Bonded Proof-of-Stake

Tendermint/Cosmos Team

Working Draft

Abstract

Bonded proof-of-stake is the Sybil-resistance construction utilized by the Cosmos Hub in conjunction with Tendermint BFT consensus to provide a quantifiably secure distributed ledger backbone.

Contents

0.1 Prerequisites

- BFT voting consensus algorithm
- Scarce fungible token in the state machine

0.2 Desiderata

- Imposition of scarcity on voting within an unbonding period (both full nodes / lite clients)
- Imposition of cost on downtime

0.3 Terminology

- Stakers: validators, delegators
- Validators: bonded, unbonding, unbonded
- Slash
- Equivocation
- Unbonding period

0.4 Implementation

- Tracking of what stake contributed to which vote
- Proportional slashing of contributing stake on equivocation discovery
- Microslashing for prolonged downtime

0.4.1 Deviations

- Simplified accounting in slashing for past infractions
- Tombstone (limited to one slash event while bonded)

0.4.2 Idiosyncrasies

- Must limit liquidity of stake due to proposer reward
- Unbonding delegations, redelegations cannot be canceled

0.5 Future Improvements

0.5.1 Light Client Efficiency

- Bisectable light client proofs
- Must slash for signatures when not bonded.