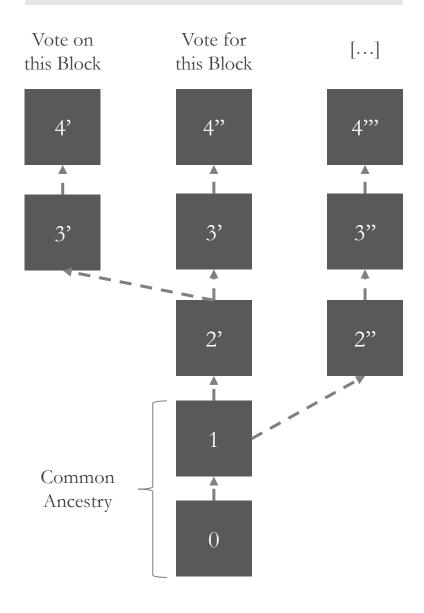
Tezos (Emmy, Nakamoto)



Cosmos (Tendermint Consensus)



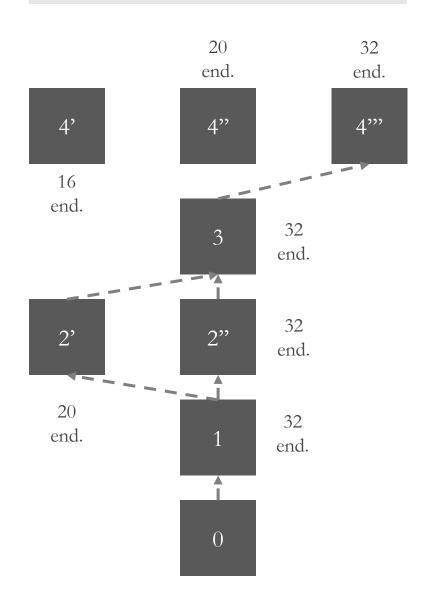
Polkadot (Al's Finality Gadget)

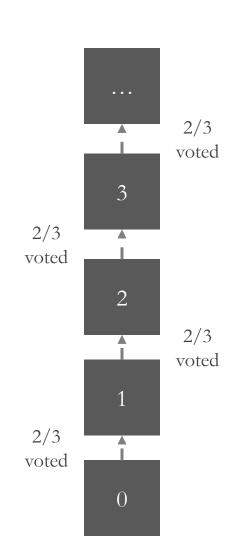


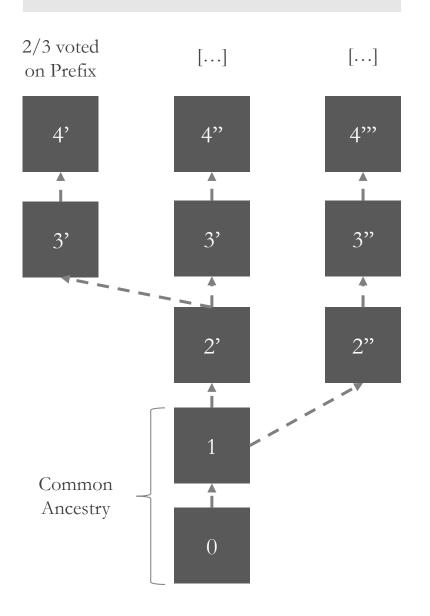
Tezos (Emmy, Nakamoto)

Cosmos (Tendermint Consensus)

Polkadot (Al's Finality Gadget)







4. Comparing Economic Models

	Tezos LPoS	Cosmos BPoS	Polkadot NPoS
Requirement to Participate	10,000 XTZ (8,000 XTZ)		
Rights' Assignment	Pseudorandom by Stake and Priority List		
Inflation	5.51%/Year when 60s. block times & all blocks in priority 0		
Other Rewards	Accusations (50% of amount to validator)		
Safety Slashing Conditions	Security Deposits for the entire cycle in the worst case		
Liveness Slashing	Missing the Rewards		

	Tezos LPoS	Cosmos BPoS	Polkadot NPoS
Requirement to Participate		Top 100 by Stake	
Rights' Assignment		Round-Robin by Stake	
Inflation		7-20% Adaptive to Global Stake	
Other Rewards		Double-Voting evidences (rewards shared among all validators)	
Safety Slashing Conditions		5% of Total Stake (Self-Bond and Delegations) + Execution	
Liveness Slashing		Jailing Time (~7 days)	

	Tezos LPoS	Cosmos BPoS	Polkadot NPoS
Requirement to Participate			_
Rights' Assignment			Pseudorandom and all validators have equal weights
Inflation			_
Other Rewards			Fishermen (not necessarily validators)
Safety Slashing Conditions			Self-Bond will be slashed before Delegations 1% for uncorrelated faults 100% for 1/3 same fault
Liveness Slashing			_

	Tezos LPoS	Cosmos BPoS	Polkadot NPoS
Requirement to Participate	10,000 XTZ (8,000 XTZ)	Top 100 by Stake	-
Rights' Assignment	Pseudorandom by Stake and Priority List	Round-Robin by Stake	Pseudorandom and all validators have equal weights
Inflation	5.51%/Year when 60s. block times & all blocks in priority 0	7-20% Adaptive to Global Stake	-
Other Rewards	Accusations (50% of amount to validator)	Double-Voting evidences (rewards shared among all validators)	Fishermen (not necessarily validators)
Safety Slashing Conditions	Security Deposits for the entire cycle in the worst case	5% of Total Stake (Self-Bond and Delegations) + Execution	Self-Bond will be slashed before Delegations 1% for uncorrelated faults 100% for 1/3 same fault
Liveness Slashing	Missing the Rewards	Jailing Time (~7 days)	-

