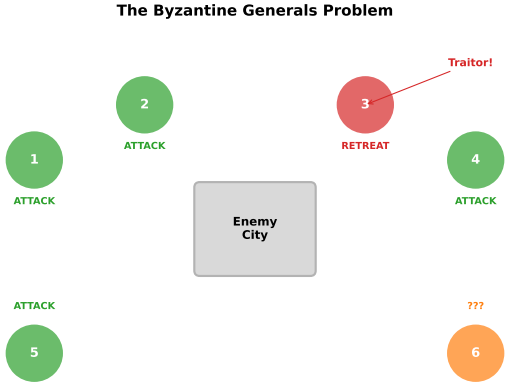
Consensus Mechanisms

Lesson 4: Summary

Prof. Joerg Osterrieder

Spring 2026

The Byzantine Generals Problem



Problem: Agree on truth when some participants may be malicious.

Bitco

solved this for open networks using economic incentives

Proof of Work

How It Works:

- Find nonce: $H(\text{block}) < \text{target}$
- Requires massive computation
- Easy to verify, hard to produce

Security: 51% attack requires majority hash power (billions \$). **Trade-off:** High energy use, slow finality, but proven security.

Convert electricity into security

Proof of Stake

How It Works:

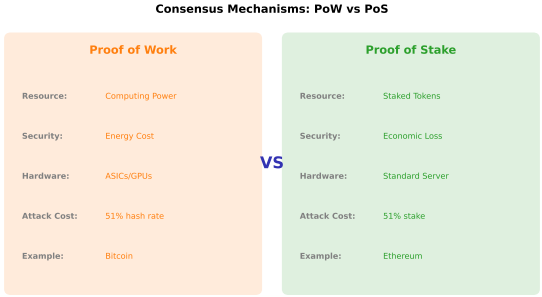
- Validators stake tokens as collateral
- Selected randomly weighted by stake
- Malicious behavior = slashing (lose stake)

Security: Attack requires majority of staked tokens. **Trade-off:** Energy efficient but newer, less battle-tested.

PoS:

Convert capital at risk into security

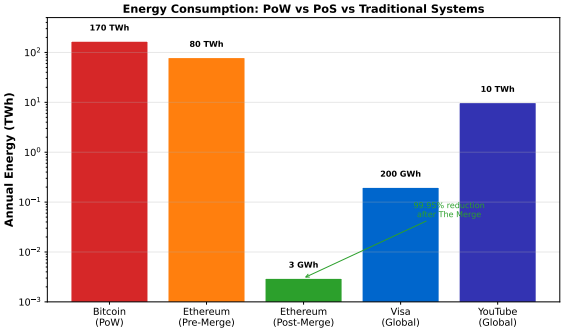
PoW vs PoS



PoW

spend energy — PoS: risk capital

Energy Comparison



Ether

99.95% energy reduction after switching to PoS

Other Mechanisms

DPoS: Vote for delegates, fast but centralized.
PBFT: Known validators, deterministic finality, doesn't scale.
PoA: Identity at stake, efficient but requires trust.

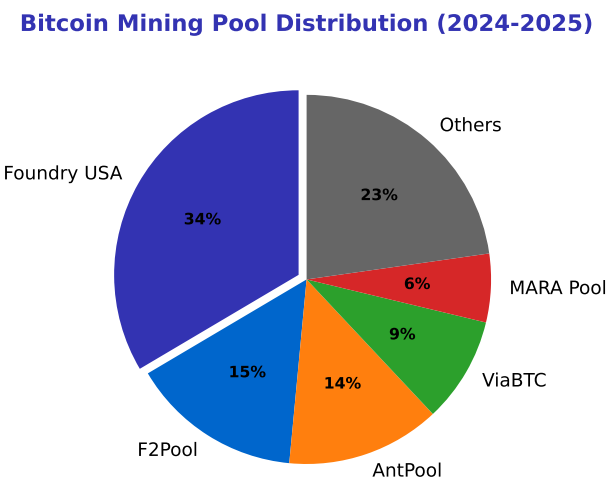
The Trilemma: Cannot optimize all three:

- Security + Decentralization + Scalability

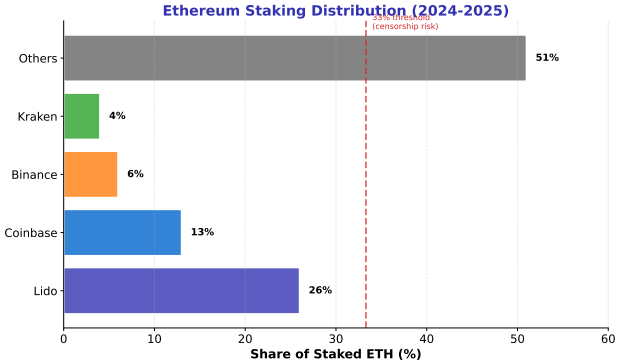
Every

mechanism makes trade-offs

Mining Pool Distribution



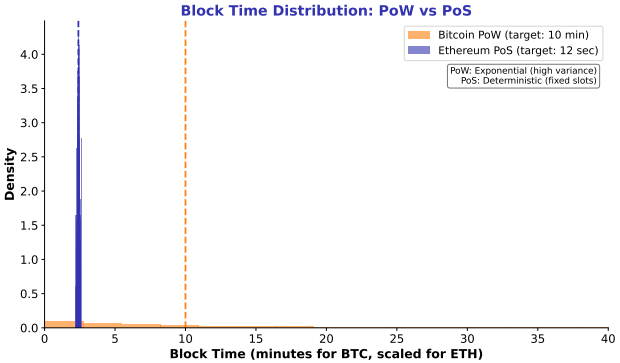
Staking Concentration



staking protocols dominate—raises centralization concerns

Liqui

Block Time Variance



PoW has high variance (Poisson), PoS more predictable

Key Takeaways

1. **Byzantine problem**: Agreement with potential traitors
2. **PoW**: Proven security, high energy
3. **PoS**: Energy efficient, newer
4. **Trilemma**: Cannot have all three

Core Insight: Consensus converts scarce resources into security.

Next:

Token Economics

Thank You

Questions?