Lesson 17: Proof of Stake

Module 2: Blockchain Fundamentals

Digital Finance

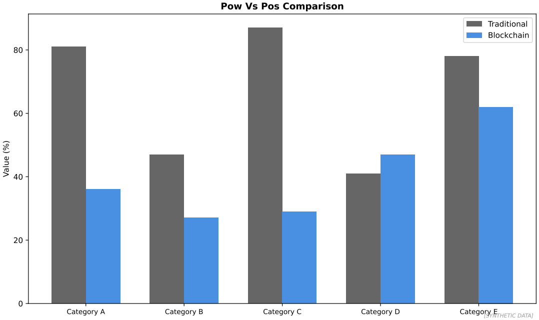
Why Proof of Stake?

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)

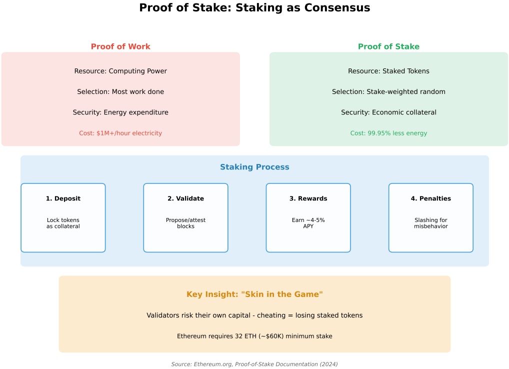
PoS Alternative:

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



Proof-of-Stake offers energy efficiency while maintaining decentralization.

Core Concept: Stake as Security Deposit



Proof of Stake: Staking as Consensus

Proof of Work

Resource: Computing Power

Selection: Most work done

Security: Energy expenditure

Cost: $1M+/hour electricity

Proof of Stake

Resource: Staked Tokens

Selection: Stake-weighted random

Security: Economic collateral

Cost: 99.95% less energy

Staking Process

1. Deposit
Lock tokens
as collateral

2. Validate
Propose/attest
blocks

3. Rewards
Earn ~4-5%
APY

4. Penalties
Slashing for
misbehavior

Key Insight: "Skin in the Game"

Validators risk their own capital - cheating = losing staked tokens

Ethereum requires 32 ETH (~$60K) minimum stake

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

Key Idea:

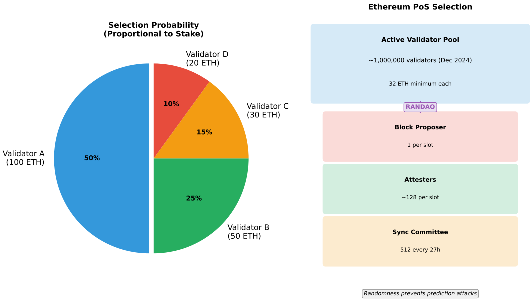
- Validators lock up capital (stake) as collateral
- Selected to propose blocks based on stake size
- Earn rewards for honest behavior
- Lose stake for dishonest behavior (slashing)
- **Attack cost:** Must acquire and lock majority of stake

Security analysis identifies vulnerabilities and helps design robust systems.

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 × time held
   - Resets after block proposal
   - Incentivizes long-term holding



Ethereum PoS Selection

Active Validator Pool

~1,000,000 validators (Dec 2024)

32 ETH minimum each

RANDAO

Block Proposer

1 per slot

Attesters

~128 per slot

Sync Committee

512 every 27h

Randomness prevents prediction attacks

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

Key concepts from this slide inform practical applications in finance.

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 (∼13 minutes)

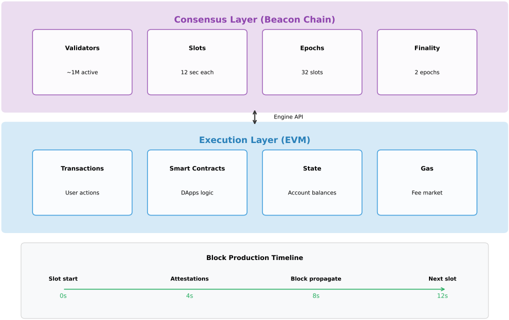
Roles per Epoch:

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

Ethereum pioneered smart contracts and remains the dominant platform for DeFi and NFTs.

Ethereum PoS Architecture

Ethereum Proof of Stake Architecture



Consensus Layer (Beacon Chain)

Validators
~1M active

Slots
12 sec each

Epochs
32 slots

Finality
2 epochs

Engine API

Execution Layer (EVM)

Transactions
User actions

Smart Contracts
DApps logic

State
Account balances

Gas
Fee market

Block Production Timeline

Slot start	Attestations	Block propagate	Next slot
0s	4s	8s	12s

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)

Ethereum pioneered smart contracts and remains the dominant platform for DeFi and NFTs.

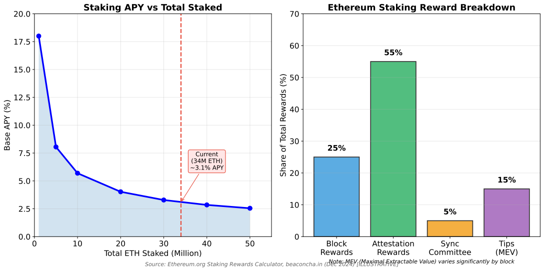
Rewards and Penalties

Rewards (per epoch):

- Timely attestations: ∼0.000015 ETH
- Block proposals: ∼0.0002 ETH
- Sync committee: ∼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)



Note: MEV (Maximal Extractable Value) varies significantly by block

Source: Ethereum.org Staking Rewards Calculator, beaconcha.in (Dec 2024) [ILLUSTRATIVE]

Key concepts from this slide inform practical applications in finance.

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

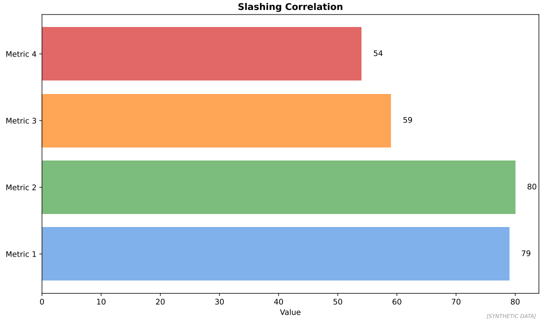
Slashing Penalties:

- 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

Key concepts from this slide inform practical applications in finance.

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

Key concepts from this slide inform practical applications in finance.

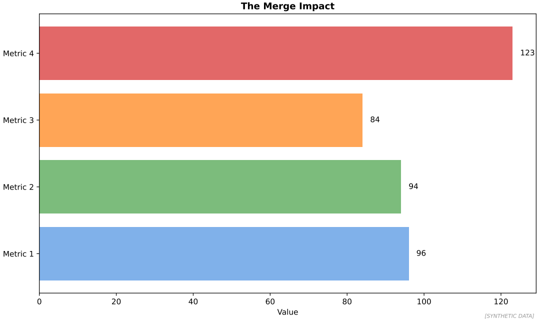
The Merge: Ethereum's Transition (Sept 15, 2022)

Before:

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

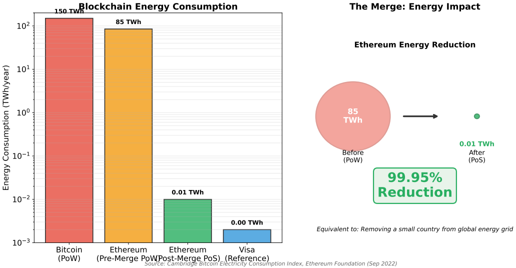
After:

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



Ethereum pioneered smart contracts and remains the dominant platform for DeFi and NFTs.

Environmental Impact: Before and After The Merge



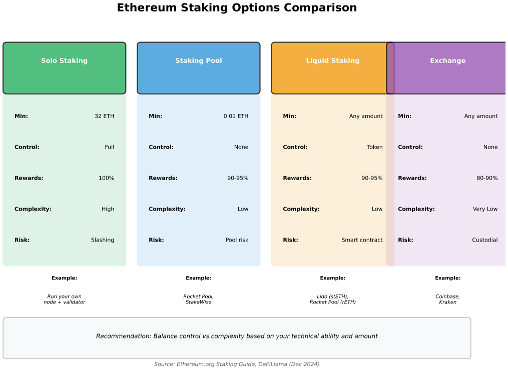
Source: Cambridge Bitcoin Electricity Consumption Index, Ethereum Foundation (Sep 2022)

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)

Key concepts from this slide inform practical applications in finance.

Staking Economics: Solo vs Pooled



Ethereum Staking Options Comparison

	Solo Staking	Staking Pool	Liquid Staking	Exchange
Min:	32 ETH	0.01 ETH	Any amount	Any amount
Control:	Full	None	Token	None
Rewards:	100%	90-95%	90-95%	80-90%
Complexity:	High	Low	Low	Very Low
Risk:	Slashing	Pool risk	Smart contract	Custodial
Example:	*Run your own node + validator*	*Rocket Pool, StakeWise*	*Lido (stETH), Rocket Pool (rETH)*	*Coinbase, Kraken*

Recommendation: Balance control vs complexity based on your technical ability and amount

Source: Ethereum.org Staking Guide, DeFiLlama (Dec 2024)

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

Comparative analysis helps identify the right tool for specific requirements.

Liquid Staking Derivatives (LSDs)

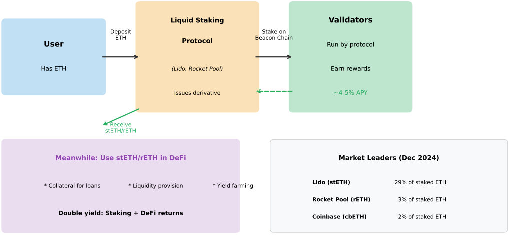
Problem:

- 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

Liquid Staking: Have Your Cake and Eat It Too



Market Leaders (Dec 2024)

Lido (stETH)	29% of staked ETH
Rocket Pool (rETH)	3% of staked ETH
Coinbase (cbETH)	2% of staked ETH

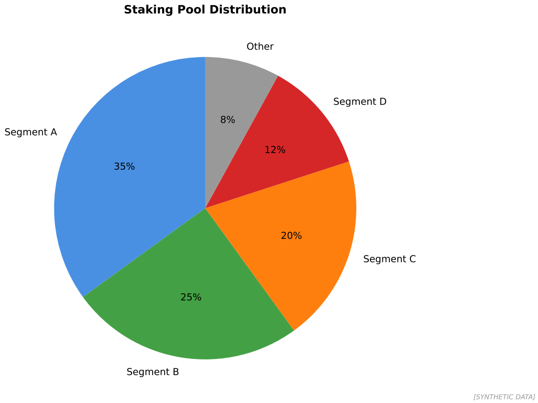
Risks: Smart contract bugs, centralization concerns, peg stability

Source: DeFiLlama, Lido Finance, Rated.network (Dec 2024)

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

Derivatives enable risk transfer and price discovery.

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

Key concepts from this slide inform practical applications in finance.

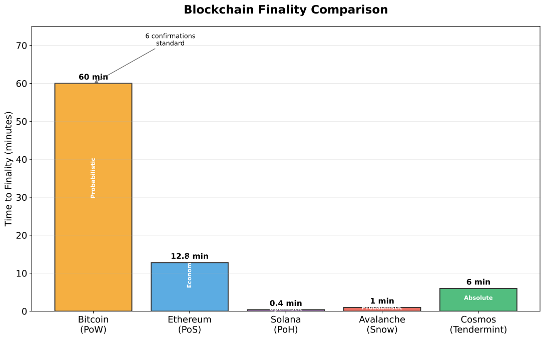
Finality: Proof of Stake Advantage

Proof of Work:

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

Proof of Stake (Ethereum):

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



Probabilistic: Reversible but increasingly unlikely | Economic: Costly to reverse | Absolute: Mathematically final

Source: Blockchain protocol documentation, Messari Research (2024)

Proof-of-Stake offers energy efficiency while maintaining decentralization.

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

Comparative analysis helps identify the right tool for specific requirements.

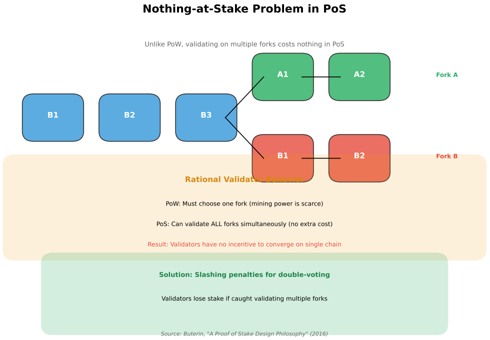
Nothing-at-Stake Problem

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



Nothing-at-Stake Problem in PoS
Unlike PoW, validating on multiple forks costs nothing in PoS
B1
B2
B3
A1
A2
Fork A
B1
B2
Fork B
Rational Validator Behavior
PoW: Must choose one fork (mining power is scarce)
PoS: Can validate ALL forks simultaneously (no extra cost)
Result: Validators have no incentive to converge on single chain
Solution: Slashing penalties for double-voting
Validators lose stake if caught validating multiple forks

Source: Buterin, "A Proof of Stake Design Philosophy" (2016)

Key concepts from this slide inform practical applications in finance.

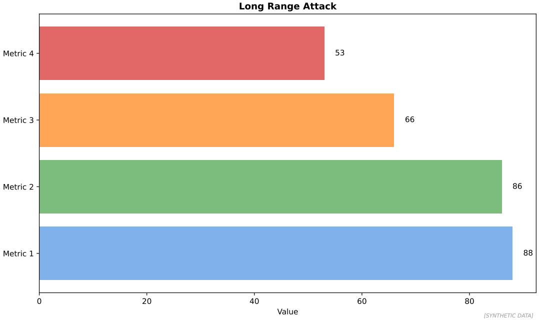
Long-Range Attack and Weak Subjectivity

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



Security analysis identifies vulnerabilities and helps design robust systems.

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

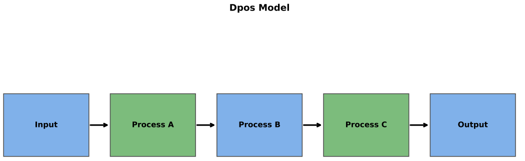
Delegated Proof of Stake (DPoS)

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)



[SYNTHETIC DATA]

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

Proof-of-Stake offers energy efficiency while maintaining decentralization.

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)

Proof-of-Stake offers energy efficiency while maintaining decentralization.

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 → 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