THE GRAINGER COLLEGE OF ENGINEERING
SIEBEL SCHOOL OF COMPUTING AND DATA SCIENCE

CS 521

Technological Foundations of Blockchain and Cryptocurrency

Grigore Rosu

Topic 3 – Bitcoin

ILLINOIS

Early Cryptographic Digital Currencies … All Failed

- DigiCash (David Chaum) – 1989
- Mondex (National Westminster Bank) - 1993
- CyberCash (Lynch, Melton, Crocker & Wilson) – 1994
- E-gold (Gold & Silver Reserve) – 1996
- Hashcash (Adam Back) – 1997
- Bit Gold (Nick Szabo) – 1998
- B-Money (Wei Dai) - 1998
- Lucre (Ben Laurie) – 1999

Why did Early Digital Currencies Fail?

- Merchant adoption
- Centralization
- Double spending
- Consensus

Double Spend attack

- A simple attack:
  - When one person can use the same coin multiple times to buy things
- Easily solved with a centralized system
- Much harder when decentralized

The Riddle Remained

How to move value
peer-to-peer
without any
trusted central intermediary

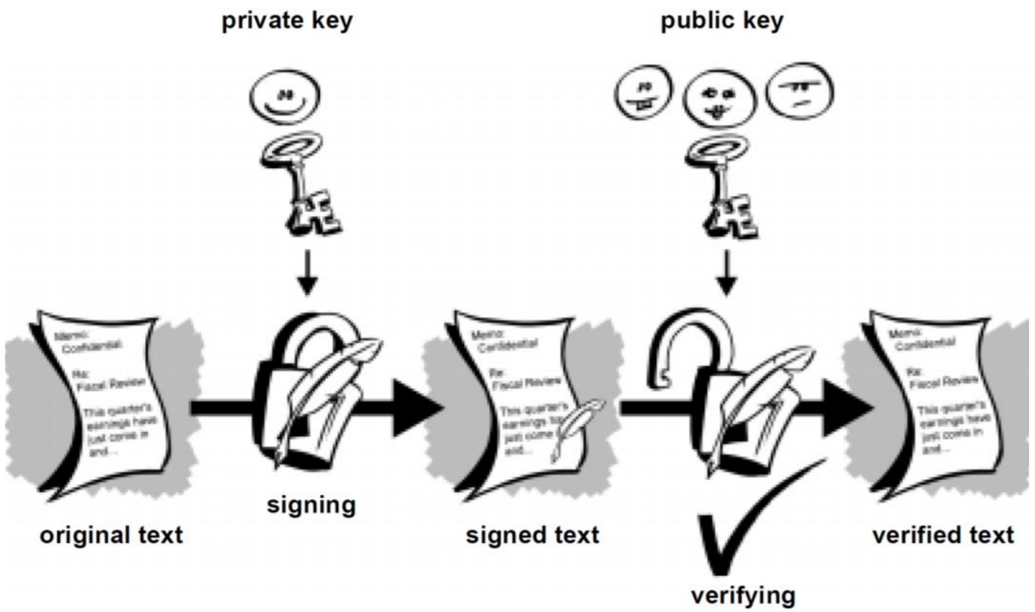
Bitcoin: A Peer-to-Peer Electronic Cash System

- From: Satoshi Nakamoto <satoshi <at> vistomail.com>
  Subject: Bitcoin P2P e-cash paper
  Newsgroups: gmane.comp.encryption.general
  Date: Friday 31st October 2008 18:10:00 UTC

- “I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.”

Bitcoin's Goal

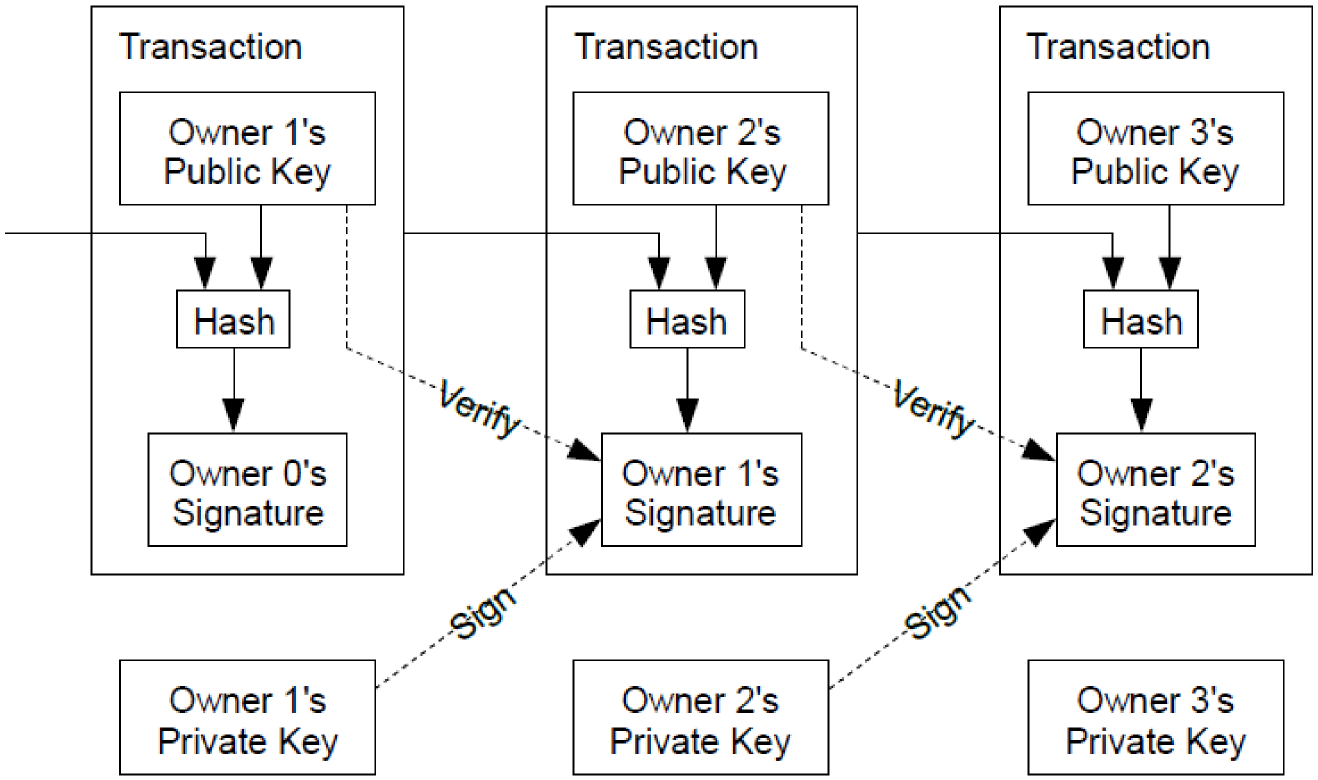
- Peer-to-peer digital money
  - No intermediaries (banks, centralized parties)
- Digital signatures were clearly the right direction



  - But the double-spending riddle could not be solved
  - Centralized / intermediary can solve double-spending, but defies the purpose

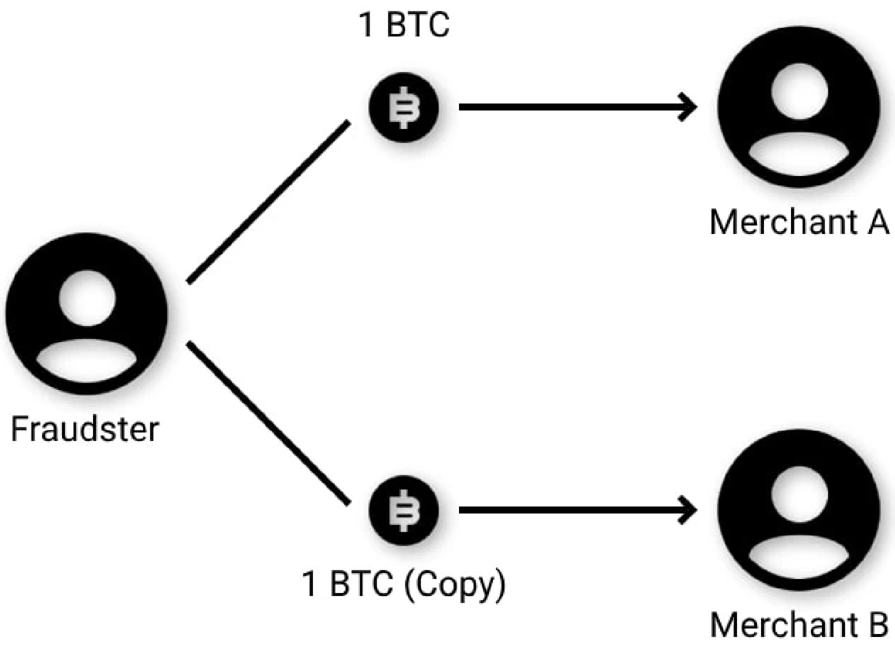
Coins and Transactions

- Coins and transfers
  - Coin: chain of digital signatures (hash pointer list data-structure)
  - Transfer C from A to B: C’ = sign(A, hash(C,B))



Double Spending

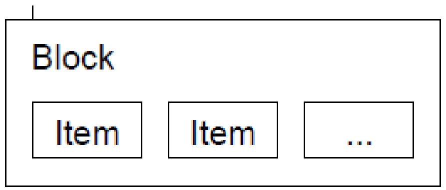
- So far nothing to stop a fraudster to send the same coin to two parties



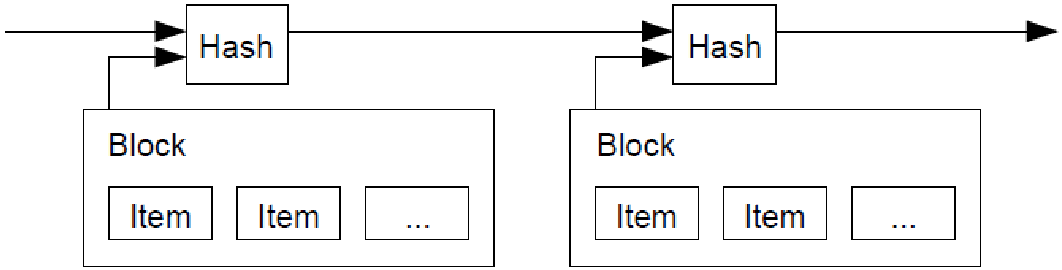
- Solution: enforce with a very high probability, a total order on transactions

Timestamp Servers: Blocks and Total Orders

- Put each transaction in a totally-ordered block of transactions
  - This is the only way transactions get communicated



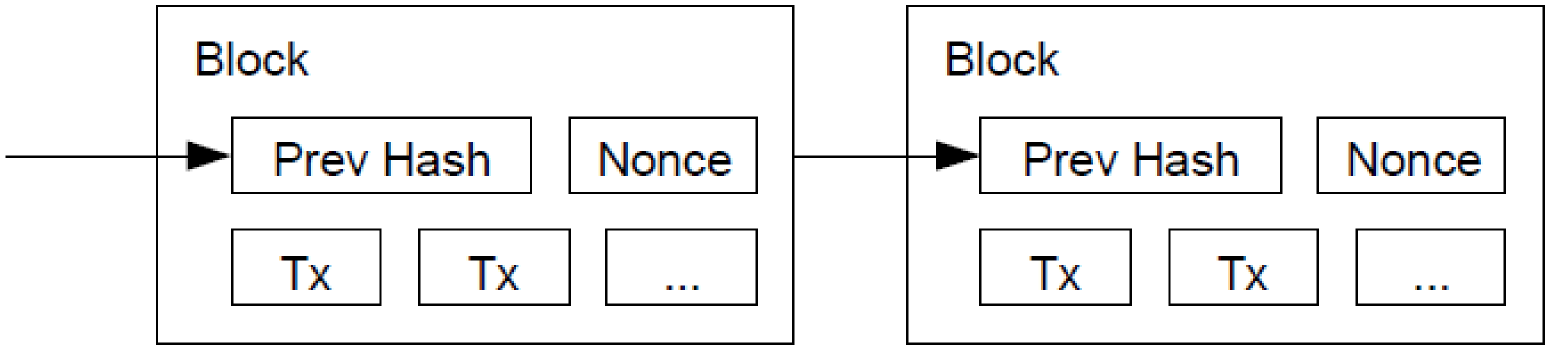
- Linked list of hash pointers to enforce total order on blocks:



- Problem of divergence remains, but lifted from transactions to blocks
- Need to enforce total order on blocks; in a decentralized way

Proof-of-Work

- Idea
  - Have only one block proposer at a time, but who?
  - Whoever solves a puzzle generation challenge first (recall previous lecture)
    - Requires computational power, so solving it is … proof of work
- Specifically, the puzzle challenge is to find Nonce in the block such that the hash of the block is smaller than an epsilon (hash starting with zeros)



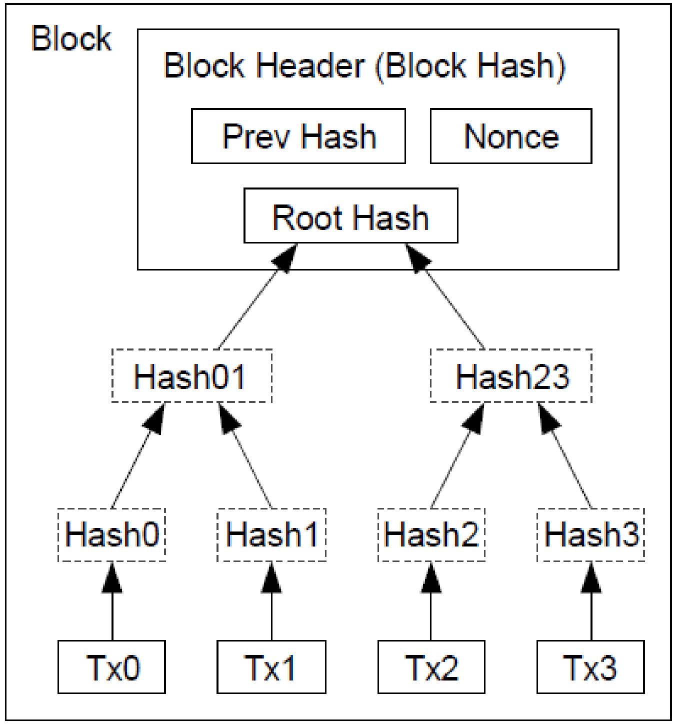
- Easy to verify that such Nonce is indeed correct, so all nodes update chain
- Problem of divergence still exists in theory; but nodes pick longest chain

Decentralized Network

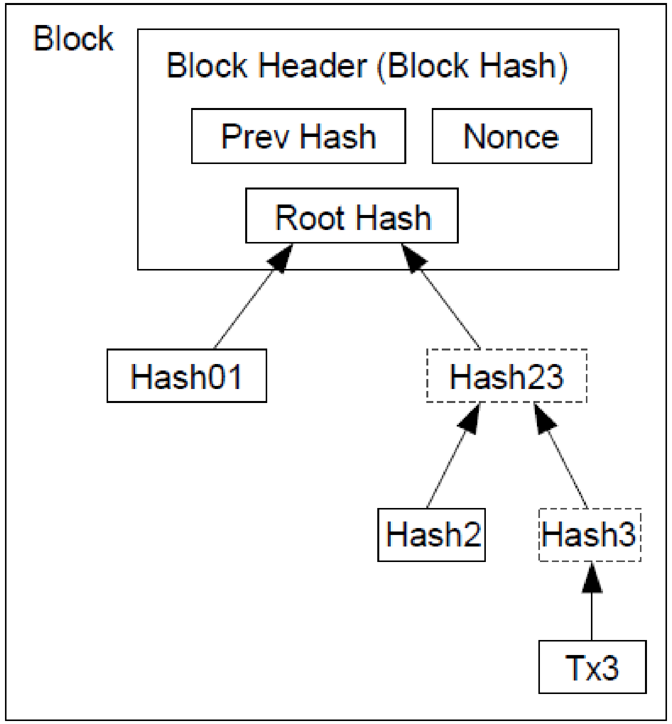
- Nodes can join and leave. They all execute the same protocol:
  1. New transactions are broadcast to all nodes.
  2. Each node collects new transactions into a block.
  3. Each node works on finding a difficult proof-of-work for its block.
  4. When a node finds a proof-of-work, it broadcasts the block to all nodes.
  5. Nodes accept the block only if all transactions in it are valid and not already spent.
  6. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.
- Nodes always consider the longest chain
- Economic incentive:
  – First transaction in the block is a new coin owned by the block creator/proposer/miner

Reclaiming Space

- Transactions need not be stored on-chain
- Stored in Merkle-tree, whose root hash is stored on-chain



Transactions Hashed in a Merkle Tree



After Pruning Tx0-2 from the Block

Proving / Verifying Payment

- Transactions need not be stored on-chain
- Stored in Merkle-tree, whose root hash is stored on-chain