Lesson 17: Proof of Stake

Module 2: Blockchain Fundamentals

Digital Finance

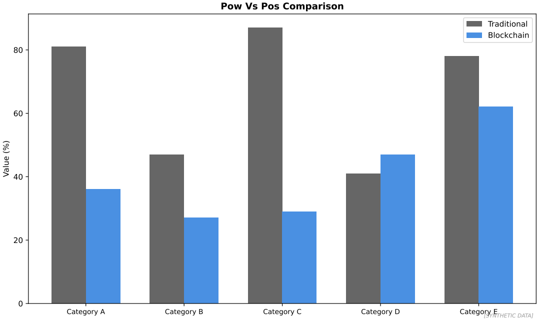
Why Proof of Stake?

Proof of Work Limitations:

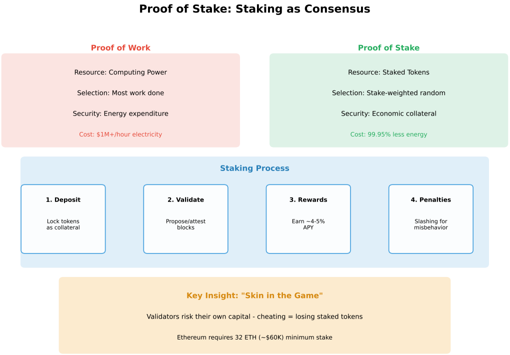
- Energy consumption (150+ TWh/year)
- Hardware waste (ASICs obsolete in 1–2 years)
- Centralization pressure (economies of scale)
- Slow finality (probabilistic)

PoS Alternative:

- Replace computation with capital
- Energy efficiency (99.95% reduction)
- Economic security
- Faster finality



Core Concept: Stake as Security Deposit



Source: Ethereum.org, Proof-of-Stake Documentation (2024)

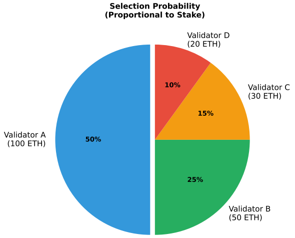
Key Idea:

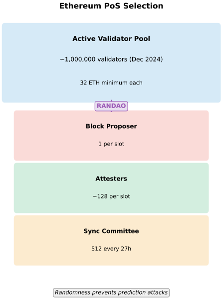
- Validators lock up capital (stake) as collateral
- Selected to propose blocks based on stake size
- Earn rewards for honest behavior
- Lose stake for dishonest behavior (slashing)
- **Attack cost:** Must acquire and lock majority of stake

Validator Selection Mechanisms

1. **Random Selection (weighted):**
   - Higher stake = higher probability
   - Not purely proportional (prevents centralization)
   - Randomness from VRF (Verifiable Random Function)

2. **Coin Age:**
   - Priority based on stake $\times$ time held
   - Resets after block proposal
   - Incentivizes long-term holding





Source: Ethereum Beacon Chain Specification, beaconcha.in (Dec 2024)

Ethereum's Proof of Stake: Beacon Chain

Requirements:

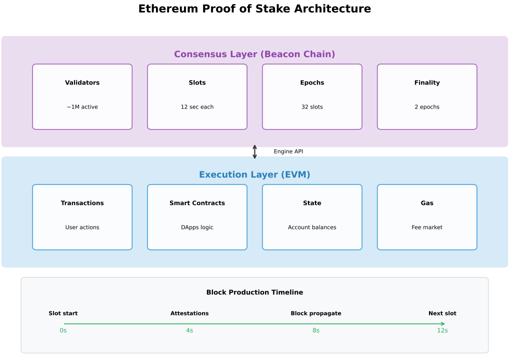
- Minimum stake: 32 ETH per validator
- Run validator node (beacon node + execution client)
- Uptime requirement: $>$99% to maintain profitability

Epoch and Slot Structure:

- **Slot:** 12 seconds (one block opportunity)
- **Epoch:** 32 slots = 6.4 minutes
- Each epoch, validators assigned to slots and committees
- Finality achieved after 2 epochs ($\sim$13 minutes)

Roles per Epoch:

- **Proposer:** One validator per slot, proposes block
- **Attesters:** Committees of validators vote on block validity



Source: Ethereum.org, The Merge Documentation (Sep 2022)

Consensus Flow:

1. Proposer selected for slot (pseudo-random, stake-weighted)
2. Proposer creates block, broadcasts to network
3. Attesters vote on block (organized in committees)
4. Aggregated attestations included in next block
5. After 2 epochs, block finalized (cannot be reverted)

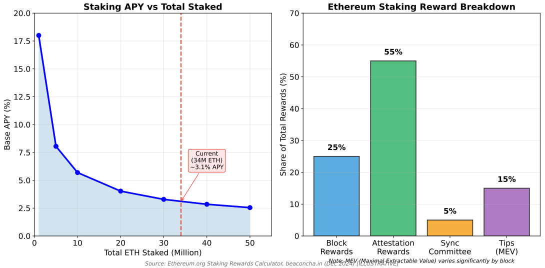
Rewards and Penalties

Rewards (per epoch):

- Timely attestations: $\sim$0.000015 ETH
- Block proposals: $\sim$0.0002 ETH
- Sync committee: $\sim$0.0001 ETH
- Annual yield: 3–5% APR

Penalties:

- Offline: Miss rewards + small penalty
- Late attestations: Reduced rewards
- Slashing: Major stake loss (see next slide)



Slashing: Punishing Malicious Behavior

Slashable Offenses:

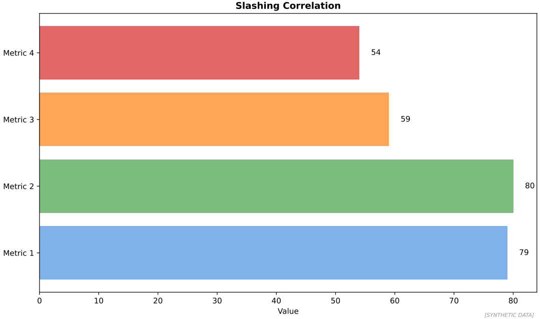
1. **Double Proposal:** Proposing two different blocks in same slot
2. **Surround Vote:** Attestation contradicting previous attestation
3. **Double Vote:** Two attestations for same slot with different targets

Slashing Penalties:

- Immediate penalty: 1 ETH (minimum)
- Correlation penalty: Scales with number of validators slashed simultaneously
- Maximum penalty: Entire 32 ETH stake (if many validators slashed together)
- Forced exit: Validator ejected from network

Design Goal: Make coordinated attacks extremely expensive

Slashing Correlation Penalty



Formula:

$$\text{Penalty} = \text{Base} + \text{Stake} \times \frac{\text{Slashed Validators}}{\text{Total Validators}} \times 3$$

Example: If 33% of validators slashed together, each loses entire stake

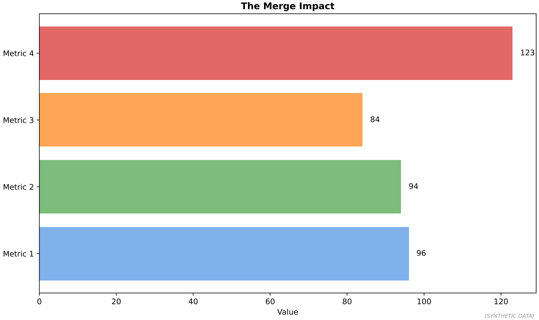
The Merge: Ethereum's Transition (Sept 15, 2022)

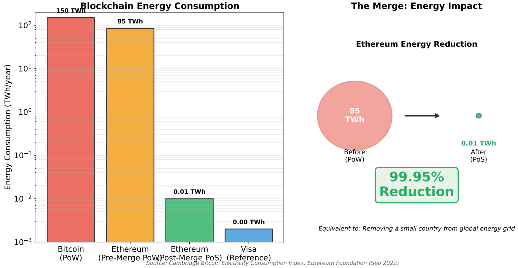
Before:

- Proof of Work (since 2015)
- Energy: ∼78 TWh/year
- Issuance: ∼13,000 ETH/day
- Block time: ∼13 seconds

After:

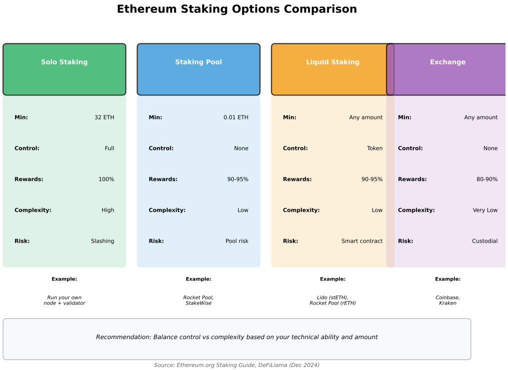
- Proof of Stake
- Energy: ∼0.01 TWh/year (99.95% reduction)
- Issuance: ∼1,600 ETH/day (88% reduction)
- Block time: 12 seconds (fixed)





Comparison (Annualized):

- **PoW Ethereum:** 78 TWh/year ≈ Chile's electricity consumption
- **PoS Ethereum:** 0.01 TWh/year ≈ 2,000 households
- **Per transaction:** PoW ∼200 kWh → PoS ∼0.01 kWh (20,000x improvement)



Solo Staking:

- 32 ETH minimum
- Full control, maximum rewards
- Technical expertise required
- Hardware costs

Pooled/Liquid Staking:

- Any amount (e.g., Lido, Rocket Pool)
- Receive staking derivative (stETH)
- Lower rewards (pool fees 10–15%)
- Easier, but centralization risk

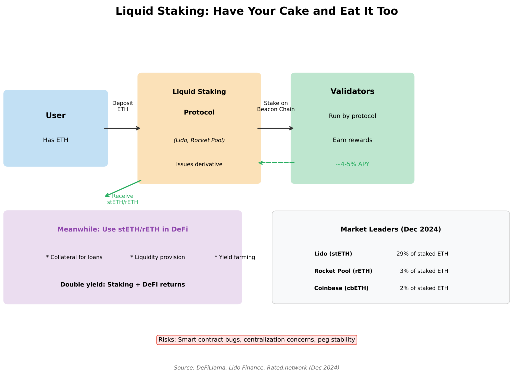
Liquid Staking Derivatives (LSDs)

Problem:

- Staked ETH locked until withdrawals enabled
- Lost liquidity
- Opportunity cost

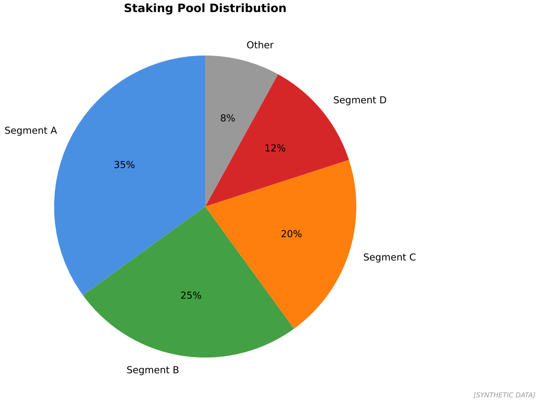
Solution:

- Deposit ETH, receive stETH (1:1)
- stETH accrues staking rewards
- Tradeable on DeFi markets
- Use as collateral



Risks: Centralization (Lido has >30% of staked ETH), smart contract risk, de-peg risk

Lido Dominance: Centralization Concern



Concerns:

- Lido controls >30% of staked ETH (as of 2024)
- Single point of failure for governance
- Risk of coordinated censorship

Mitigation: Self-limiting proposals, multi-operator model, community governance

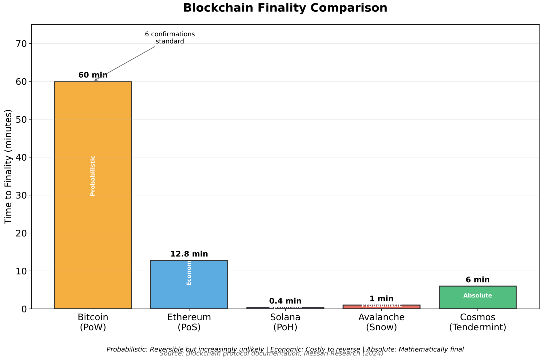
Finality: Proof of Stake Advantage

Proof of Work:

- Probabilistic finality
- Never 100% certain
- 6 confirmations $\approx$ 1 hour (Bitcoin)
- Longest chain rule

Proof of Stake (Ethereum):

- Economic finality
- 2 epochs ($\sim$13 minutes)
- Reversion requires $>$50% stake loss
- Absolute finality



Security Model: PoW vs PoS

Aspect	Proof of Work	Proof of Stake
Attack Cost	Buy hashrate (hardware + electricity)	Acquire majority stake
Attack Aftermath	Can reuse hardware	Stake slashed, loses capital
Defense	Increase difficulty, dilute attacker hashrate	Slash attacker stake
Recovery	Continue mining normally	Coordination for hard fork
Long-Range Attack	Not possible (checkpoints)	Weak subjectivity needed

Key Difference: PoS attacks destroy attacker's capital, PoW attacks do not

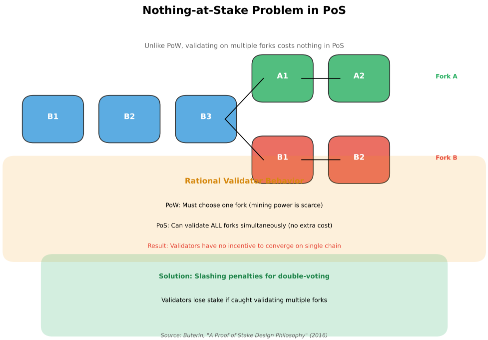
Nothing-at-Stake Problem

Problem:

- In PoW, mining on two chains splits hashrate
- In PoS, validating on two chains costs nothing
- Rational to vote on all forks
- Prevents convergence

Solution:

- Slashing for double-voting
- Casper FFG rules (Ethereum)
- Economic penalties enforce single chain



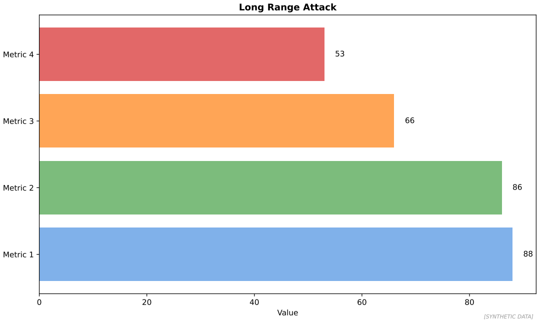
Long-Range Attack and Weak Subjectivity

Long-Range Attack:

- Attacker acquires old private keys
- Rewrites history from genesis
- No computational cost (unlike PoW)
- Creates alternative chain

Weak Subjectivity:

- New nodes must checkpoint recent state
- Cannot sync from genesis alone
- Trusted source for initial sync
- Checkpoints updated periodically



Other PoS Implementations

Chain	Consensus	Min Stake	Features
Ethereum	Casper FFG + LMD GHOST	32 ETH	Slashing, finality
Cardano	Ouroboros	Any (pool delegation)	Peer-reviewed, formal verification
Polkadot	GRANDPA + BABE	350 DOT (nominator)	Nominated PoS, parachains
Cosmos	Tendermint	Any (delegated)	Instant finality, IBC
Solana	Tower BFT	Any (delegated)	Proof of History hybrid

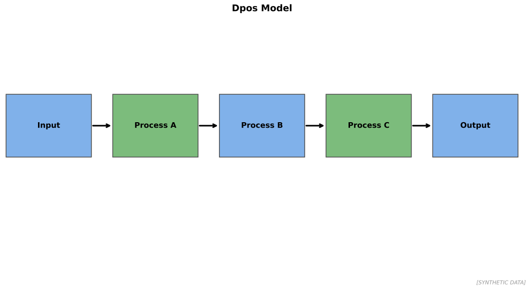
Delegated Proof of Stake (DPoS)

Mechanism:

- Token holders vote for validators
- Limited validator set (21–100)
- Validators produce blocks in rotation
- Faster, more scalable

Examples:

- EOS (21 validators)
- Tron (27 validators)
- Cosmos Hub (175 validators)



Trade-off: Performance vs decentralization (fewer validators = more centralized)

Criticisms of Proof of Stake

- **"Rich Get Richer":** Rewards proportional to stake, concentrates wealth
  - Counterargument: PoW also centralizes (economies of scale in mining)
- **Centralization:** Large staking pools (Lido >30% on Ethereum)
  - Counterargument: PoW mining pools also concentrated
- **Complexity:** Slashing, finality gadgets, weak subjectivity
  - Counterargument: Enables features impossible in PoW
- **Plutocracy:** Governance by wealthy token holders
  - Counterargument: Better than PoW's hardware oligopoly
- **Unproven:** Shorter track record than PoW
  - Counterargument: Ethereum's Merge successful so far (2+ years)

Summary

- **Proof of Stake:** Replace computation with capital, 99.95% energy reduction
- **Validators:** Lock stake (32 ETH on Ethereum), earn rewards, slashed if malicious
- **The Merge (2022):** Ethereum transitioned PoW $\rightarrow$ PoS successfully
- **Finality:** 2 epochs ($\sim$13 min) for absolute finality vs probabilistic PoW
- **Challenges:** Centralization (Lido), nothing-at-stake, long-range attacks
- **Trade-offs:** Energy efficiency vs complexity, different trust assumptions

Next Lesson: Bitcoin Architecture – UTXO model and transaction mechanics