

# Proof of Stake Consensus

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module A: Blockchain Foundations

By the end of this lesson, you will be able to:

- Explain the proof-of-stake consensus mechanism
- Describe validator responsibilities: staking, attestation, block proposal
- Understand slashing conditions and economic penalties
- Analyze Ethereum's Beacon Chain architecture
- Distinguish between justification and finality
- Calculate staking rewards and economics
- Evaluate centralization risks in proof-of-stake systems

## Proof of Work

- Security via computational cost
- Miners compete by hash power
- Energy-intensive
- Hardware requirements (ASICs)
- Block rewards + transaction fees
- 51% attack requires hash rate majority

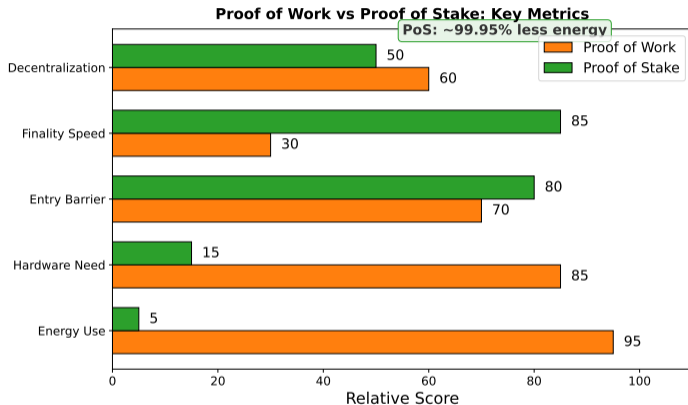
## Core Difference:

- PoW: external resource (electricity) → security
- PoS: internal resource (staked tokens) → security

## Proof of Stake

- Security via economic stake
- Validators selected by stake weight
- Energy-efficient (99% reduction)
- Capital requirements (staking)
- Transaction fees only (or low issuance)
- 51% attack requires token majority

# PoW vs PoS: Quantitative Comparison



*PoS dramatically reduces energy while improving finality time and throughput.*

# The Nothing-at-Stake Problem

## Theoretical Vulnerability:

In case of blockchain fork:

- PoW miners must choose one fork (cannot mine both simultaneously)
- PoS validators can vote on multiple forks simultaneously (no cost)
- Rational strategy: vote on all forks to maximize rewards

## Solutions:

- 1 **Slashing:** Detect and penalize validators voting on conflicting blocks
- 2 **Finality Gadgets:** Checkpoint mechanisms (Casper FFG) prevent reversals

## Practical Observation:

- Well-designed PoS systems have never experienced nothing-at-stake attacks
- Slashing and economic incentives effectively mitigate the threat

## The Merge (September 15, 2022):

- Ethereum transitioned from PoW to PoS
- Beacon Chain (PoS) launched December 2020, ran parallel 21 months
- No downtime, seamless transition

## Impact:

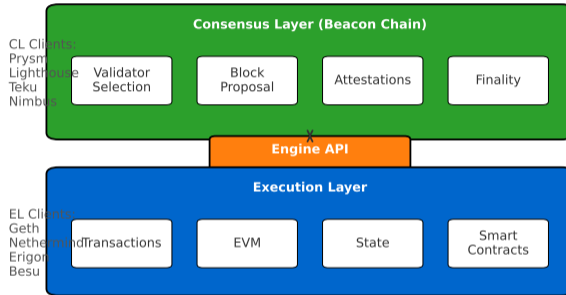
- Energy consumption reduced by  $\sim 99.95\%$
- ETH issuance reduced by  $\sim 90\%$  (13,000  $\rightarrow$  1,600 ETH/day)
- Block time:  $\sim 13s \rightarrow \sim 12s$

## Misconceptions Cleared:

- Did NOT reduce gas fees (addressed by Layer 2s)
- Did NOT increase throughput (scalability via sharding planned later)
- Changed consensus mechanism only

# Ethereum Beacon Chain Architecture

## Ethereum Post-Merge: Two-Layer Architecture



*The Merge unified execution and consensus layers under PoS.*

## ① Execution Layer (EL):

- Processes transactions and smart contracts
- Maintains Ethereum Virtual Machine (EVM)
- Manages account state

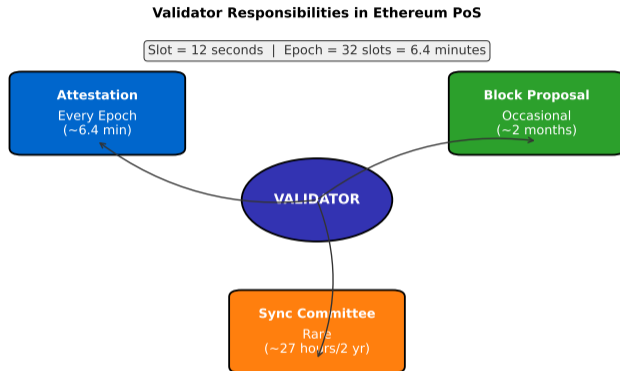
## ② Consensus Layer (CL / Beacon Chain):

- Selects block proposers
- Coordinates validators
- Manages staking and slashing
- Finalizes blocks

## Client Diversity:

- Execution: Geth, Nethermind, Erigon, Besu
- Consensus: Prysm, Lighthouse, Teku, Nimbus, Lodestar
- Engine API connects EL and CL

# Validator Responsibilities



*Validators perform multiple duties with varying frequencies and reward structures.*

## ① Attestation (every epoch):

- Vote on head of chain (latest block)
- Vote on justified and finalized checkpoints
- Attestations aggregated into blocks

## ② Block Proposal (occasionally):

- Selected pseudo-randomly based on stake
- Propose new block with transactions
- Earn transaction fees + block reward

## ③ Sync Committee (rarely):

- Rotating committee (~27 hours of service)
- Help light clients sync to chain

**Timing:** Slot = 12 seconds — Epoch = 32 slots = 6.4 minutes

## Minimum Stake:

- 32 ETH per validator (all-or-nothing activation)
- Can run multiple validators (64 ETH = 2 validators)

## Staking Process:

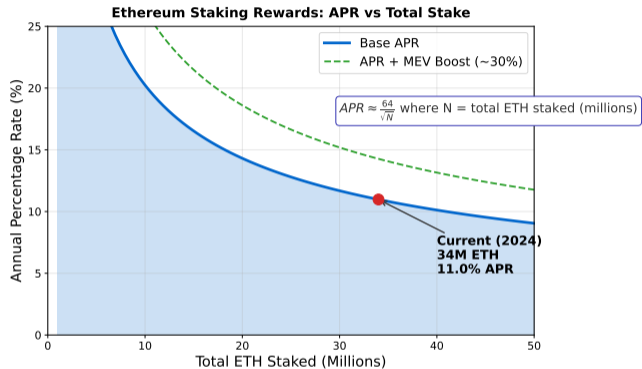
- 1 Generate validator keys (BLS12-381 signature scheme)
- 2 Deposit 32 ETH to deposit contract
- 3 Run validator client (Prysm, Lighthouse, etc.)
- 4 Wait for activation (24 hours to weeks)
- 5 Start attesting and proposing blocks

## Hardware Requirements:

- CPU: 4+ cores — RAM: 16+ GB — Storage: 2+ TB SSD
- Internet: 99%+ uptime — Monthly cost: \$50-200

**Alternatives:** Staking pools (Lido, Rocket Pool), exchanges (Coinbase), SaaS

# Staking Rewards: APR Curve



*More stakers = lower APR due to reward dilution. MEV adds 30%+ boost.*

## Reward Components:

- 1 **Attestation Rewards:** Earned for timely, correct attestations
- 2 **Block Proposal Rewards:** Transaction fees + attestation inclusion
- 3 **Sync Committee Rewards:** Small bonus for participation

## Annual Percentage Rate (APR):

$$\text{APR} \approx \frac{64}{\sqrt{N}}$$

where  $N$  = total ETH staked (in millions)

## Current State (2024-2025):

- 34M+ ETH staked:  $\text{APR} \approx 3.2\text{-}3.5\%$
- Over 1 million active validators
- MEV-Boost adds 30-50% to base rewards

## Missed Attestation Penalty:

- Equal to reward you would have earned
- Validator balance decreases (linear, no compounding)

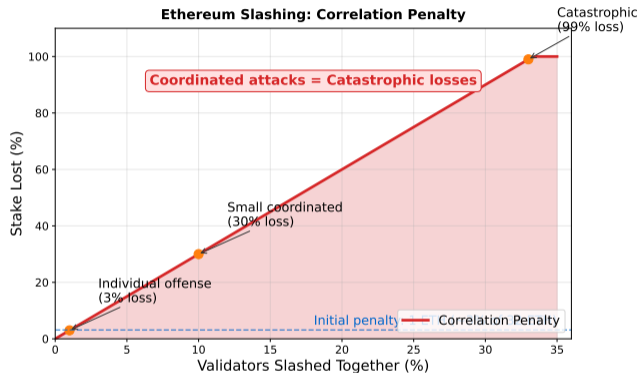
## Inactivity Leak:

- Activated when chain fails to finalize ( $> 4$  epochs)
- Offline validators lose stake at increasing rate (quadratic)
- Purpose: eject offline validators to restore finality

## Example Scenario:

- Network partition: 40% validators offline
- Chain cannot finalize (requires 67% participation)
- Inactivity leak begins, offline validators lose stake rapidly
- Eventually chain resumes finalization with remaining validators

# Slashing: Correlation Penalty



*Coordinated attacks result in catastrophic losses – strong deterrent against collusion.*

## Three Types:

- 1 **Double Proposal:** Proposing two blocks for same slot
- 2 **Surround Vote:** Attesting to conflicting checkpoint votes
- 3 **Double Vote:** Attesting to two different blocks in same epoch

## Slashing Penalties:

- **Initial penalty:** 1 ETH (immediate)
- **Correlation penalty:**  $\text{Stake} \times 3 \times (\text{slashed} / \text{total validators})$
- **Forced exit:** validator ejected from active set
- **Withdrawal delay:** 36 days before funds withdrawable

## Penalty Examples:

- 1% slashed together: lose  $\sim 3\%$  of stake
- 33% slashed together: lose  $\sim 99\%$  of stake (catastrophic)

## Casper FFG: Justification and Finalization

Justified: 67%+ ~~actualized~~ Justified + next justified



67%+ validators vote on (source, target) pairs

Reverting finalized block requires 33%+ stake to be slashed

*Finalized blocks cannot be reverted without 33%+ stake being slashed.*

## Purpose:

- Provide economic finality
- Prevent long-range reorganizations
- Make finalized blocks irreversible

## Checkpoint Voting:

- Checkpoint = first block of each epoch
- Validators vote on checkpoint pairs: (source, target)

## Justification vs Finalization:

- **Justified:** 67%+ attestations (temporary, can revert)
- **Finalized:** Justified + next epoch also justified (permanent)
- Finalization typically occurs after 2 epochs (~12.8 minutes)

## Accountable Safety:

- Two conflicting checkpoints cannot both finalize
- Economic guarantee: attacker loses massive stake

**Purpose:** Determine canonical chain head before finalization

**LMD GHOST (Latest Message Driven Greedy Heaviest Observed SubTree):**

- 1 Start at last finalized checkpoint
- 2 At each fork, choose subtree with most validator attestations
- 3 Recursively descend until leaf (chain head)

**Example:**

- Block A: 100 attestations — Block B: 150 attestations
- LMD GHOST selects Block B as canonical

**Combination with Casper FFG:**

- LMD GHOST: determines head (short-term)
- Casper FFG: determines finality (long-term)
- Together: fast confirmation + eventual certainty

## States:

- ➊ **Deposited:** 32 ETH deposited, waiting in activation queue
- ➋ **Active:** Attesting and proposing, earning rewards/penalties
- ➌ **Exiting:** Voluntary exit initiated, still active for  $\sim 1$  day
- ➍ **Exited:** No longer active, funds locked for 27 hours
- ➎ **Withdrawable:** Funds available (auto-withdrawal after Shanghai)

## Forced Exit:

- Triggered by slashing or balance  $< 16$  ETH
- Validator ejected automatically

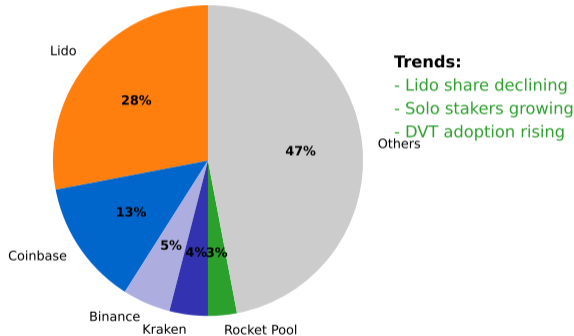
## Rewards:

- Base APR: 3-5% (varies with total staked)
- Transaction fees: 0.5-2% during high activity
- MEV (via MEV-Boost): 0.5-1% additional
- Total yield: ~4-8% annually

## Risks:

- **Slashing:** lose stake due to malicious behavior or bugs
- **Inactivity penalties:** offline validators lose rewards + leak
- **Opportunity cost:** locked capital (36-day exit)
- **Technical risk:** node downtime, hardware failure
- **Price risk:** ETH volatility affects total returns

## Ethereum Staking Concentration (2024)



**Top 5 entities: ~53% of staked ETH**

*33% threshold = finality blocking power*

*Top 5 entities control ~53% of staked ETH – 33% threshold gives finality blocking power.*

## Key Risks:

- 1 **Wealth Concentration:** Rich get richer (compound rewards), high 32 ETH barrier
- 2 **Exchange Dominance:** Lido ~28%, Coinbase ~13%, top 5 ~55%
- 3 **Staking Pool Centralization:** Pool operators control validators
- 4 **Client Diversity:** Prysm ~40% creates systemic risk

## Mitigation Efforts:

- Promote client diversity (incentives for minority clients)
- Decentralized pools (Rocket Pool, DVT)
- Community norms against >33% concentration
- Lido share declining, solo stakers growing

# MEV (Maximal Extractable Value)

**Definition:** Additional profit from reordering, inserting, or censoring transactions

## How it Works:

- 1 Searchers find opportunities (arbitrage, liquidations)
- 2 Submit bundles to block builders
- 3 Builders construct MEV-optimized blocks
- 4 Validators select highest-paying block (MEV-Boost)

**MEV-Boost:** Used by  $\sim 90\%$  of validators, increases rewards 50-100%

## Concerns:

- Centralizes block production (few builders dominate)
- Censorship risk (builders can exclude transactions)
- Users pay hidden costs (sandwich attacks)

## Network Growth:

- 34M+ ETH staked (28% of total supply)
- 1+ million active validators
- Network securing \$400B+ in value

## Protocol Upgrades:

- **Dencun (March 2024):** Proto-danksharding (EIP-4844), L2 fees down 90%+
- **July 2024:** Spot Ethereum ETFs approved by SEC
- Institutional staking products expanding

## Restaking (EigenLayer):

- \$15B+ in restaked ETH
- Validators secure additional networks
- Liquid restaking tokens (LRTs) proliferate

- Proof-of-stake replaces computational work with economic stake
- Validators attest to blocks and occasionally propose new blocks
- Slashing penalizes malicious behavior, aligning incentives
- Casper FFG provides economic finality through checkpoint voting
- Ethereum's Beacon Chain reduced energy consumption by 99.95%
- Staking requires 32 ETH and generates 4-8% annual returns
- Centralization risks remain (exchanges, pools, client diversity)

## Core Insight:

Proof-of-stake shifts blockchain security from external resources (energy) to internal resources (staked capital). Attackers must own and risk a significant portion of the network's value.

- 1 How does slashing solve the nothing-at-stake problem?
- 2 Why is client diversity critical for proof-of-stake security?
- 3 What are the trade-offs between solo staking and using a staking pool?
- 4 How does the inactivity leak mechanism help restore finality?
- 5 Is proof-of-stake more or less centralized than proof-of-work?
- 6 What role does MEV play in validator economics?
- 7 How would a 33% attack differ from a 51% attack in PoS?

### Topics to be covered:

- Comprehensive comparison: PoW vs PoS vs DPoS vs PBFT
- Security models and assumptions
- Scalability and throughput trade-offs
- Energy consumption and sustainability
- Decentralization metrics
- Finality and confirmation times

### Preparation:

- Review proof-of-work (Lesson 7) and proof-of-stake (Lesson 9)
- Read about Delegated Proof of Stake (DPoS) used in EOS, Tron
- Explore BFT consensus in Hyperledger, Cosmos