Blockchain Fundamentals

A Visual Introduction

Standalone Mini-Lecture

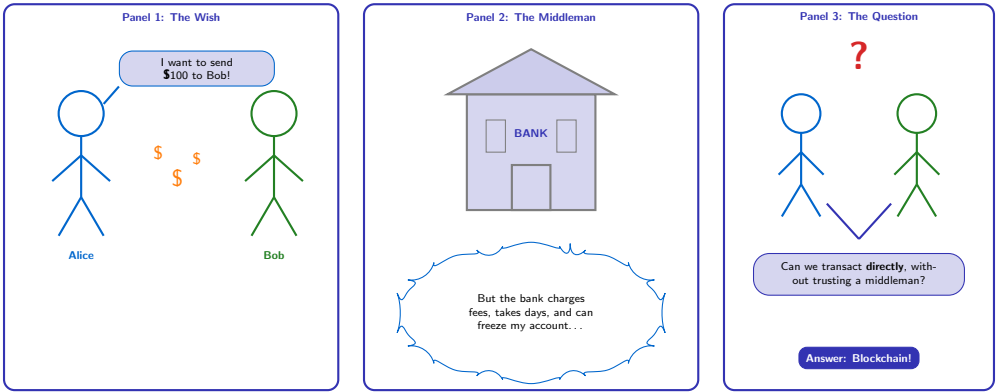
"A digital chain of trust"

Prof. Dr. Joerg Osterrieder

University Lecture Series

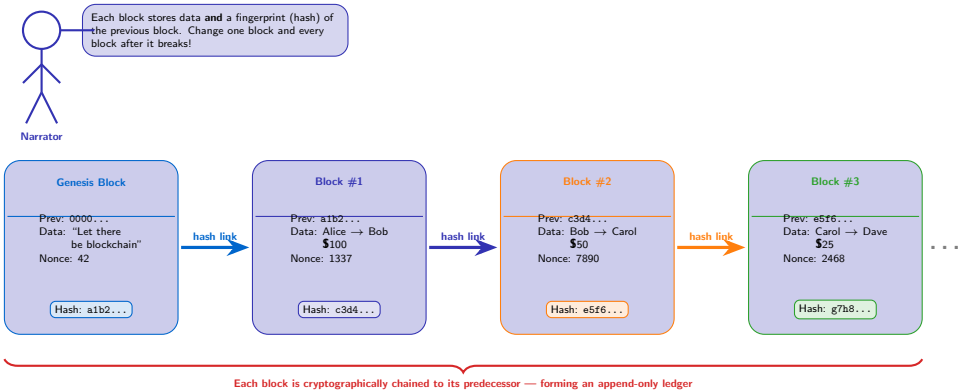
February 25, 2026

The Trust Problem



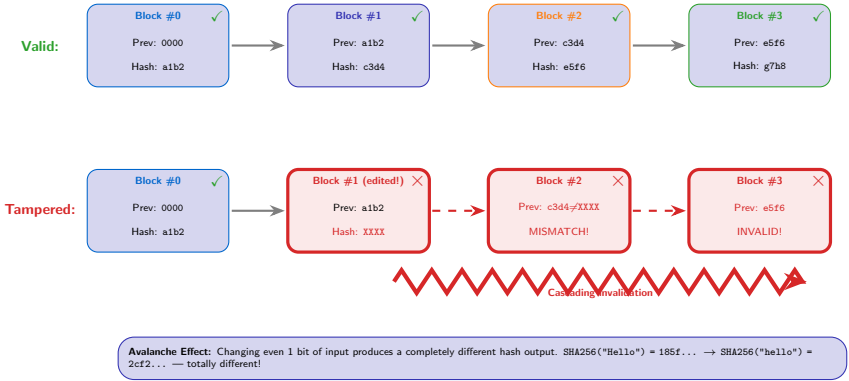
Key insight: Blockchain solves the double-spending problem without requiring a trusted intermediary.

Chaining Blocks Together



Source: Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System." Each block's hash includes the previous block's hash, creating an unbreakable chain.

Immutability: Why You Cannot Cheat



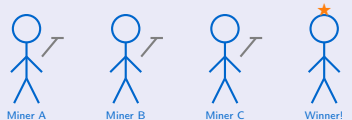
Key insight: Tampering with one block invalidates every subsequent block, making fraud computationally infeasible.

Consensus: How the Network Agrees

Proof of Work (PoW)

Analogy: A Computational Lottery

Miners compete to solve a puzzle (find a nonce that makes the block hash start with N zeros). The winner gets to add the next block and earns a reward.

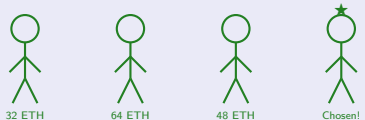


Trade-off: Extremely energy-intensive — Bitcoin uses more electricity than many countries

Proof of Stake (PoS)

Analogy: Skin in the Game

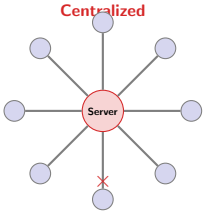
Validators lock up ("stake") their own coins as collateral. The protocol randomly selects a validator, weighted by stake. Cheaters lose their staked coins ("slashing").



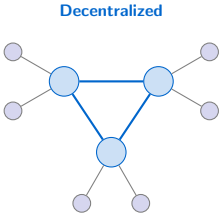
Advantage: >99.9% less energy than PoW — Ethereum switched to PoS in Sept 2022 ("The Merge")

Source: Ethereum Foundation, 2022. PoW secures via computational cost; PoS secures via economic penalty.

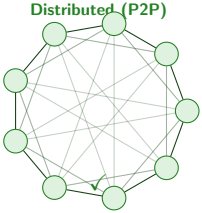
Decentralization: No Single Point of Failure



Single point of failure.
If the server goes down,
everyone loses access.



Multiple hubs share control.
Better, but hubs are still
critical coordination points.



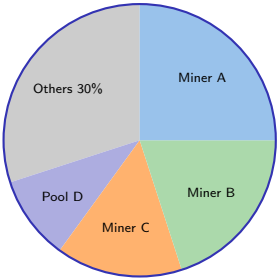
Every node is equal.
No single point of failure.
This is how blockchains work.

Centralized: Bank, Google, Facebook **Decentralized:** Federated systems **Distributed:** Bitcoin, Ethereum

Key insight: True decentralization means no entity can unilaterally censor, modify, or halt the network.

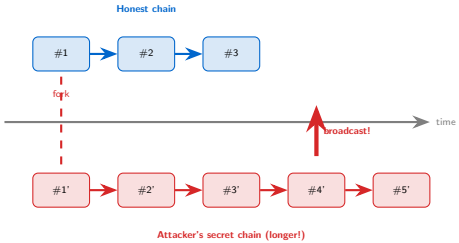
Risks: The 51% Attack

Hash Power Distribution



Healthy: No one controls >50%

Attack Scenario



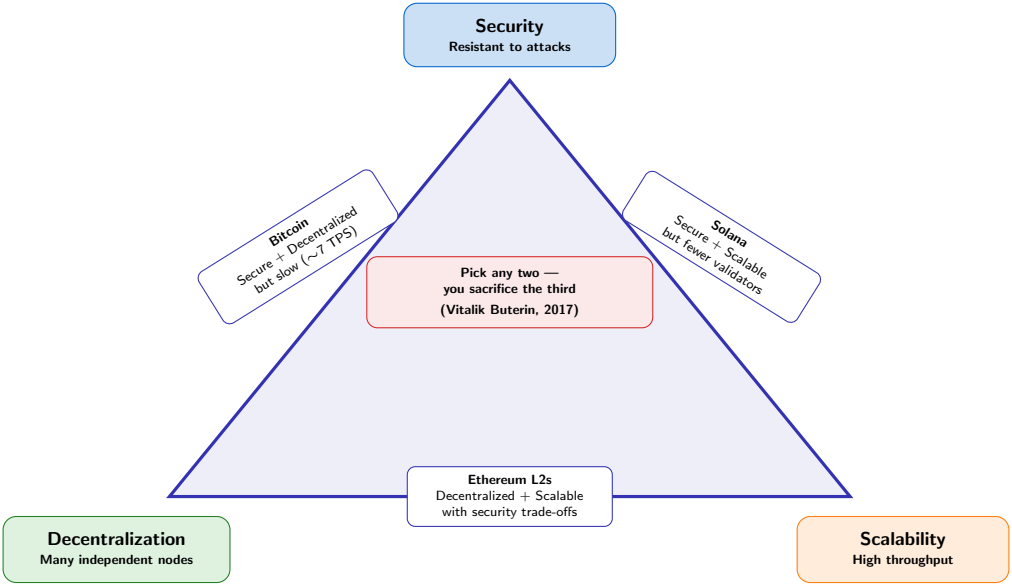
Network accepts the longer chain
→ honest transactions **reversed**

Mitigation Strategies

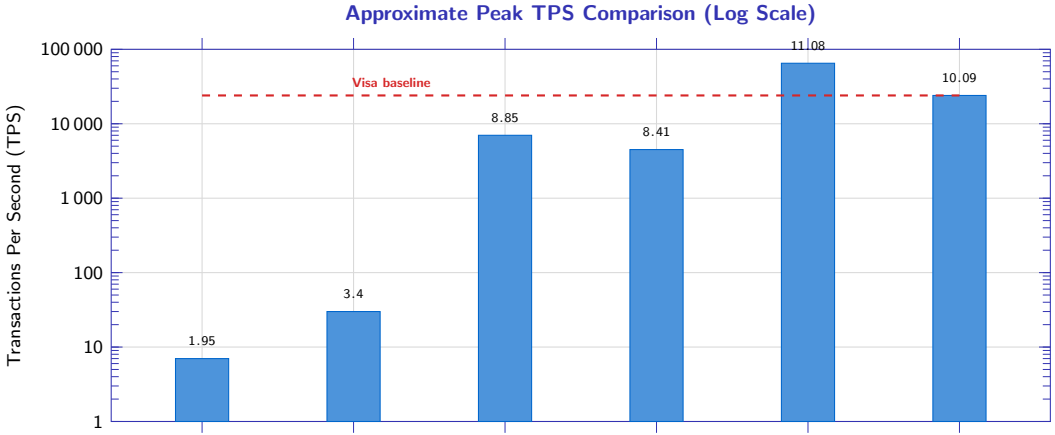
- Wait for multiple confirmations (Bitcoin: 6 blocks ≈ 60 minutes)
- Economic cost: attacking Bitcoin would require **$**billions in hardware
- PoS makes attacks even costlier (attacker's stake gets "slashed")

Source: Majority attacks have occurred on smaller chains (Ethereum Classic, 2019; Bitcoin Gold, 2018).

The Scalability Trilemma



Blockchain by the Numbers: Transactions Per Second



Note: Theoretical peak TPS varies significantly from real-world sustained throughput. Bitcoin ≈7, Ethereum ≈15–30 (pre-sharding), Solana claimed peak ≈65,000. Visa processes ≈24,000 TPS on average. Layer 2 solutions (rollups) aim to bridge this gap.

Source: Data approximate as of 2024. Actual throughput depends on network conditions, block size, and consensus parameters.

Takeaways and Evaluation Framework

Key Concepts Covered

1. **Trust Problem** — Why intermediaries are costly
2. **Block Chaining** — Hash-linked append-only ledger
3. **Immutability** — Tamper-evident via cryptographic hashing
4. **Consensus** — PoW (lottery) vs. PoS (stake)
5. **Decentralization** — No single point of failure
6. **51% Attack** — Majority control risk
7. **Scalability Trilemma** — Security vs. decentralization vs. throughput

5-Point Evaluation Framework

For any blockchain project, ask:

1. ☐ Is it truly **decentralized**?
2. ☐ Is the ledger **immutable**?
3. ☐ Are transactions **transparent**?
4. ☐ Can it **scale** to real-world demand?
5. ☐ Is it **secure** against known attacks?

Remember: Blockchain is not a solution to every problem. Apply the 5-point framework to distinguish genuine innovation from hype. *"Not your keys, not your coins."* — The crypto community mantra.

Key insight: A strong blockchain project should score well on all five criteria. Trade-offs are inevitable — understand them.