Blockchain Economics and Consensus

Theme III: Decentralized Finance

Research Question: What are the economic incentives underlying consensus mechanisms, and when do they fail?

PhD Seminar in Digital Finance

The Consensus Problem: Byzantine Fault Tolerance

Byzantine Generals Problem
n generals, f traitors. Need agreement.
Classic Result (Lamport et al., 1982)

Proposition

Byzantine agreement possible iff:

$$n \geq 3f + 1$$

Blockchain Innovation
Replace trust with:

- Economic incentives
- Cryptographic proofs
- Probabilistic finality

Nakamoto Consensus
Longest chain rule + Proof of Work.
Key Properties

- Permissionless participation
- Sybil resistance via cost
- Probabilistic finality

Security Assumption
Honest majority of *compute power*:

$$h > 0.5 \cdot \text{Total Hash Rate}$$

Not honest majority of *nodes*.

Lamport, Shostak & Pease (1982), "The Byzantine Generals Problem"

Proof of Work: Mining Economics

Miner's Problem
Choose hash rate h_i to maximize:

$$\pi_i = \frac{h_i}{\sum_j h_j} \cdot R - c \cdot h_i$$

where R = block reward, c = cost per hash.
Equilibrium
With free entry:

$$\pi_i = 0 \implies \sum_j h_j = \frac{R}{c}$$

Security Budget
Total hash rate proportional to $R \cdot P_{BTC}$.

Selfish Mining (Eyal & Sirer, 2014)
Strategic block withholding.

Proposition

With fraction α of hash power, selfish mining profitable if:

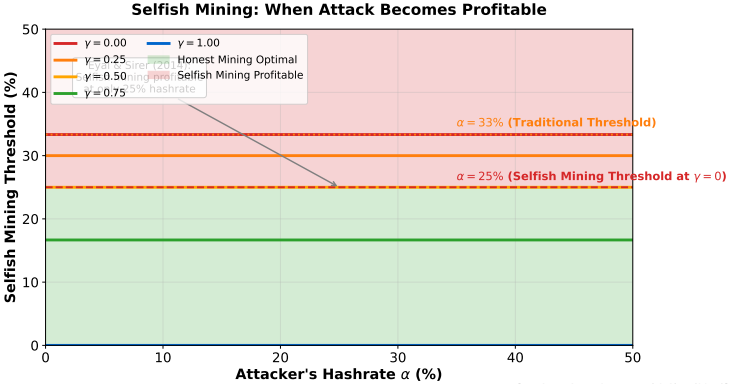
$$\alpha > \frac{1-\gamma}{3-2\gamma}$$

where γ = propagation advantage.

For $\gamma = 0$: $\alpha > 1/3$
Implication
50% threshold is optimistic; 33% may suffice for attack.

Eyal & Sirer (2014), "Majority is Not Enough: Bitcoin Mining is Vulnerable"

Selfish Mining: Profitability Threshold



[THEORETICAL MODEL - Eyal & Sirer (2014)]

Selfish mining becomes profitable at lower thresholds than the naive 50% attack.

Proof of Stake: Economic Security

PoS Mechanism
Validators stake capital s_i:

$$\Pr(\text{selected}) = \frac{s_i}{\sum_j s_j}$$

Slashing
Misbehavior penalized:

$$s_i \to s_i \cdot (1 - \text{slash})$$

Nothing-at-Stake Problem
Without slashing: Vote on all forks (costless).
Solution: Punish equivocation.

Long-Range Attacks
Old validators can rewrite history.
Weak Subjectivity
New nodes must trust checkpoint.
Ethereum PoS (2022)

Parameter	Value
Min stake	32 ETH
Validators	900K+
Slash penalty	1-100%
Finality	12 min

Buterin et al. (2020), "Combining GHOST and Casper" – Ethereum PoS specification

Maximal Extractable Value (MEV)

Definition
Value extractable by ordering transactions:

$$\text{MEV} = \max_{\sigma} V(\sigma) - V(\sigma_{FIFO})$$

where σ = transaction ordering.

MEV Types

- **Arbitrage**: DEX price discrepancies
- **Liquidations**: Collateral seizure
- **Sandwich**: Front/back-run trades

MEV Scale (2024)
Ethereum MEV extracted:

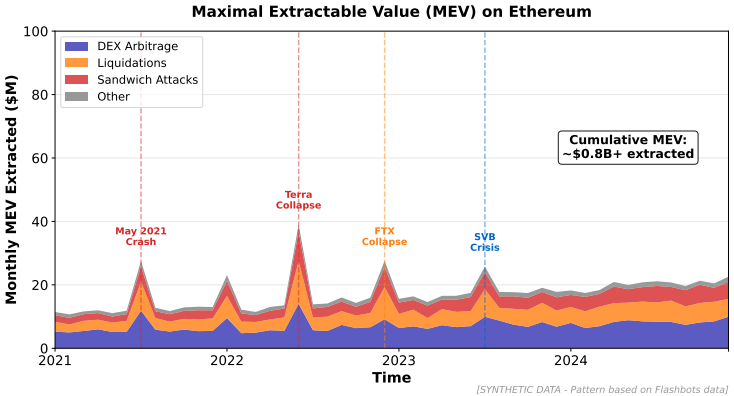
- Total: \$600M+ annually
- Arbitrage: 60%
- Liquidations: 25%
- Sandwiches: 15%

Economic Implications

1. Implicit tax on users
2. Validator revenue diversification
3. Centralization pressure (MEV specialists)

Flashbots (2021), "MEV Explore" – real-time MEV tracking

MEV Extraction: Types and Magnitude



MEV extraction totals billions annually; arbitrage and liquidations dominate, with sandwich attacks growing.

Transaction Fee Mechanism Design

EIP-1559 (Ethereum)
Base fee + priority fee:

$$\text{Fee} = \text{baseFee} + \text{tip}$$

Base fee burned (not paid to validators).
Mechanism Properties
Roughgarden (2020) analyzes:

- Incentive compatibility
- Myopic miner-proofness
- Off-chain agreement resistance

Key Results

Proposition

EIP-1559 is approximately incentive-compatible under non-strategic demand.

Limitations

- Strategic users can still manipulate
- Not optimal auction
- Base fee volatility

Alternative: First-Price Auction
Simple, but leads to fee estimation games.

Roughgarden (2020), "Transaction Fee Mechanism Design for the Ethereum Blockchain"

Measuring Decentralization

Nakamoto Coefficient
Minimum entities to control 51%:

$$NC = \min\{k : \sum_{i=1}^{k} s_{(i)} > 0.51\}$$

Current Values (2024)

Chain	NC
Bitcoin (pools)	4
Ethereum	4
Solana	19
Cosmos	7

Multi-Dimensional View
Decentralization across:

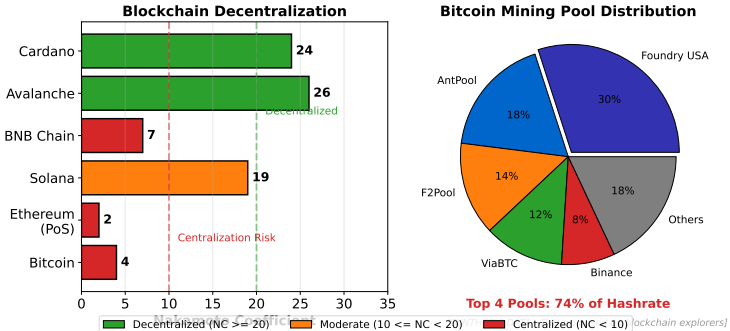
1. Consensus (validators/miners)
2. Development (core contributors)
3. Clients (software diversity)
4. Hosting (cloud concentration)
5. Ownership (token distribution)

Trade-Offs
More decentralization $\rightarrow$:

- Lower throughput
- Higher latency
- More coordination cost

Srinivasan (2017), "Quantifying Decentralization" – introduced Nakamoto Coefficient

Decentralization Metrics Across Blockchains



Nakamoto Coefficient measures minimum entities needed to control 51%; higher is more decentralized.

Open Research Questions

Publishable Research Directions

1. **MEV and Welfare**
   - RQ: Does MEV extraction improve or harm price discovery?
   - Method: Compare execution quality with/without MEV protection
   - Gap: Welfare analysis beyond simple rent extraction
2. **PoS Security Over Time**
   - RQ: How does stake distribution evolve, and what are security implications?
   - Method: Longitudinal analysis of validator concentration
   - Gap: Limited long-run PoS data (Ethereum PoS since 2022)
3. **Optimal Fee Mechanisms**
   - RQ: What is the welfare-maximizing transaction fee mechanism?
   - Method: Mechanism design with realistic user heterogeneity
   - Gap: EIP-1559 not proven optimal; alternatives underexplored

---

Game theory + empirics combination is fruitful for blockchain research

Exercises

Mathematical
Derive the selfish mining threshold.
Given:

- Attacker: α hash rate
- Propagation: γ

Show profitability requires:

$$\alpha > \frac{1-\gamma}{3-2\gamma}$$

Empirical
Using Etherscan/Dune:

1. Track validator distribution
2. Compute Nakamoto coefficient
3. Analyze trends over 6 months

Data: Dune Analytics

Research Proposal
Draft 1-page proposal:

- "MEV and Retail Execution"
- Define MEV exposure measure
- Identify affected transactions
- Welfare implications

Due: Week 8 – Selfish mining derivation follows Eyal-Sirer closely

Blockchain provides unusually good public data for empirical research

Required Readings

Core Papers (Read Before Class)

1. **Eyal & Sirer** (2014). "Majority is Not Enough: Bitcoin Mining is Vulnerable." *FC 2014*.
   - Focus: Selfish mining strategy, threshold derivation
2. **Roughgarden** (2020). "Transaction Fee Mechanism Design for the Ethereum Blockchain." *EC 2021*.
   - Focus: EIP-1559 analysis, incentive compatibility

Supplementary

- Nakamoto (2008): Bitcoin whitepaper – foundational
- Buterin et al. (2020): Casper/Ethereum 2.0 – PoS design
- MDPI Jan 2024: "Game-Theory-Based Incentive Design for Blockchain"

Eyal-Sirer changed the conversation on PoW security; Roughgarden is mechanism design master