Bitcoin: A Peer-to-Peer Electronic Cash System

Financial Technologies and Applications (T-714-FINT)

Giorgio Saldana

Reykjavík University

29 November 2024

Problem Statement and Motivation

- Traditional electronic payments rely on trusted third parties (e.g., financial institutions).
- Issues:
  - High costs due to mediation.
  - Non-reversible payments are difficult, limiting their utility.
- **Solution:** A cryptographic, peer-to-peer electronic payment system with irreversible transactions, avoiding reliance on third parties.

Coin and Transaction Definition to Avoid Central Authority

- **Coin:** A chain of digital signatures.
- **Transaction:** Ownership transfer through signing a hash of the previous transaction and new owner's public key.
- **Double-Spending Problem:** A coin used in multiple transactions simultaneously.
- **Solution:** Public announcement system ensuring a consensus on transaction history.

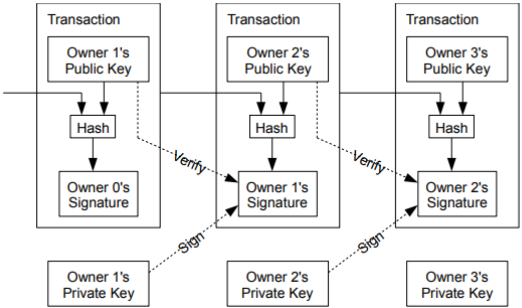

Figure 1: Transaction diagram

Solution: A Timestamp Server

Use of a **timestamp server** to solve double-spending:

- Timestamp a block of transactions.
- Hash linked to the previous block, creating an immutable chain.

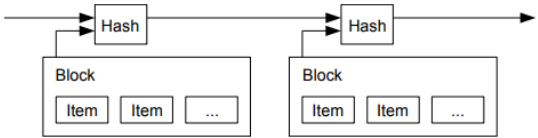

Figure 2: Timestamp-server

Proof of Work (PoW) to Implement Distributed TS

- Hash computation with k leading zeros using:
  - **Nonce** and **previous block's hash**.
- **Majority Decision:**
  - Longest chain = most PoW invested.
  - Honest nodes collectively overpower attackers, preserving security.

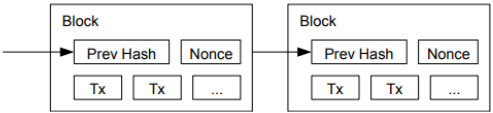

Figure 3: Proof of Work

Network Composition

(1) Transactions broadcasted to all nodes.
(2) Nodes collect and mine transactions into blocks.
(3) Longest chain is accepted.
(4) Nodes save alternative branches if they may become the longest.
(5) Minimal structure ensures robustness.

Incentives for Network Sustainability

- **Mining Reward:** First transaction in a block creates a new coin for the miner.
- **Transaction Fees:** Encourages honest participation.
- **Greedy Attackers:** Better off adhering to rules for higher rewards.

Disk Space Optimization via Merkle Tree

- Use of **Merkle Trees** to compact data:
  - Only root hash is stored in blocks.
  - Prune unnecessary branches.
- Results in efficient storage and scalability.

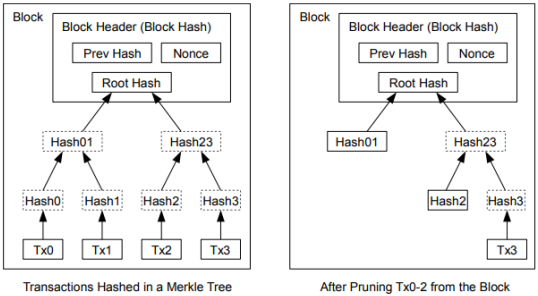

Figure 4: Merkle Tree Pruning

Verifying Payments

- Simplified Payment Verification (SPV):
  - Keep only block headers of the longest chain.
  - Verify transactions via Merkle branches.

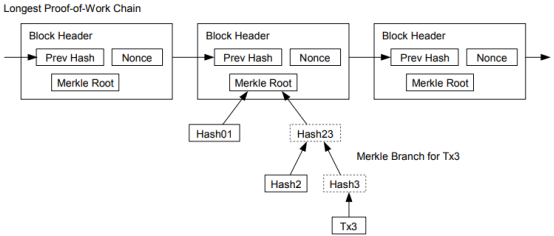

Figure 5: Payments Verification

Privacy in Bitcoin

- Transactions publicly announced but maintain pseudonymity:
  - Anonymous public keys.
  - New key pairs for each transaction.
- Multi-input transactions may reveal linkages.

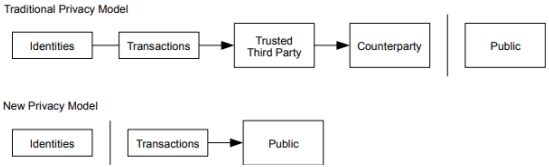

Figure 6: Privacy Model

Probability of Network Attack

- **Attacker Chain vs Honest Chain:**
  - Binomial Random Walk modeling.
- **Parameters:**
  - p: Probability an honest node finds the next block.
  - q: Probability an attacker finds the next block ($q < p$).
  - z: Number of blocks by which the honest chain is ahead of the attacker.
- **Relation to z:**
  - As z increases, the probability of an attacker catching up diminishes exponentially.
  - The attacker's chain must overcome the increasing lead of the honest chain, making success progressively less likely.
- Modeled as a Gambler's Ruin problem.

```
q=0.1
z=0     P=1.0000000
z=1     P=0.2045873
z=2     P=0.0509779
z=3     P=0.0131722
z=4     P=0.0034552
z=5     P=0.0009137
z=6     P=0.0002428
z=7     P=0.0000647
z=8     P=0.0000173
z=9     P=0.0000046
z=10    P=0.0000012

q=0.3
z=0     P=1.0000000
z=5     P=0.1773523
z=10    P=0.0416605
z=15    P=0.0101008
z=20    P=0.0024804
z=25    P=0.0006132
z=30    P=0.0001522
z=35    P=0.0000379
z=40    P=0.0000095
z=45    P=0.0000024
z=50    P=0.0000006
```

Figure 7: Probability of Successful Attacks ($q = 0.1$)

Conclusion

- Introduced a decentralized, trustless system for electronic transactions.
- Double-spending problem solved with:
  - Timestamp server.
  - Proof-of-work.
- Network incentivized and sustainable.
- Secure and scalable solution for digital cash.