EE374: Fundamentals of Blockchain Infrastructure
Lecture 10: Proof-of-Stake Industry, Accountability, and Economic Security

Prof. David Tse
Scribe: Natalie Cao

April 30, 2025

1 Lecture Overview

This lecture provides an in-depth exploration of the Proof-of-Stake (PoS) blockchain ecosystem, discussing current industry metrics, economic security principles, and mechanisms for accountability within PoS systems. We closely examine Ethereum's staking environment, analyze various trust models in blockchain, and perform a detailed case study of accountability within the Tendermint consensus protocol.

2 Current State of the PoS Industry

Proof-of-Stake has become a predominant consensus model, incentivizing validators to participate actively by staking their cryptocurrency. The Proof of Stake industry began around 2017-2018 and has matured significantly over the past 7-8 years. This section examines the current state of major POS blockchains.

Key Metrics to Monitor

Reward rate: The percentage returns validators receive for staking **Staking market cap**: Total value of staked tokens **Staking ratio**: Percentage of total token supply being staked

2.1 Top POS Blockchains

The primary blockchains discussed are:

- **Ethereum**: Reward rate of approximately 3.1%, total staked market cap around $61.4B. Ethereum employs a hybrid consensus model called Casper the Friendly Finality Gadget (Casper FFG), combining longest-chain consensus with Byzantine Fault Tolerance (BFT)-style finality.
- **Solana**: Notably higher reward rate of 8.32% and staking market cap of $57B, primarily driven by meme coin activities.

  Reward Rate: 3.1%

  Staking Market Cap: $61.4 billion

  Staking Ratio: 28.24% of total ETH supply

- **Sui**: A newer protocol using Directed Acyclic Graph (DAG)-based consensus, featuring high throughput and approximately $26B market cap.

  Features: Relatively new blockchain (launched 1.5 years ago)

  Staking Market Cap: $28.26 billion

  Note: High throughput, pushing the state-of-the-art in DFT protocols

- **BNB Chain**: Origin: Associated with Binance exchange

  Consensus Protocol: Built on Tendermint protocol

  Note: While associated with Binance, the chain itself is decentralized

- **Cardano**: Consensus Approach: Proof of stake adaptation of Bitcoin's longest chain protocol

  Note: Interesting study of applying Bitcoin concepts to proof of stake

- **Other Notable Chains**: **Avalanche**: Founded by Emin Gün Sirer (developer of selfish mining concept) **Aptos**: Built on Hot Stuff, which is derived from Tendermint **Bitcoin Staking**: Not native Bitcoin PoW, but a separate protocol for staking Bitcoin to secure proof of stake blockchains

The rewards for staking primarily originate from two sources: block rewards (inflationary emissions) and transaction fees (such as Ethereum's gas fees).

2.2 Ethereum Staking Analysis

- **Staking Metrics**

  Total ETH staked: 34 million

  ETH (worth $61 billion)

  Number of validators: 1 million

  Each validator is secured by 32 ETH

- **Validator Distribution**

  Lido: 26.85% of staking market share

  Coinbase: Major exchange-based validator

  Binance: Major exchange-based validator

  Various professional validator companies: Kraken, Figment, etc.

- **Liquid Staking**

  Concept: Providing liquidity for staked assets that would otherwise be locked

  Process: Users stake ETH with a liquid staking provider and receive a derivative token (e.g., stETH) that represents their staked ETH

  Advantage: Users can earn staking rewards while maintaining liquidity to trade or use in DeFi Major providers: Lido, EtherFi, Rocket Pool

  Concern: Lido's market dominance approaching 33% (the threshold at which network censorship becomes possible)

3 Economic Security and Trust Models

3.1 Economic Security

Economic security in PoS blockchains is defined by the total monetary value locked in staking. Validators face economic penalties ("slashing") for protocol violations, providing strong deterrents against malicious behaviors. Ethereum currently stakes approximately 34 million ETH ($61B market cap) but applies modest slashing penalties (1 ETH per 32 ETH stake).

3.2 Trust Spectrum

Trust models range from centralized control to purely cryptographic assurances:

1. **"Trust Me, Bro" (Highest Trust)**: Centralized trust in a single organization or entity
   Represents traditional, centralized models
2. **"Trust Us, Bros" (Decentralized Trust)**:
   Trust distributed across many participants
   Examples: Bitcoin (51% honest assumption), Tendermint (2/3 honest assumption)
   Better than centralized trust, but still requires assumptions about honest majority
3. **Crypto-economic Trust**: Economic penalties ensure accountability.
   Trust backed by financial incentives and penalties
   Uses collateral to ensure honest behavior
   Pioneered by Tendermint designers and Vitalik Buterin
   Superior to simple decentralized trust, but not as strong as trustless systems
4. **"Trust Only Math" (Lowest Trust / Trustless)**:
   Relies purely on mathematical guarantees
   Example: Cryptographic primitives (signatures, hash functions)
   Strongest form of trust minimization, but not achievable for full consensus protocols

4 Accountability in PoS Protocols

4.1 Definitions

Economic Security

- Definition: The financial cost an attacker would incur to successfully attack the network
- Ethereum's Economic Security: $61 billion total staked, but actual slashing penalties are typically 1 ETH out of 32 ETH staked per validator
- Slashing Rationale: Small initial penalties accommodate honest mistakes, with potential for higher penalties in future versions

Accountability ensures that protocol violations are verifiable, and offenders can be unequivocally identified and penalized. Specifically, accountability statements assert:

- Safety: "If less than 1/3 validators are dishonest, the protocol is safe"
- Accountability: "If there is a safety violation, at least 1/3 of validators can be held accountable with irrefutable evidence"
- Advantage: Accountability is a stronger guarantee, as it provides a path to punish violators rather than just assuming honesty

4.2 Certificates and Irrefutable Evidence

Unlike Bitcoin, which lacks cryptographic certificates to prove finality externally, Tendermint explicitly uses certificates created from pre-commit votes of validators to establish finality and accountability.

Important distinction:

- **Bitcoin**: No way to prove to others that a transaction is confirmed using trustless certificates
- **Tendermint**: Provides cryptographically transferable evidence (certificates) ensuring transparent and provable accountability. Uses certificates (2/3 pre-commit votes) that can prove block confirmation to anyone. It enables transferable knowledge and accountability mechanisms.

5 Tendermint Accountability Case Study

5.1 Case 1: Same-Round Violations

When two blocks B_1 and B_2 are confirmed in the same round, a protocol violation can be proven through quorum intersection:

- **Scenario**: Two blocks (B_1, B_2) confirmed in the same round
- **Confirmation Requirement**: Each block received $\geq 2f + 1$ pre-commits
- **Mathematical Analysis**:
  - Let Q_1 = set of validators voting for B_1
  - Let Q_2 = set of validators voting for B_2
  - $|Q_1| \geq 2f + 1$, $|Q_2| \geq 2f + 1$ (assuming $n = 3f + 1$)
  - By quorum intersection: $|Q_1 \cap Q_2| \geq f$
- **Protocol Violation**:
  - Validators in $Q_1 \cap Q_2$ sent pre-commits for both blocks
  - Violates rule of sending only one pre-commit per round
- **Accountability Mechanism**:
  - Two conflicting pre-commit sets serve as irrefutable evidence
  - At least f validators ($\geq 1/3$) can be identified and slashed
  - Evidence is objective and third-party verifiable
- **Conclusion**: Tendermint is accountable for same-round safety violations

5.2 Case 2: Cross-Round Violations

A more intricate scenario occurs when:

1. Round 1: B_1 confirmed by a quorum ($\geq 2f + 1$), validators locked to B_1.
2. Round 2: B_2 confirmed separately by another quorum ($\geq 2f + 1$), different round votes.
3. Intersection validators ($\geq f + 1$) improperly issue prevotes for B_2, violating their prior locks on B_1.

Note: Block B1 confirmed in Round 1 with 2/3+ pre-commits; Block B2 confirmed in Round 2 with 2/3+ pre-commits; Analysis of voting sets reveals protocol violation: Validators who locked on B1 shouldn't send pre-votes for B2 ; Intersection of these sets (¿f+1 validators) violated the protocol

- **Scenario**:
  - B1 confirmed with $\geq 2/3$ pre-commits in round 1
  - B2 confirmed with $\geq 2/3$ pre-commits in round 2
- **Mathematical analysis**:
  - 2f+1 validators sent pre-commits for B1 in round 1
  - These validators must have "locked" on B1
  - Protocol requires that validators locked on B1 should not send pre-votes for B2
  - 2f+1 validators sent pre-commits for B2 in round 2
  - These validators must have sent pre-votes for B2
  - By quorum intersection: At least f+1 validators both locked on B1 and sent pre-votes for B2
- **Protocol violation identified**:
  - At least f+1 validators violated the protocol by sending pre-votes for B2 despite being locked on B1
  - This is sufficient to identify $\geq 1/3$ of validators as dishonest
- **Accountability problem**:
  - The violation occurs at the pre-vote level
  - But confirmation certificates only contain pre-commits
  - From examining only the pre-commits, one cannot derive irrefutable evidence of the violation
  - Cannot produce evidence to convince a third party of the violation
- **Conclusion**: Tendermint is NOT accountable for safety violations across different rounds

Critical Issue: The violation occurs at the pre-vote level, but confirmation certificates only contain pre-commits. This creates an accountability gap where violations can't be proven with irrefutable evidence

Solution Proposal: Tendermint is not fully accountable in its current form. Future homework will explore modifications to make Tendermint fully accountable. Augmenting Tendermint by explicitly recording prevotes to provide irrefutable proof of misconduct and strengthen overall accountability.

Potential solution:

- Include pre-votes in the confirmation certificates
- Record the locking status of validators in a verifiable way
- Require validators to prove their locked status when voting in subsequent rounds

Upcoming homework will investigate specific modifications to make Tendermint fully accountable. Minor additions to the protocol could potentially close this accountability gap

6 Key Takeaways

- Proof of Stake has evolved into a mature industry securing hundreds of billions in value across multiple blockchain networks
- The security model has shifted from simple honest majority assumptions to economic security with quantifiable costs for attacks
- Liquid staking represents a major innovation addressing capital efficiency while maintaining security properties
- Trust in blockchain systems exists on a spectrum from centralized trust to trustless mathematical guarantees
- Accountability provides stronger security guarantees than traditional safety statements by enabling punishment of dishonest validators
- Tendermint provides partial accountability (for same-round violations) but has a critical accountability gap for cross-round violations
- Certificate-based confirmation enables transferable knowledge and accountability mechanisms that are not possible in Bitcoin-style protocols

PoS blockchains represent an evolving balance between decentralization, economic security, and accountability. While cryptographic and crypto-economic methods provide robust frameworks, ongoing improvements (particularly in accountability mechanisms, such as those identified in Tendermint) are crucial to maintaining trust and security in blockchain infrastructures.