

Principals and Practice of Cryptocurrencies

Cornell CS 5437, Spring 2016

Introduction

Principals and Practice of Cryptocurrencies



- Probability
- Distributed systems
- Game theory
- Cryptography

- Design choices
- Real-world challenges
- Analysis tools
- **Project**

- Practical decentralized currencies of the Bitcoin family
- Older and newer systems

Staff

Instructor

Ittay Eyal

455 Gates Hall

ittay.eyal@cornell.edu start title with [CS 5437]

Teaching Assistant – HW grading

Kyle Croman

411 Gates Hall

kcroman@cs.cornell.edu start title with [CS 5437]

Material

- **Text books**
 - **Bitcoin and Cryptocurrency Technologies**
Narayanan, Bonneau, Felten, Miller, Goldfeder; Princeton, 2015
<https://piazza.com/princeton/spring2015/btctech/resources>
 - **Mastering Bitcoin**
Antonopoulos; O'reilly, 2014
<http://chimera.labs.oreilly.com/books/1234000001802>
- **Lecture**
- **Papers**
- **Book chapters**

Prerequisites

- Algorithms
- Protocols
- Operating systems
 - Programming intensive
- Probability – an advantage
- Distributed systems theory – an advantage

Grade

- **Homework:** 30%
 - n assignments ($n \approx 10$)
 - Average of best $n - 2$
 - Much of the grade for submission
 - -25% per day late (4 days for free)
- **Project:** 60%
Details in next lesson
- **Other factors:** 10%

Plan

- First week { 1. Overview
2. Projects
- Rest of semester { 3. Principals and practice of Cryptocurrencies

Before Money



Barter

Forms of Money



Commodity money

- Divisible
- Stable value
- Scarcity is key



Forms of Money

Commodity money

- Divisible
- Stable value
- Scarcity is key

Representative money

- Easier to transact
- Enforced unforgeability



Token



Ledger

Forms of Money



Commodity money

- Divisible
- Stable value
- Scarcity is key

Representative money

- Easier to transact
- Enforced unforgeability

Fiat State Money

- Controlled scarcity



Forms of Money

Commodity money

- Divisible
- Stable value
- Scarcity is key

Representative money

- Easier to transact
- ~~Enforced unforgeability~~

Fiat State Money

- ~~Controlled scarcity~~

Decentralized Cyber-currencies

- No single trusted entity
- Protocol-controlled scarcity
- Protocol-enforced unforgeability
- Rich API



Bitcoin

2008: The Bitcoin white paper

2009: Reference implementation



Probably not this guy

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto

satoshin@gmx.com

www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers

Cyber-Currencies Uses

Credit card transaction

1. Alice gives Bob CC number
2. Bob gets money from CC company
3. CC company gets money from Alice

Bank transaction

1. Alice orders bank to pay Bob
2. Bank(s) update records



Cryptocurrency transaction

1. Alice pays Bob over Internet

Don't trust merchant and credit card



Cyber-Currencies Uses

No middleman: Micropayments, Cheap remittance

**WESTERN
UNION**

**Send warm
wishes today.**

FOR ONLY SEND UP TO
\$5/\$50
TRANSFER FEE

FOR PICKUP WITHIN THE U.S.

moving money for better

 **bitcoin**

**Send warm
wishes 24/7.**

FOR ONLY SEND UP TO
\$0.01/\$ANY
TRANSFER FEE AMOUNT

FOR PICKUP ANYWHERE

moving money far better

Cyber-Currencies Uses

No capital controls

- Iceland,
- Cyprus,
- Greece










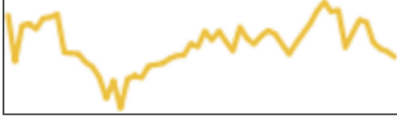




Cyber-Currencies Uses

Novel applications

- Money and beyond

Market Capitalization

| # | Name | Market Cap | Price | Available Supply | Volume (24h) | % Change (24h) | Price Graph (7d) |
|---|--|------------------|-------------|----------------------|---------------|----------------|---|
| 1 |  Bitcoin | \$ 6,853,992,723 | \$ 455.16 | 15,058,425 BTC | \$ 58,426,200 | 0.59 % |  |
| 2 |  Ripple | \$ 199,987,108 | \$ 0.005963 | 33,537,439,933 XRP * | \$ 311,546 | -1.14 % |  |
| 3 |  Litecoin | \$ 157,101,570 | \$ 3.57 | 43,958,267 LTC | \$ 2,705,570 | 0.30 % |  |
| 4 |  Ethereum | \$ 73,999,243 | \$ 0.972451 | 76,095,600 ETH | \$ 449,255 | 2.49 % |  |
| 5 |  Dash | \$ 20,574,049 | \$ 3.36 | 6,128,263 DASH | \$ 86,774 | 0.67 % |  |
| 6 |  Dogecoin | \$ 14,907,216 | \$ 0.000145 | 102,558,705,957 DOGE | \$ 164,465 | 3.86 % |  |

Research and Industry

- Wide academic interest
 - Top security conferences
 - Specialized workshops
- Startups funded by almost \$1B
 - Dealing with Bitcoin / alt-coins
 - Developing new coins
- World's largest financial institutions studying the technology (e.g. Citi, Nasdaq, UBS, SWIFT, Barclays)
- IBM started “Open Ledger” for cryptocurrency-based R&D
- Intel, Microsoft studying the technology

Financial Institutions Invested in Bitcoin



Wallets



Roles

- Generate private keys
- Store private keys
- Monitor incoming transactions
- Authorize transactions

Types

- Local
- Online service
- Dedicated hardware

Payment Services



- Handle payments for merchants
- Merchants see fiat currency
- Mask exchange rate fluctuations
- Mask cryptocurrency security challenges

Exchanges

Online exchange services
between currencies



Types

- Alt-coin only
- Alt-coin and fiat

Challenges

- Operational: like any exchange
- Legal: per jurisdiction

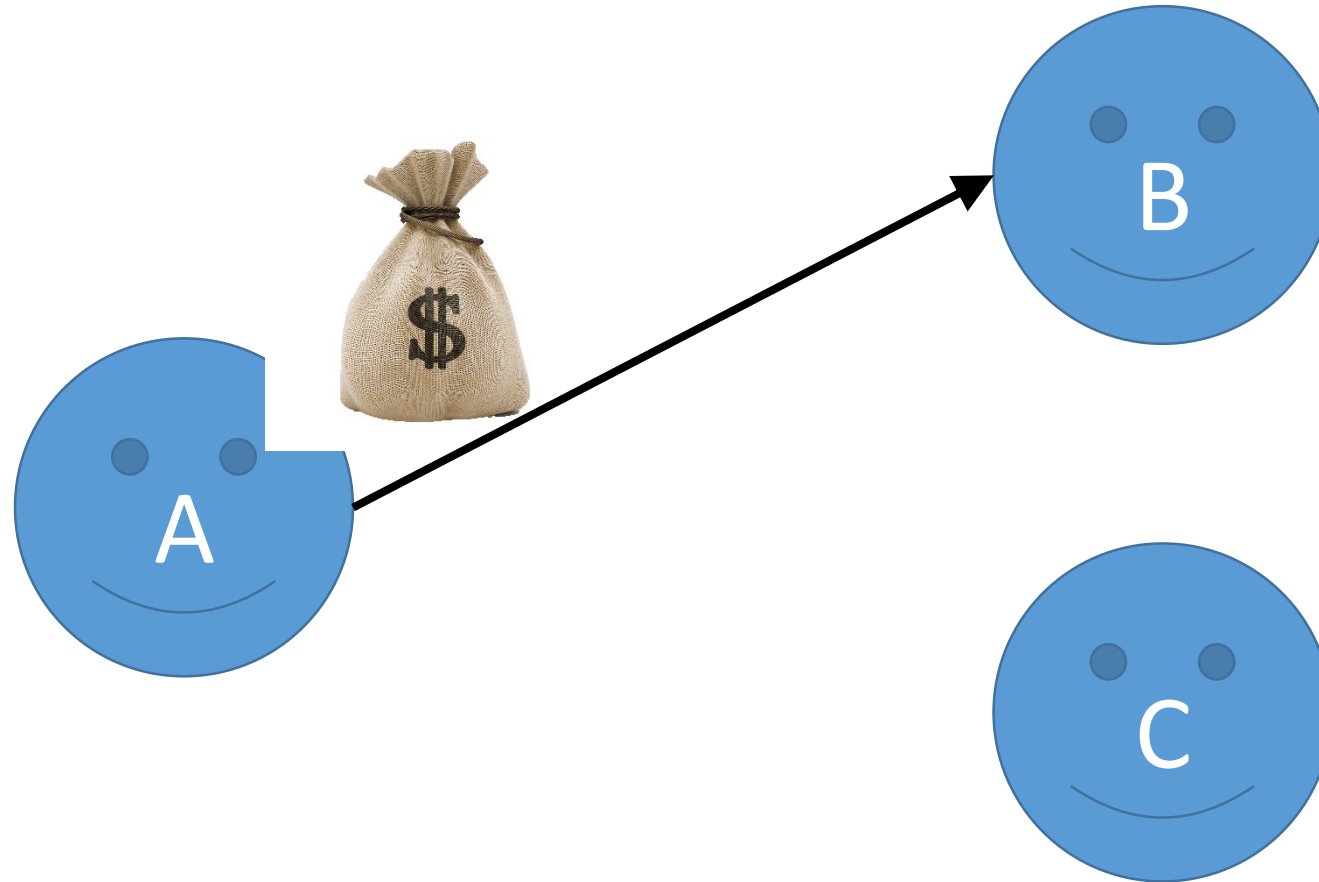
Applications



- Notary service
- Self-enforced games
- Secure gambling
- Offline transactions

Developing a Cryptocurrency

Key Challenges



1. **No stealing: Only Alice can move her money**
2. Minting: Fair money creation
3. No double-spending: Alice cannot duplicate her money

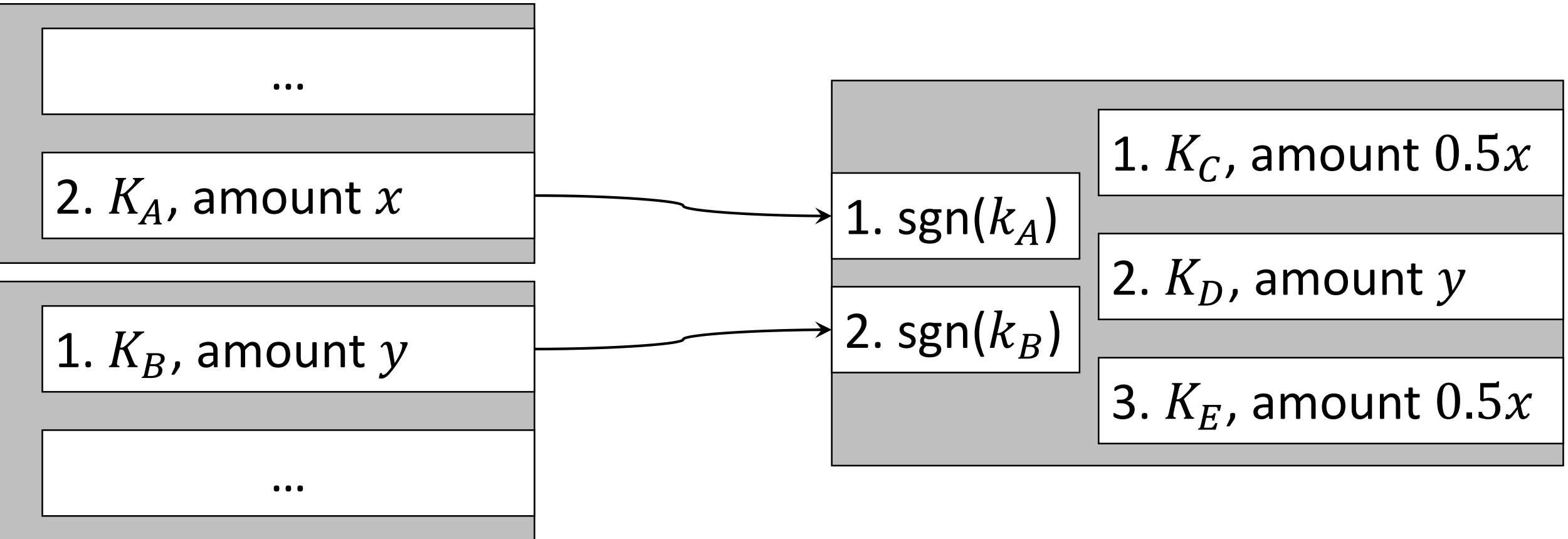
60 Seconds on Public Key Signatures

Alice generates key pair

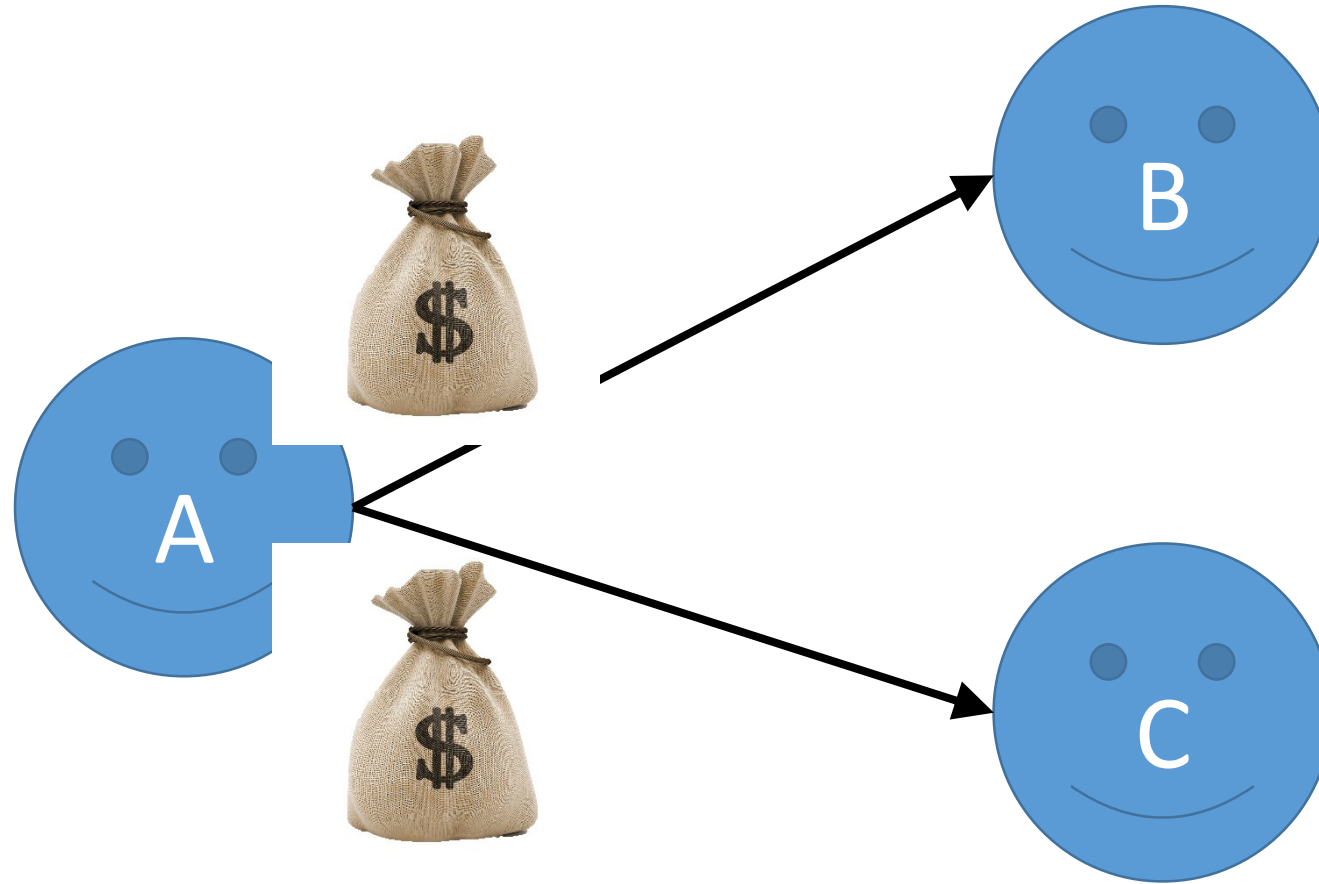
1. private key k_A , kept secret
2. public key K_A , published with ***public key infrastructure***

- Alice signs a message m with private key k_A , generating a signature s .
- Anyone can verify that s is a signature of m with key k_A given m and K_A .

Addresses and Transactions

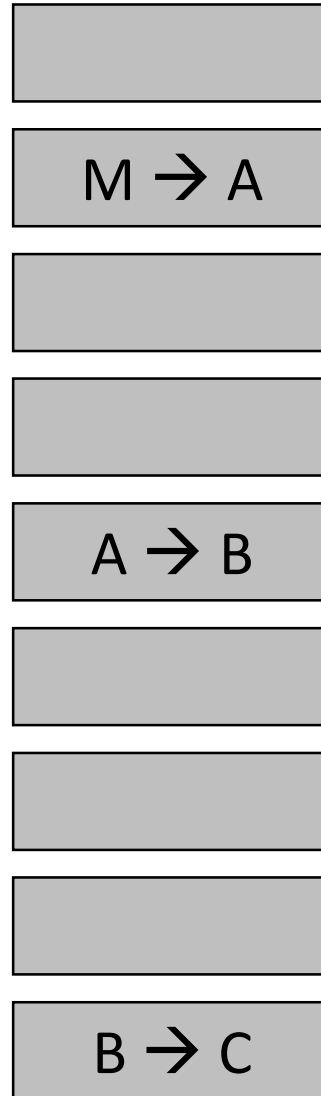


Key Challenges

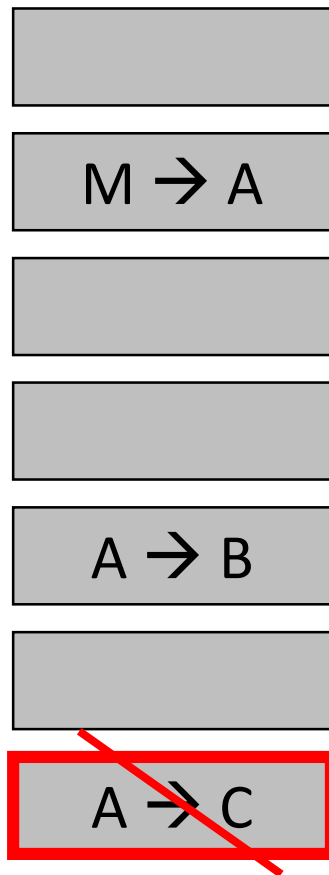


1. No stealing: Only Alice can move her money
- 2. No double-spending: Alice cannot duplicate her money**
3. Minting: Fair money creation

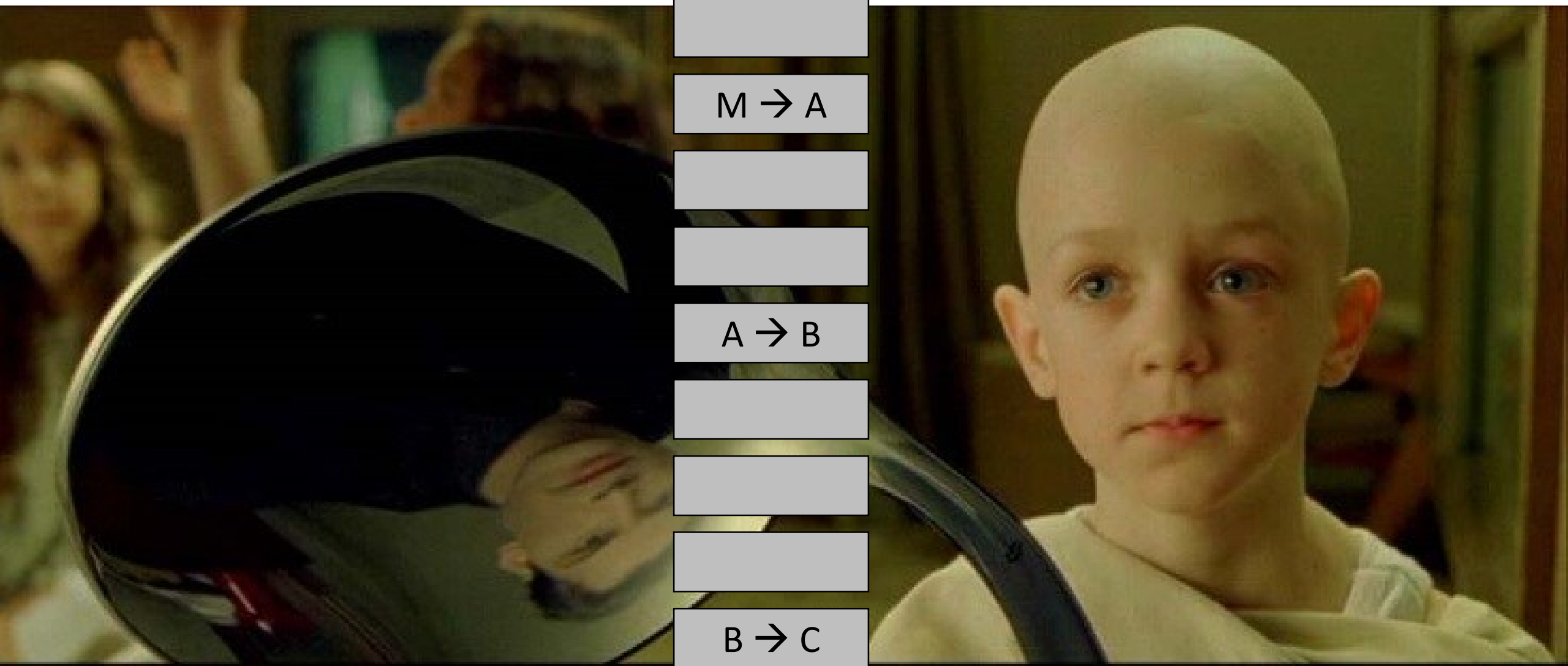
Global Ledger



Global Ledger



Global Ledger

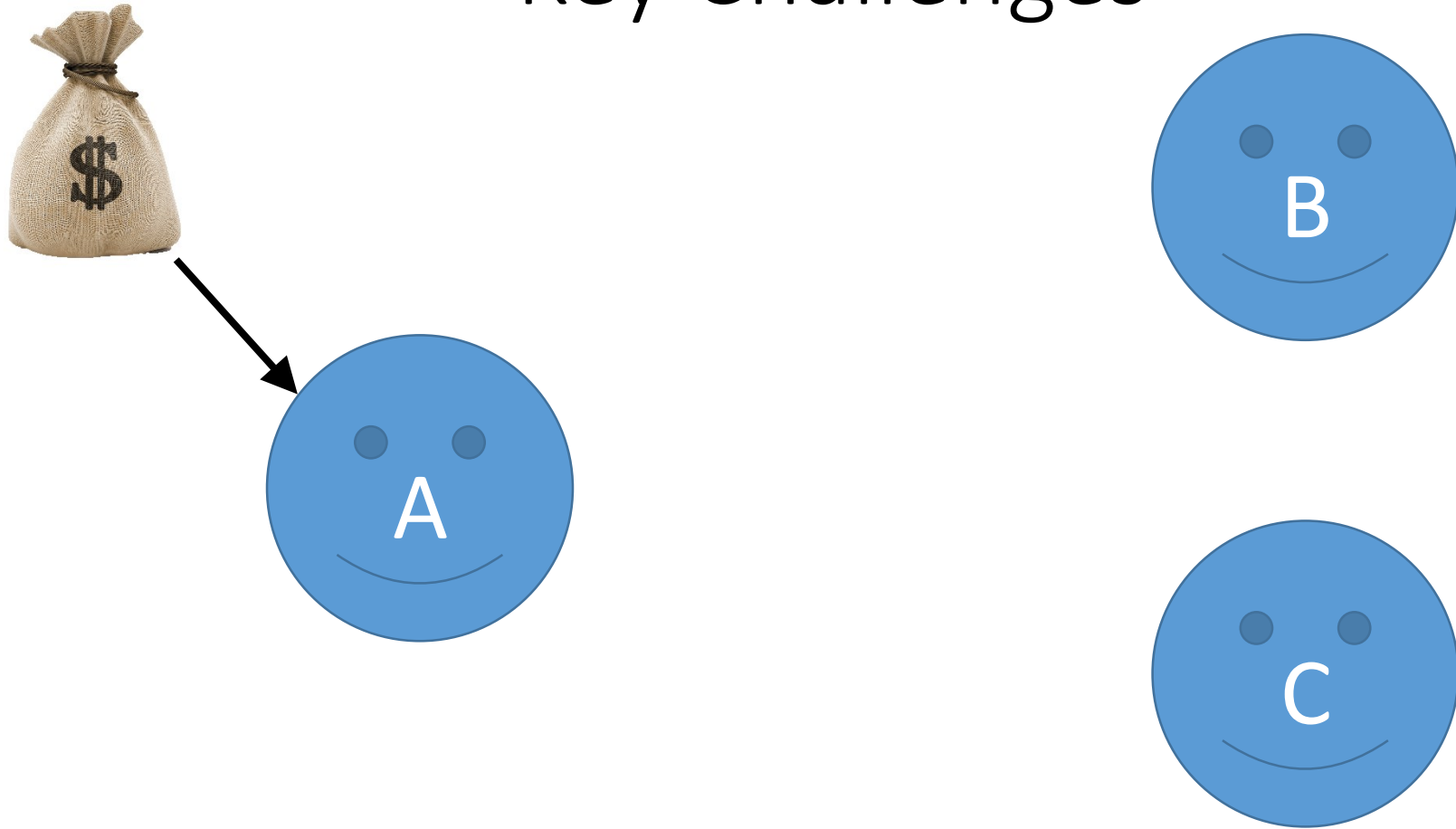


$M \rightarrow A$

$A \rightarrow B$

$B \rightarrow C$

Key Challenges



1. No stealing: Only Alice can move her money
2. No double-spending: Alice cannot duplicate her money
3. **Minting: Fair money creation**

60 Seconds on Cryptographic Hashing

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

String input

Hash
Function
 H

56293a80e0394d25
2e995f2debccea82
23e4b5b2b150bee2
12729b3b39ac4d46

256 bit number
(for example)

Given a 256bit number h , one cannot find an input string that results in h faster than repeatedly guessing inputs x and calculating $H(x)$.

Mining – Minting for Proof of Work

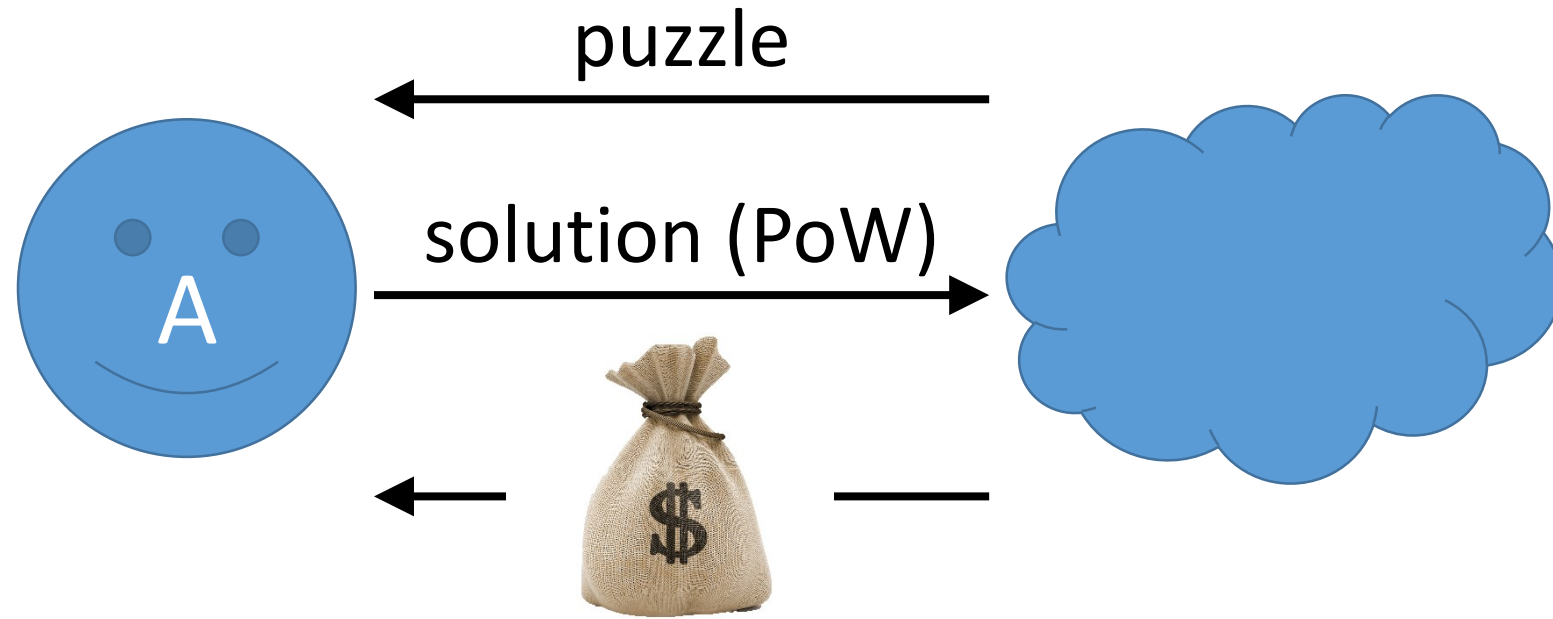
Computationally difficult puzzle:

Find x such that $H(x|y) < t$

Solver guesses values for x until finding a valid one

- Different strings y for different puzzles
- The target t determines the difficulty, average time to solve

Mining – Minting for Proof of Work



Key Challenges

1. No stealing: Only Alice can move her money

Cryptographic signatures

2. No double-spending: Alice cannot duplicate her money

Global ledger

3. Minting: Fair money creation

Mint for proof of work

Key Challenges

1. No stealing: Only Alice can move her money

Cryptographic signatures

Who runs the public key infrastructure?

2. No double-spending: Alice cannot duplicate her money

Global ledger

Who maintains the public ledger?

3. Minting: Fair money creation

Mint for proof of work

Who gives money for puzzles?

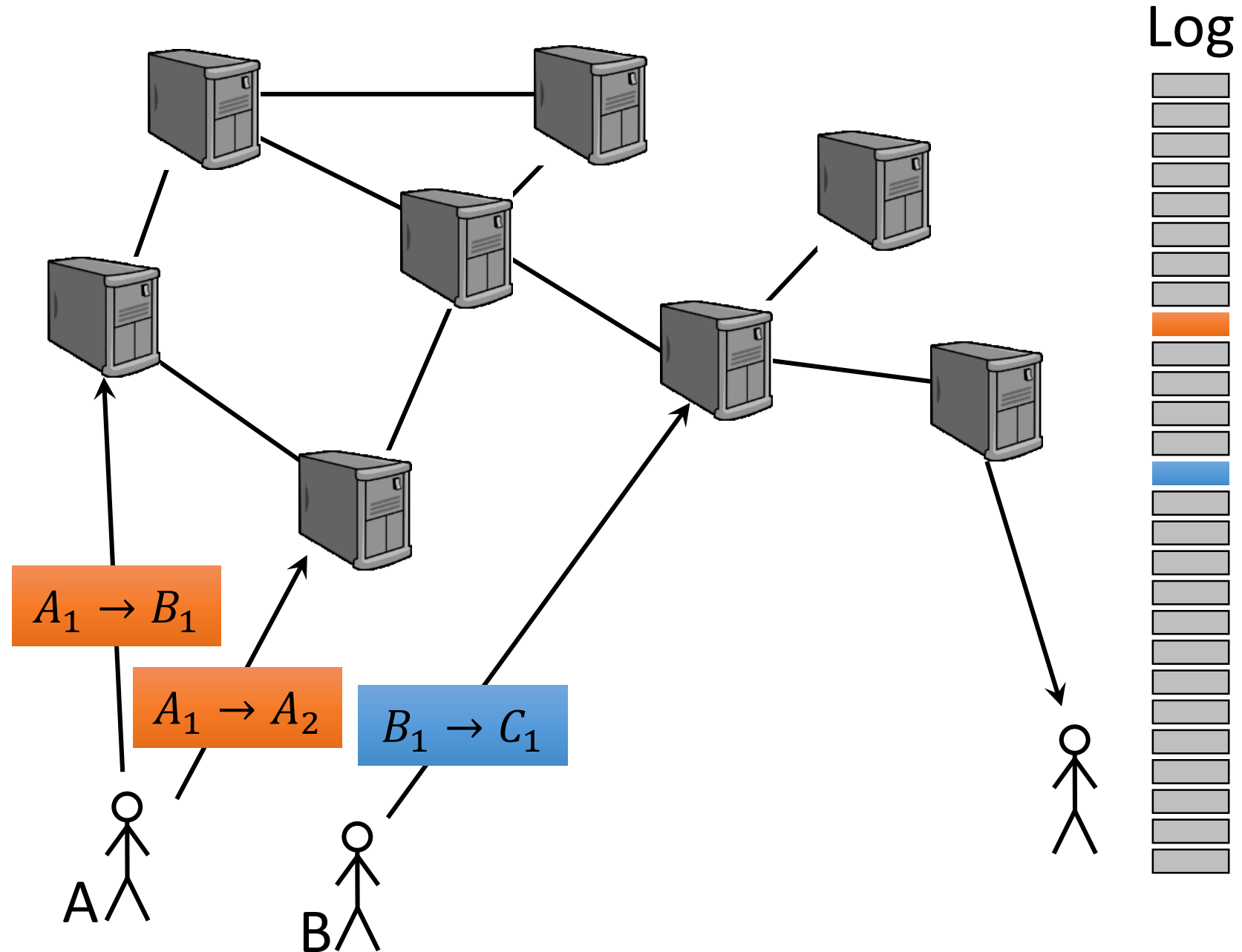
Can this be decentralized?

Replicated State Machine

- Instead of one machine, use a ***replicated state machine***
- Multiple machines operate a single ledger, PKI, and mint fairly
- A subset can behave arbitrarily – aka ***Byzantine***

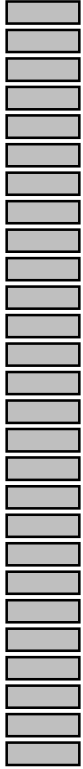
But who chooses the participating machines?

A Replicated State Machine

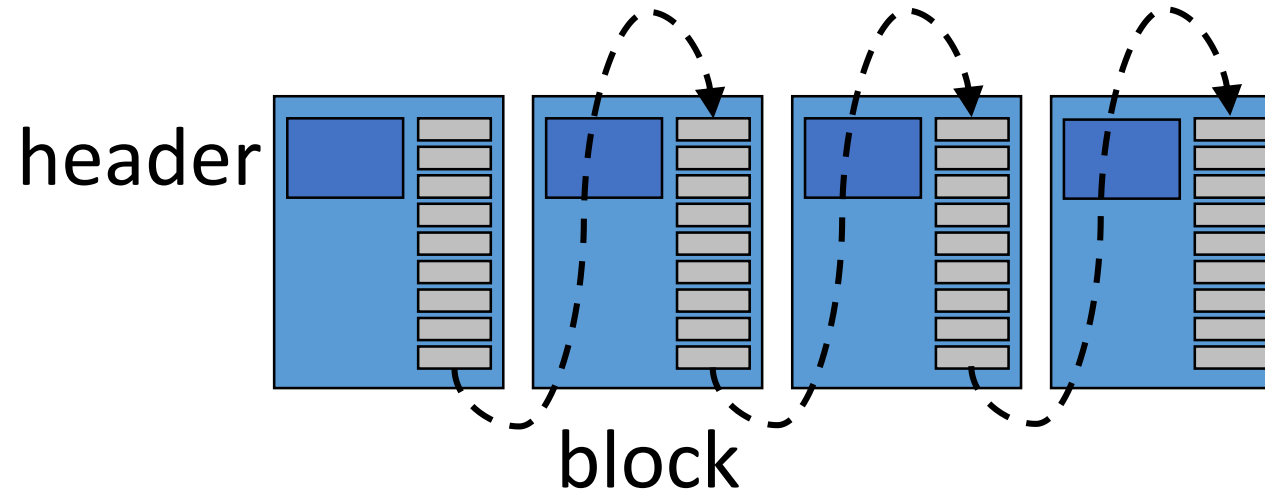


Nakamoto's Blockchain

Log

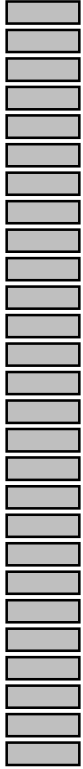


Blockchain

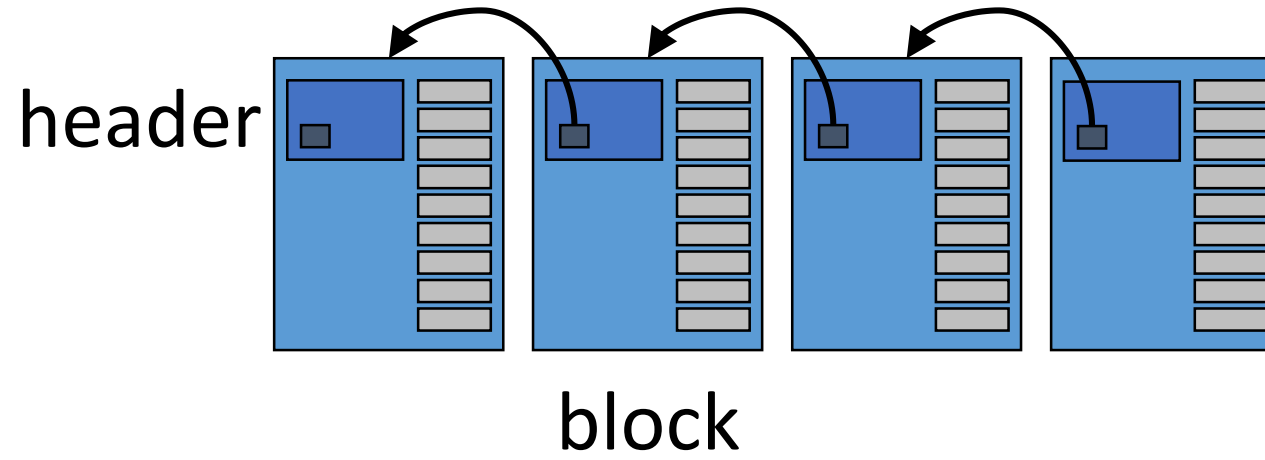


Nakamoto's Blockchain

Log

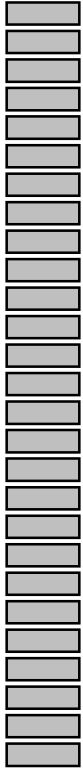


Blockchain

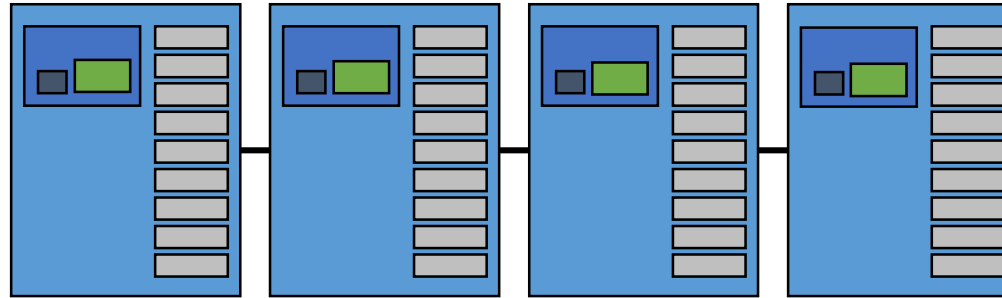


Nakamoto's Blockchain

Log



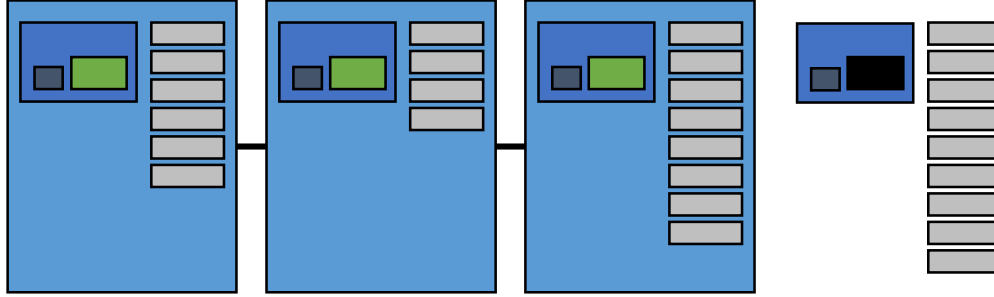
Blockchain



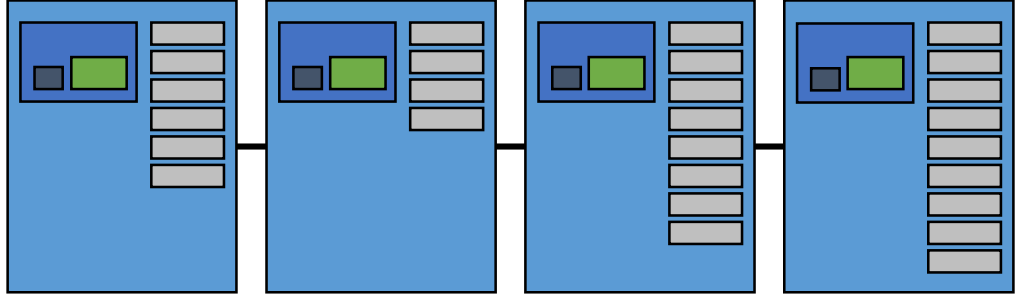
$$\text{hash}(\text{block}) < \text{target}^*$$

* *target*: a deterministic function of previous blocks

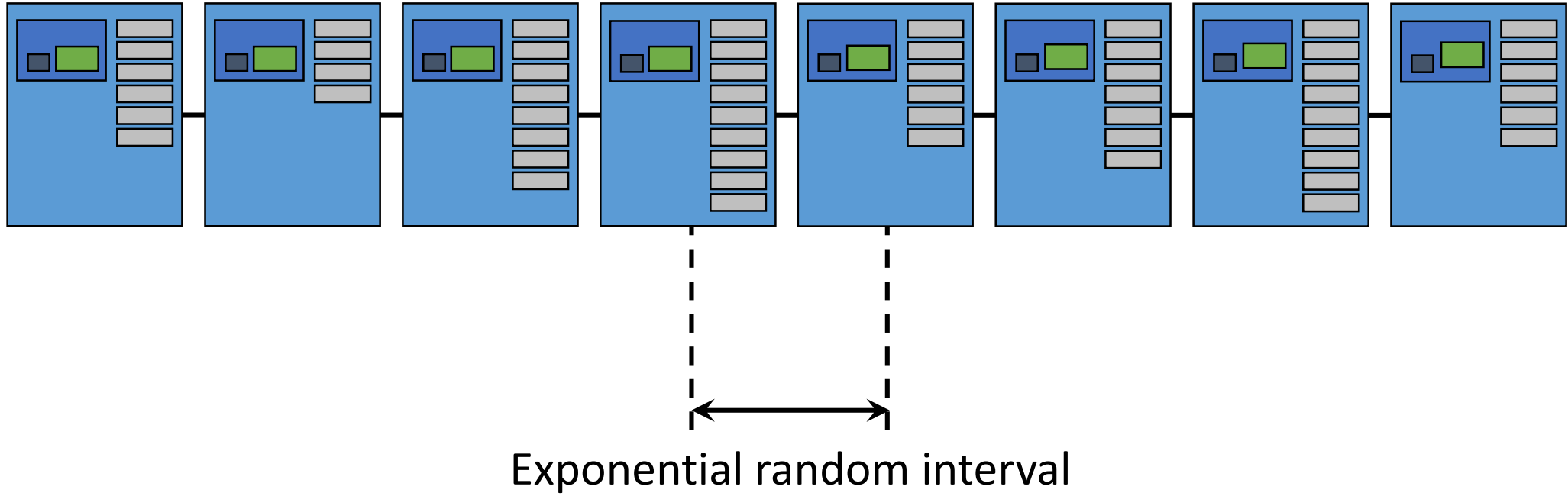
Nakamoto's Blockchain



Nakamoto's Blockchain

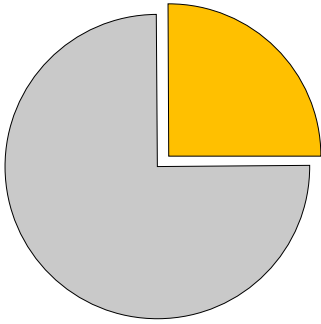
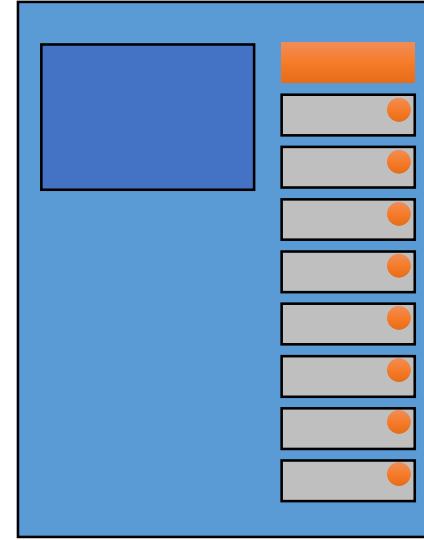


Nakamoto's Blockchain



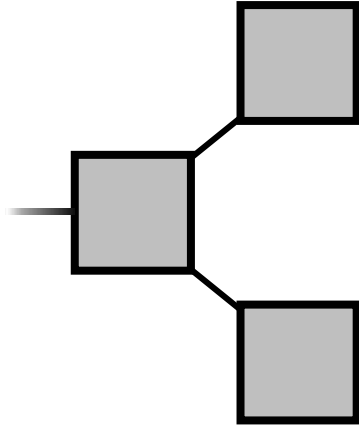
Incentive for Mining

- **Internal Prize:**
 - Minting
 - Fees



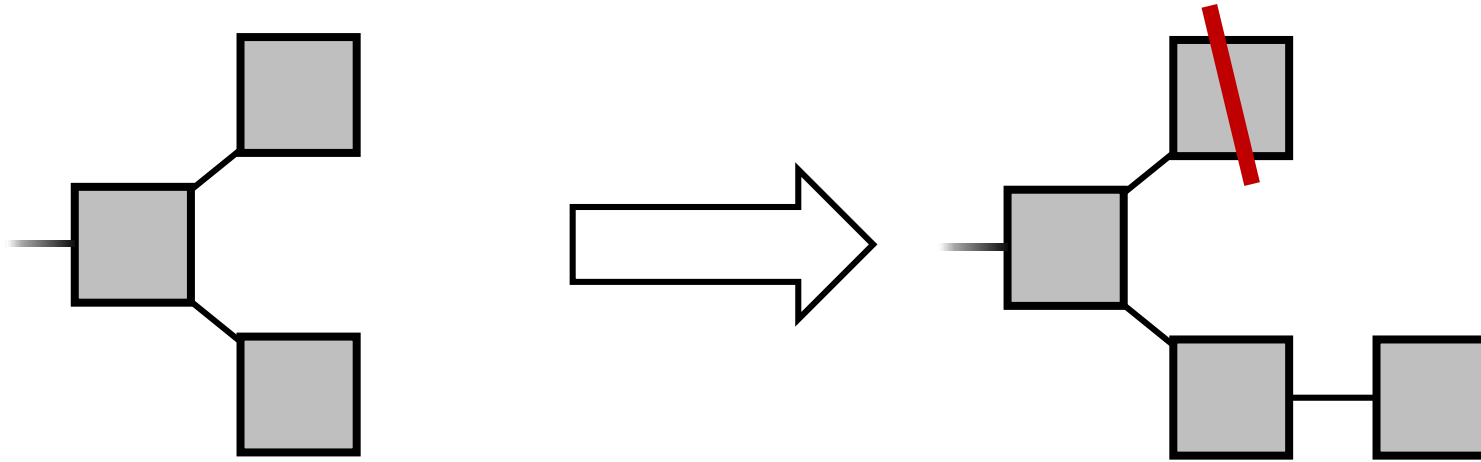
Wins proportional to computation power

Forks



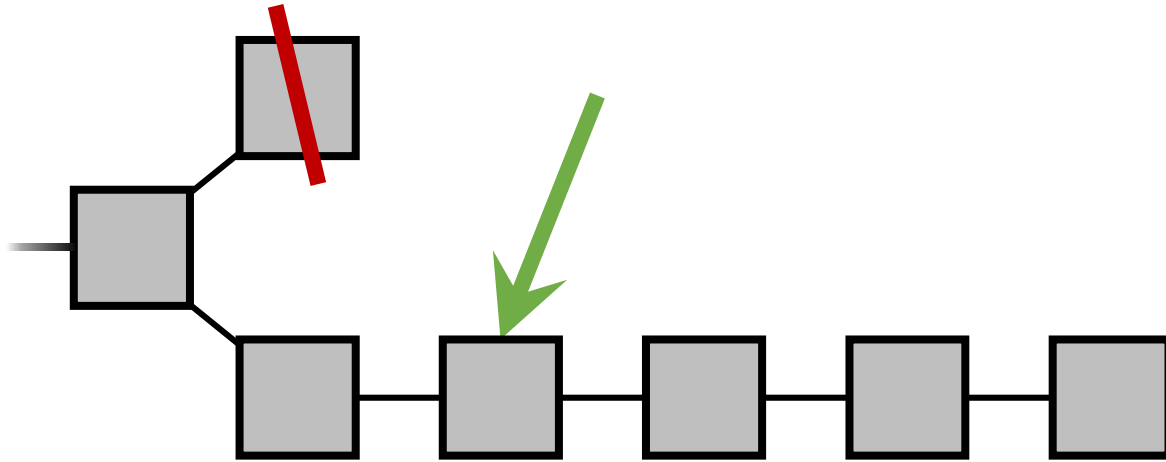
- Natural in a distributed system

Fork Resolution



- **Longest** chain wins
- Transactions are reverted
- Double-spending a threat

Fork Resolution



A transaction is **confirmed** when
it is **buried** deep enough

Key Challenges

1. No stealing: Only Alice can move her money

Cryptographic signatures

2. No double-spending: Alice cannot duplicate her money

Global ledger

3. Minting: Fair money creation

Mint for proof of work

Decentralized