

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
- Used by: Bitcoin, Litecoin, Dogecoin

Core Difference:

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

Economic Argument for PoS:

- Attacking network destroys attacker's stake (self-punishment)
- PoW attacker retains hardware after attack
- PoS aligns economic incentives more directly

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
- Used by: Ethereum, Cardano, Polkadot

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
- Prevents consensus from converging on single chain

Solutions:

1 Slashing:

- Detect validators voting on conflicting blocks
- Destroy portion of their stake as penalty
- Makes voting on multiple forks costly

2 Finality Gadgets:

- Checkpoint mechanisms (Casper FFG)
- Validators attest to finalized blocks
- Cannot reverse finalized blocks without losing stake

Practical Observation:

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

Ethereum's Transition to Proof of Stake

The Merge (September 15, 2022):

- Ethereum transitioned from PoW to PoS
- Beacon Chain (PoS) launched December 2020
- Ran in parallel with PoW chain for 21 months
- Merge combined execution layer (original chain) with consensus layer (Beacon Chain)
- No downtime, seamless transition

Impact:

- Energy consumption reduced by 99.95%
- ETH issuance reduced by 90% (from 13,000 ETH/day to 1,600 ETH/day)
- Block time reduced from 13s to 12s
- Transaction finality improved (faster finalization)

Misconceptions Cleared:

- Did NOT reduce gas fees (separate issue, addressed by Layer 2s)
- Did NOT increase transaction throughput (scalability via sharding planned later)
- Did change consensus mechanism only

Two-Layer Design:

① Execution Layer (EL):

- Processes transactions and smart contracts
- Maintains Ethereum Virtual Machine (EVM)
- Manages account state
- Formerly the entire Ethereum blockchain (pre-Merge)

② Consensus Layer (CL / Beacon Chain):

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

Communication:

- Execution layer clients: Geth, Nethermind, Erigon, Besu
- Consensus layer clients: Prysm, Lighthouse, Teku, Nimbus, Lodestar
- Engine API connects EL and CL
- Validator runs both clients simultaneously

Validator Responsibilities

Core Duties:

① Attestation (every epoch):

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

② Block Proposal (occasionally):

- Selected pseudo-randomly based on stake
- Propose new block with transactions
- Include attestations from other validators
- Earn transaction fees + block reward

③ Sync Committee Participation (rarely):

- Rotating committee (27 hours of service)
- Help light clients sync to chain
- Sign block headers

Timing:

- Slot: 12 seconds
- Epoch: 32 slots = 6.4 minutes
- Validator attests once per epoch
- Expected block proposal: every 2 months (for single validator)

Staking Requirements and Process

Minimum Stake:

- 32 ETH per validator
- Cannot partially activate (all-or-nothing)
- Can run multiple validators (64 ETH = 2 validators, etc.)

Staking Process:

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

Hardware Requirements:

- CPU: 4+ cores
- RAM: 16+ GB
- Storage: 2+ TB SSD (grows over time)
- Internet: reliable, high uptime (99%+)
- Monthly cost: \$50-200 (VPS or home setup)

Staking Alternatives:

- Staking pools (Lido, Rocket Pool): stake any amount
- Centralized exchanges (Coinbase, Kraken): custodial staking

Reward Components:

1 Attestation Rewards:

- Earned for timely, correct attestations
- Proportional to effective balance (max 32 ETH)
- Vote on: head of chain, source checkpoint, target checkpoint

2 Block Proposal Rewards:

- Transaction fees (priority fees)
- Attestation inclusion rewards
- Sync committee rewards

3 Sync Committee Rewards:

- Small bonus for participating in sync committee

Annual Percentage Rate (APR):

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

where N = total ETH staked (in millions)

Examples (2024-2025):

- 34M+ ETH staked (late 2024): $\text{APR} \approx 3.2\text{-}3.5\%$
- Over 1 million active validators
- More stakers -> lower APR (reward dilution)

Missed Attestation Penalty:

- Equal to reward you would have earned
- Example: would earn 10,000 gwei - lose 10,000 gwei
- Validator balance decreases
- No compounding penalties (linear)

Inactivity Leak:

- Activated when chain fails to finalize (4 epochs without finality)
- Offline validators lose stake at increasing rate
- Purpose: eject offline validators to restore finality
- Quadratic leak rate (accelerates over time)
- Leak stops when chain finalizes again

Example Scenario:

- Network partition: 40% validators offline
- Chain cannot finalize (requires 67% participation)
- Inactivity leak begins
- Offline validators lose stake rapidly
- Eventually, their stake falls below 33% threshold
- Online validators (60%) now constitute 67%+ of remaining stake
- Chain resumes finalization

Slashing: Severe Penalties

Slashable Offenses:

- ❶ **Double Proposal:**
 - Proposing two different blocks for same slot
 - Indicates malicious intent or serious software bug
- ❷ **Surround Vote:**
 - Attesting to two conflicting checkpoint votes
 - Vote A surrounds vote B (violates Casper FFG rules)
- ❸ **Double Vote:**
 - Attesting to two different blocks in same epoch
 - Attempting to create fork

Slashing Penalties:

- **Initial penalty:** 1 ETH (immediate)
- **Correlation penalty:** up to entire stake if many validators slashed simultaneously
- **Forced exit:** validator ejected from active set
- **Withdrawal delay:** 36 days before funds withdrawable

Correlation Penalty Formula:

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

- If 1% slashed together: lose 3% of stake
- If 33% slashed together: lose 99% of stake (catastrophic)

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)
- Source: last justified checkpoint
- Target: current epoch checkpoint

Justification:

- Checkpoint becomes justified if 67%+ of validators attest to it
- Justification is temporary, can be reverted

Finalization:

- Checkpoint becomes finalized if:
 - ① It is justified
 - ② Next epoch checkpoint is also justified
- Finalization is permanent (cannot revert without massive slashing)
- Typically occurs after 2 epochs (12.8 minutes)

Accountable Safety:

- Two conflicting checkpoints cannot both finalize

LMD GHOST: Fork Choice Rule

Purpose:

- Determine canonical chain head
- Resolve forks before finalization
- Ensure validators agree on latest block

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)
- 4 Weights updated with each attestation

Example:

- Block A has 100 attestations
- Block B (competing fork) has 150 attestations
- LMD GHOST selects Block B as canonical
- Validators build on Block B

Combination with Casper FFG:

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

States:

1 Deposited:

- 32 ETH deposited to contract
- Waiting in activation queue
- Not yet earning rewards

2 Active:

- Attesting and proposing blocks
- Earning rewards or incurring penalties
- Can be slashed

3 Exiting:

- Voluntary exit initiated
- Still active for 1 day (exit queue)
- Cannot be canceled

4 Exited:

- No longer active
- Funds locked for 27 hours (sweep delay)

5 Withdrawable:

- Funds available for withdrawal
- Automatic withdrawal to specified address (after Shanghai upgrade, April 2023)

Forced Exit:

- Triggered by slashing or balance ≤ 16 ETH
- Validator ejected automatically

Staking Economics: Risks and Rewards

Rewards:

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

Risks:

- **Slashing:** lose stake due to malicious behavior or bugs (rare)
- **Inactivity penalties:** offline validators lose rewards + leak penalties
- **Opportunity cost:** locked capital (cannot sell during 36-day exit)
- **Technical risk:** node downtime, hardware failure, software bugs
- **Price risk:** ETH price volatility affects total returns

Break-Even Analysis:

- Setup cost: \$500-2000 (hardware or VPS)
- Monthly operating cost: \$50-200
- Annual reward (32 ETH at 4% APR): 1.28 ETH
- Reward value (ETH = \$2000): \$2560/year
- Annual operating cost: \$600-2400
- Net profit: \$160-1960/year (excluding setup cost)
- Payback period: 3-15 months

Centralization Risks in Proof of Stake

Concerns:

1 Wealth Concentration:

- Rich get richer (compound rewards)
- High entry barrier (32 ETH = \$64,000 at \$2000/ETH)
- Discourages small holders

2 Exchange Dominance (2024):

- Lido: 28% of staked ETH (down from 32%)
- Coinbase: 13%
- Top 5 entities: 55% of stake
- Centralized control risk (improving slowly)

3 Staking Pool Centralization:

- Users delegate stake to pools
- Pool operators control validators
- Censorship risk (e.g., OFAC compliance)

4 Client Diversity:

- Prysm: 40% of validators (2023)
- Single client bug could finalize invalid chain
- Supermajority client creates systemic risk

Mitigation Efforts:

- Promote client diversity (incentives for minority clients)
- Decentralized staking pools (Rocket Pool, distributed validator technology)
- Community norms against >33% concentration

MEV (Maximal Extractable Value)

Definition:

- Additional profit beyond block rewards
- Extractable by reordering, inserting, or censoring transactions
- Examples: arbitrage, liquidations, sandwich attacks

How it Works:

- 1 Searchers find profitable opportunities (e.g., arbitrage between DEXs)
- 2 Submit bundles to block builders
- 3 Builders construct blocks with MEV transactions
- 4 Validators select highest-paying block (via MEV-Boost)
- 5 Profit split between searcher, builder, validator

MEV-Boost:

- Middleware connecting validators to block builders
- Validators outsource block construction
- Increases validator rewards by 50-100%
- Used by 90% of validators

Concerns:

- Centralizes block production (few builders dominate)
- Censorship risk (builders can exclude transactions)
- Users pay hidden costs (sandwich attacks)
- Ongoing research: proposer-builder separation, encrypted mempools

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)
 - Blob transactions for L2 data availability
 - L2 fees reduced by 90%+
- **July 2024:** Spot Ethereum ETFs approved by SEC
- Institutional staking products expanding

Restaking Emergence (EigenLayer):

- \$15B+ in restaked ETH
- Validators secure additional networks
- New primitive: shared security
- 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)
- MEV introduces additional revenue but raises censorship concerns

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, creating strong economic disincentives.

- ➊ How does slashing solve the nothing-at-stake problem?
- ➋ Why is client diversity critical for proof-of-stake security?
- ➌ What are the trade-offs between solo staking and using a staking pool?
- ➍ How does the inactivity leak mechanism help restore finality?
- ➎ Is proof-of-stake more or less centralized than proof-of-work?
- ➏ What role does MEV play in validator economics?
- ➐ 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
- Use cases and blockchain selection criteria

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 Byzantine Fault Tolerant (BFT) consensus in Hyperledger, Cosmos