Blockchain and Cryptocurrency

Reference Book

- There is enough material on the Internet and book as such is not required
- For readers interested to delve deeper: Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder, **Bitcoin and Cryptocurrency Technologies**

What is Blockchain?

- Blockchain is a system comprised of..
  - Transactions
  - Immutable ledgers
  - Decentralized peers
  - Encryption processes
  - Consensus mechanisms
  - Optional Smart Contracts

- Let’s explore these concepts

Transactions

- As with enterprise transactions today, Blockchain is a historical archive of decisions and actions taken
- Proof of history, provides provenance

Notable transaction use cases
Land registration – Replacing requirements for research of Deeds (Sweden Land Registration)
Personal Identification – Replacement of Birth/Death certificates, Driver's Licenses, Social Security Cards (Estonia)
Transportation – Bills of Lading, tracking, Certificates of Origin, International Forms (Maersk/IBM)
Banking – Document storage, increased back office efficiencies (UBS, Russia's Sberbank)
Manufacturing – Cradle to grave documentation for any assembly or sub assembly
Food distribution – Providing location, lot, harvest date Supermarkets can pin point problematic food (Walmart)
Audits – Due to the decentralized and immutable nature of Blockchain, audits will fundamentally change.

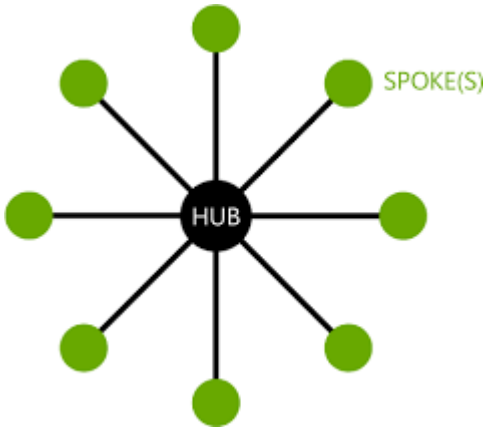
- Demo - https://anders.com/blockchain/blockchain.html

Decentralized Peers

- Rather than the centralized “Hub and Spoke” type of network, Blockchain is a decentralized peer to peer network. Where each NODE has a copy of the ledger.

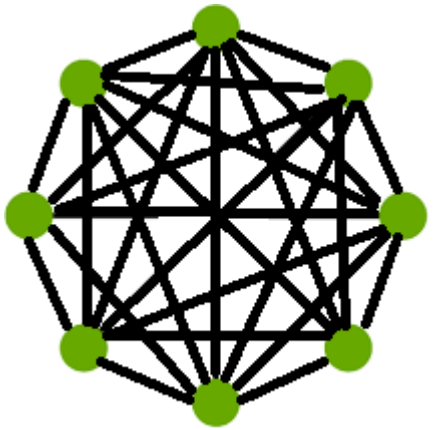
Legacy Network

Centralized DB



Blockchain Network

Distributed Ledgers



Consensus

- Ensures that the next block in a blockchain is the one and only version of the truth
- Keeps powerful adversaries from derailing the system and successfully forking the chain

Smart Contracts

- Computer code
- Provides business logic layer prior to block submission

Blockchain	Smart Contracts?	Language	
Bitcoin	No		
Ethereum	Yes	Solidity	
Hyperledger	Yes	Various	GoLang, C++, etc, depends
Others	Depends	Depends	

Blockchain Capabilities

A shared ledger technology allowing any participant in the business network to see the system of record (ledger)

Ensuring appropriate visibility; transactions are secure, authenticated & verifiable

All parties agree to network verified transaction

Business terms embedded in transaction database & executed with transactions

Blockchain Essentials

1. A business problem to be solved
   - That cannot be solved with more mature technologies
2. An identifiable business network
   - With Participants, Assets and Transactions
3. A need for trust
   - Consensus, Immutability, Finality or Provenance

Negative Indicators, Anti-Patterns

1. Need high performance (millisecond) transactions
2. Small organization (no business network)
3. Looking for a database replacement
4. Looking for a messaging replacement
5. Looking for transaction processing replacement
6. Process and metrics are not clear within the ecosystem
7. Value, velocity and/or variability are not present

Developing a Blockchain

Blockchain terminologies

- **Transaction & blocks**
  - A transaction is a value transfer; a block is a collection of transactions on the bitcoin network, gathered into a block that are hashed and added to the blockchain.

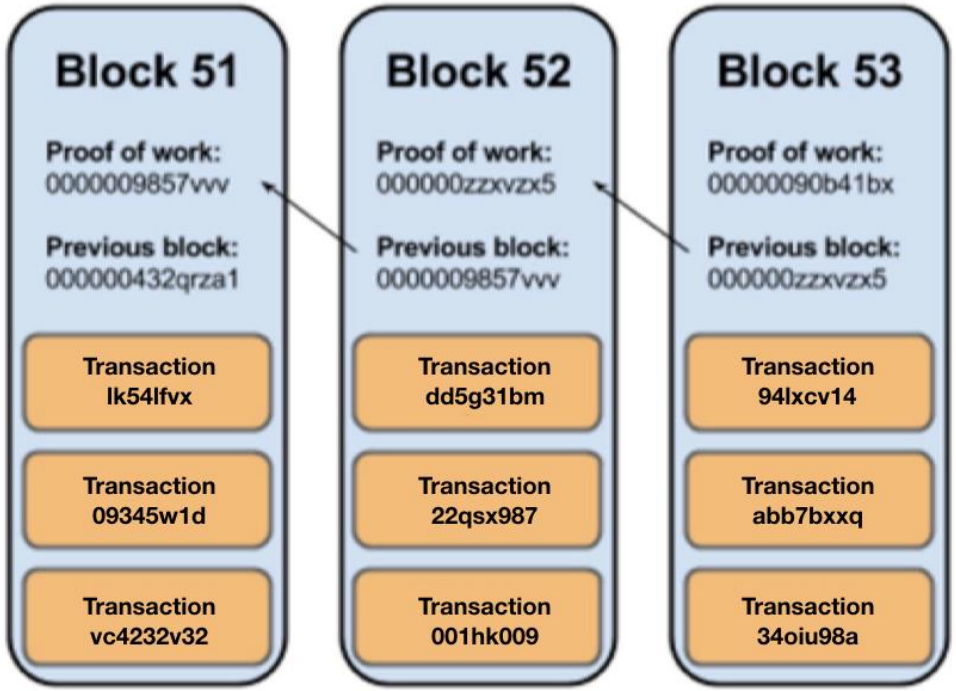
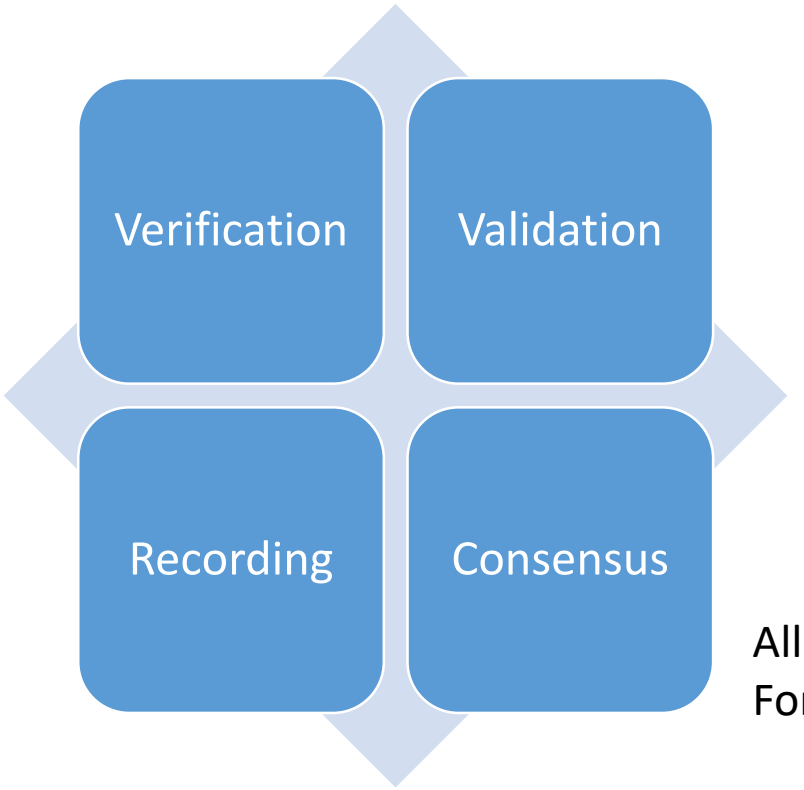
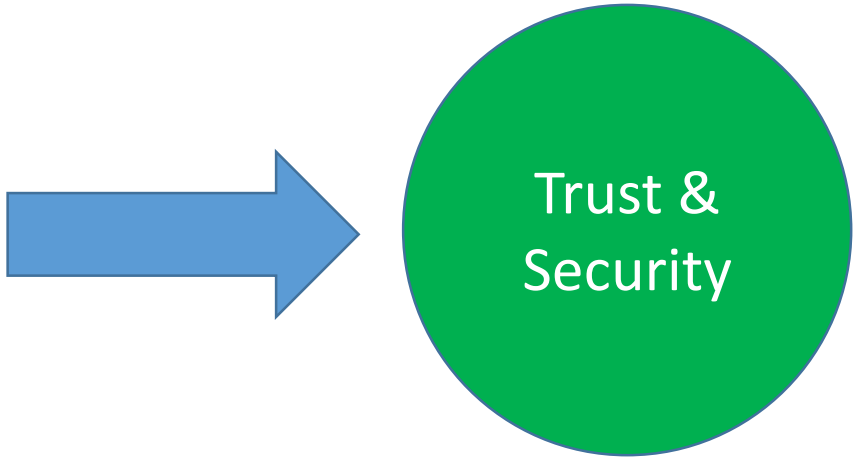


Image source: https://pplware.sapo.pt/informacao/monero-xmr-uma-moeda-segura-privada-e-sem-rasto/

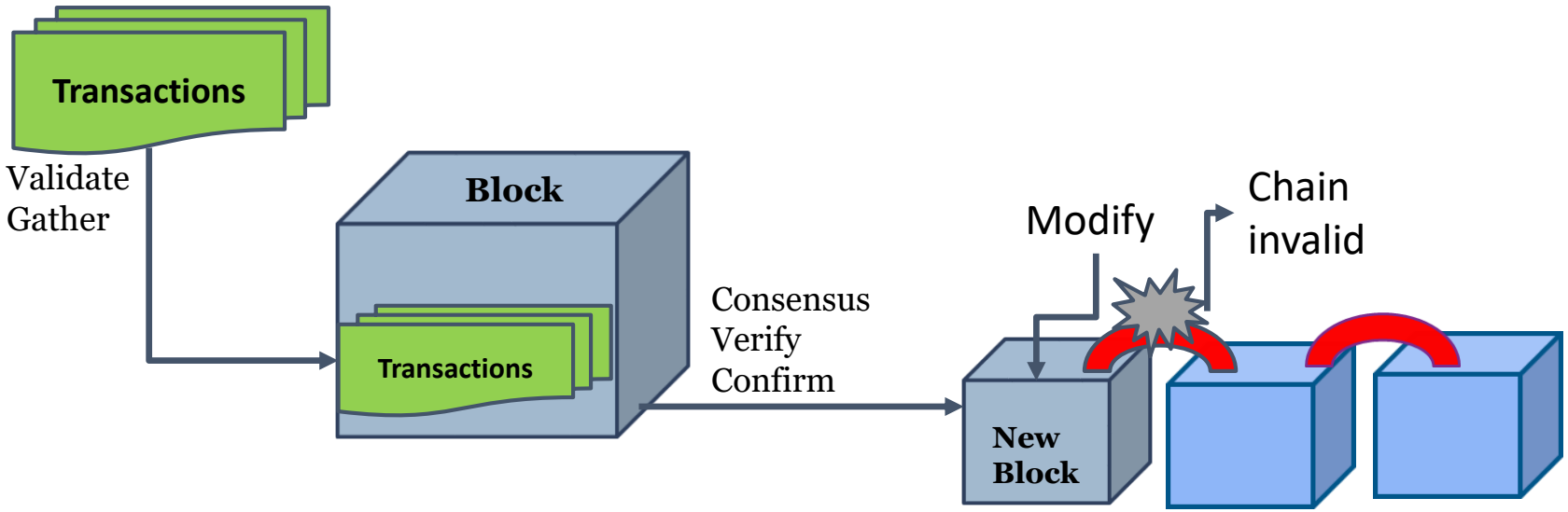
Blockchain





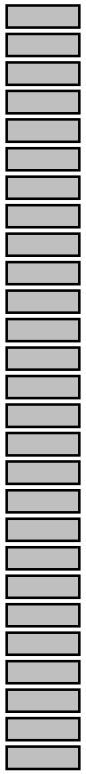
All defined by the blockchain protocol, and implemented.
For example, consider checking in for your flight at the airport.

Blockchain: Distributed, Decentralized, Immutable

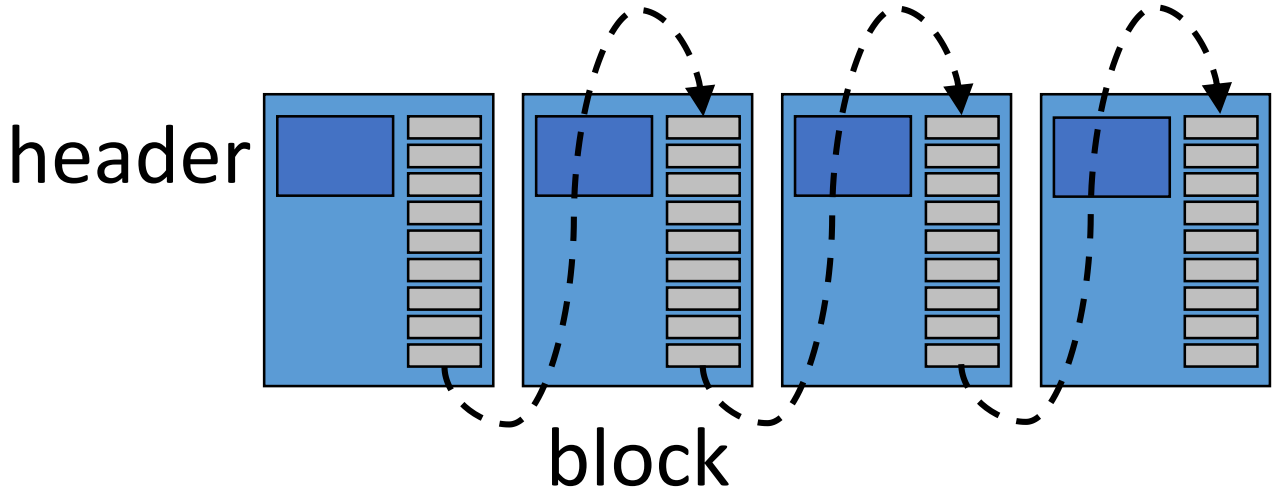


Blockchain

Log



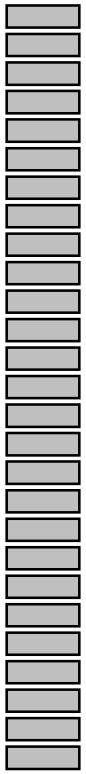
Blockchain



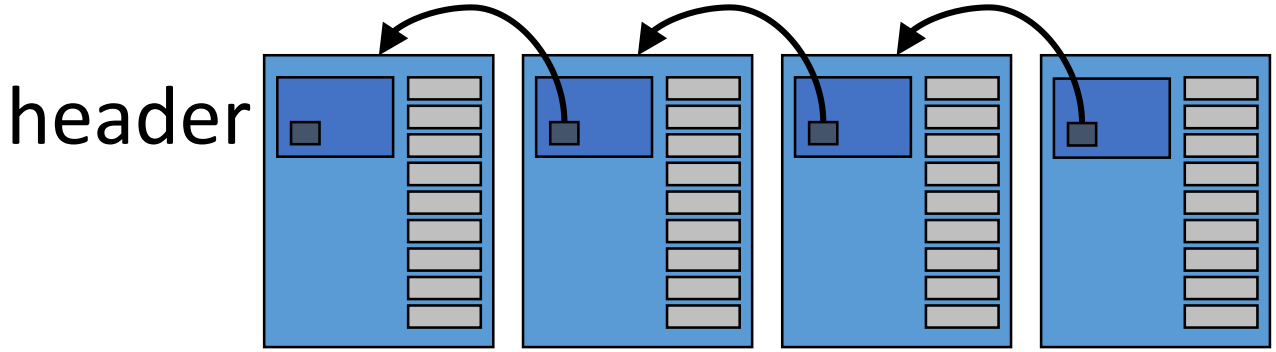
Slide courtesy of Ittay Eyal

Blockchain

Log



Blockchain

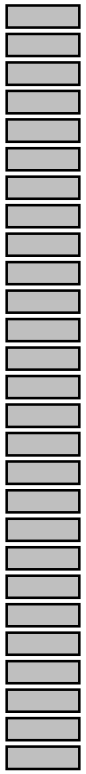


block

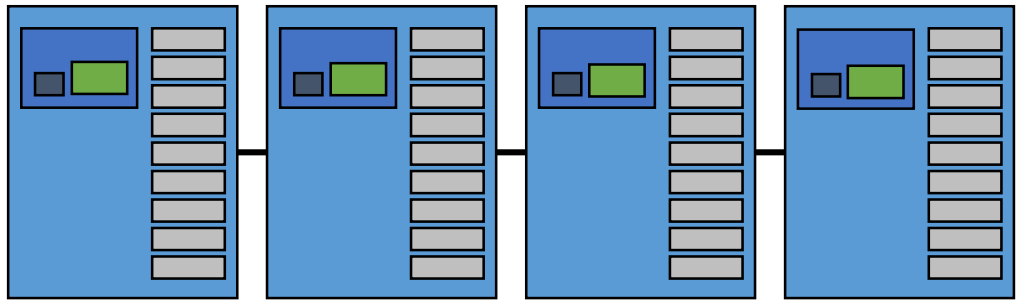
Slide courtesy of Ittay Eyal

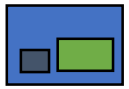
Nakamoto's Blockchain

Log



Blockchain

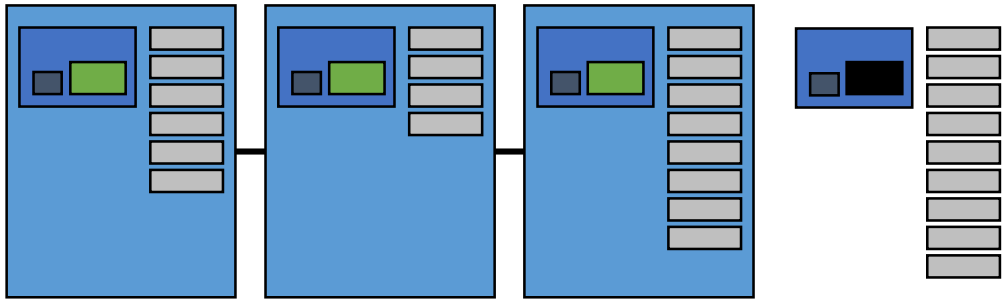


hash() < target*

* *target*: a deterministic function of previous blocks

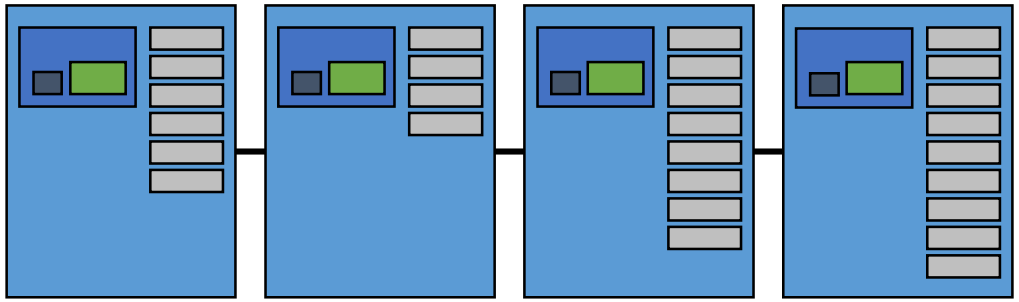
Slide courtesy of Ittay Eyal

Nakamoto’s Blockchain



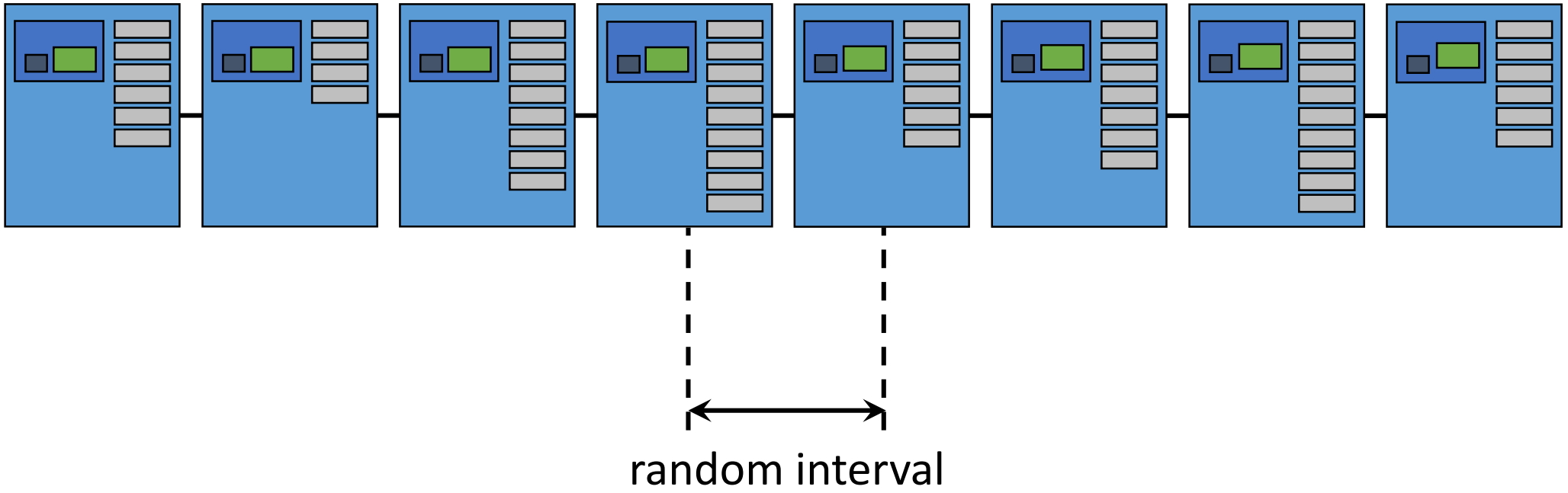
Slide courtesy of Ittay Eyal

Nakamoto’s Blockchain



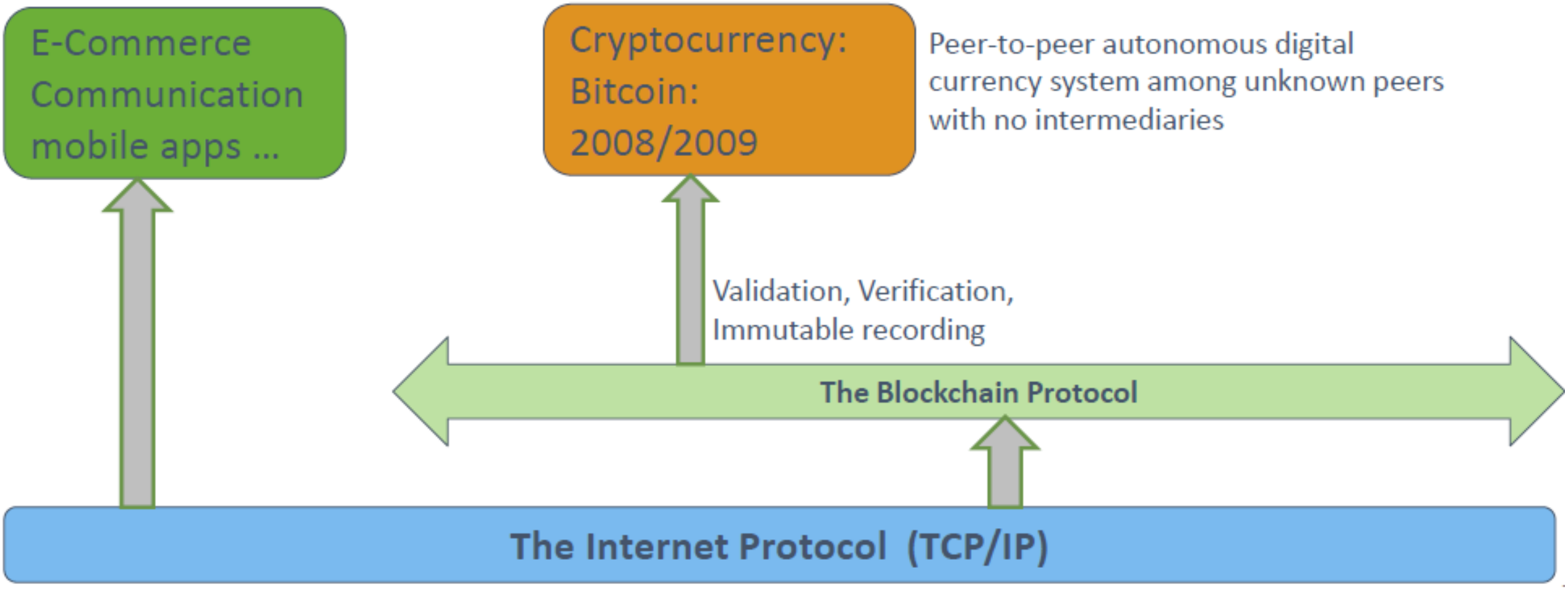
Slide courtesy of Ittay Eyal

Nakamoto’s Blockchain



Slide courtesy of Ittay Eyal

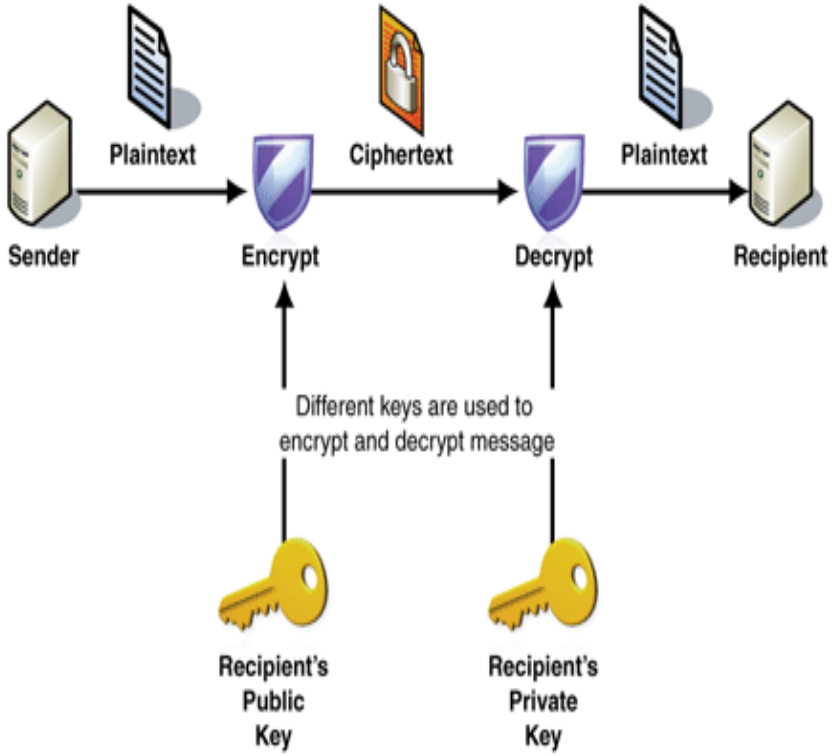
Bitcoin: Cryptocurrency



Blockchain Implementation

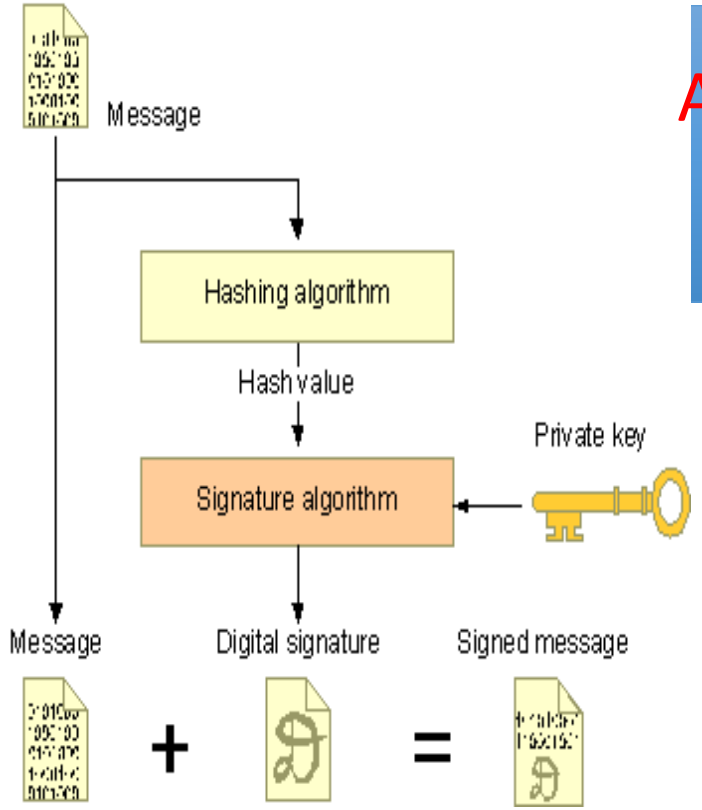
Public Key Crypto: Encryption

- Key pair: public key and private key



Public Key Crypto: Digital Signature

- First, create a message digest using a cryptographic hash
- Then, encrypt the message digest with your private key



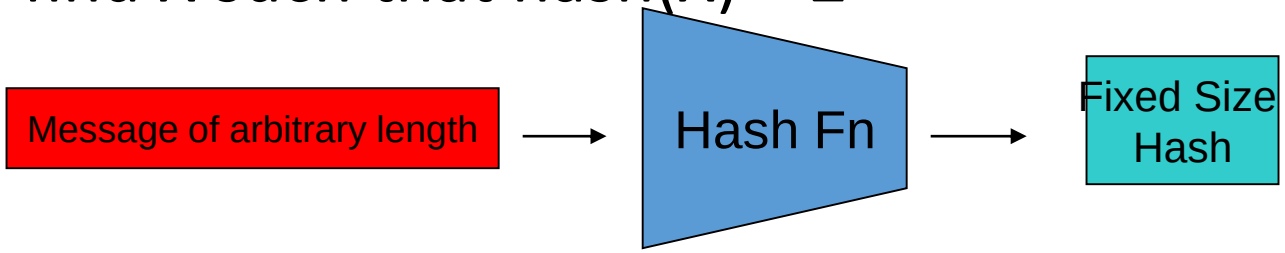
Authentication

Integrity

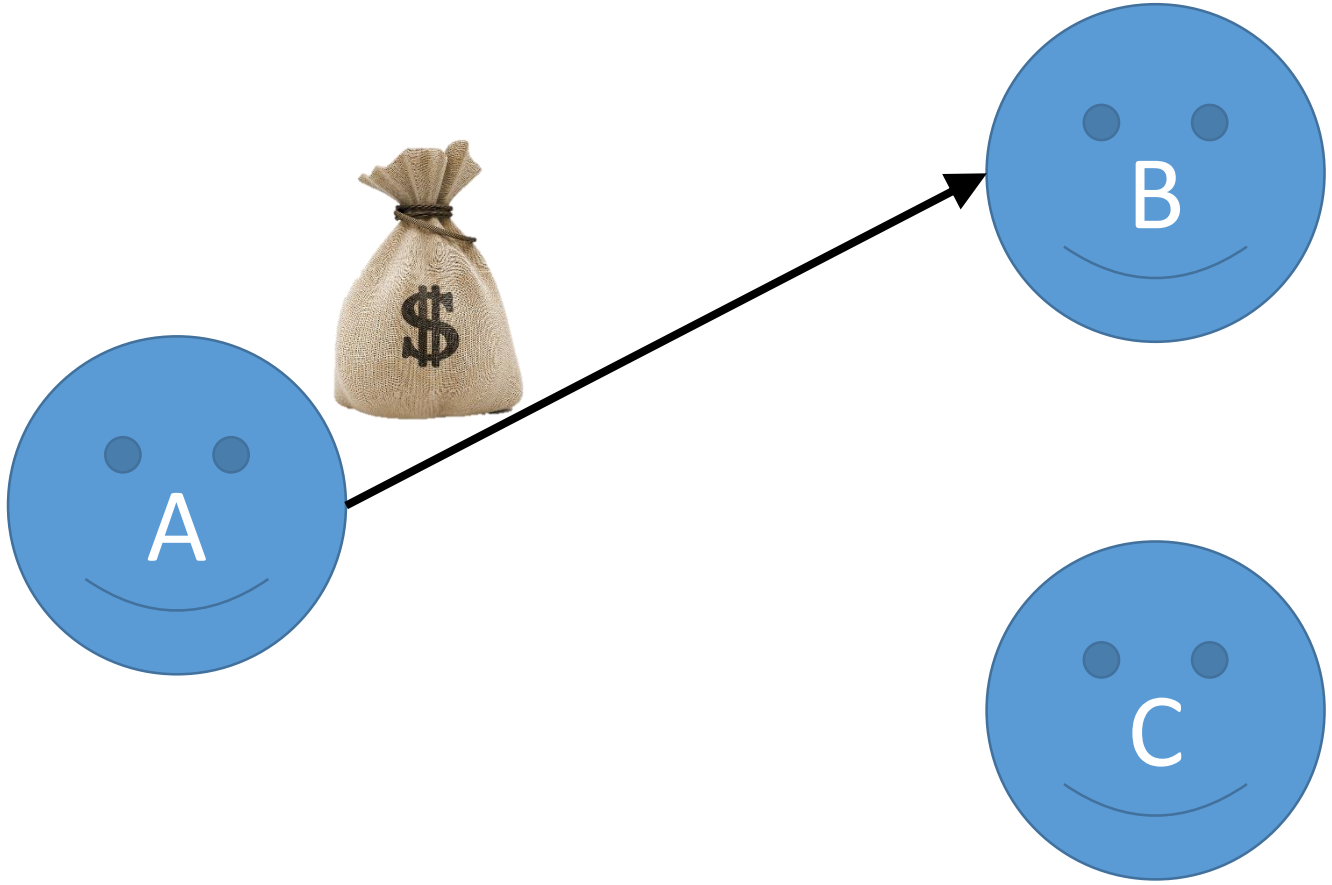
Non-repudiation

Cryptographic Hash Functions

- **Consistent:** hash(X) always yields same result
- **One-way:** given Y, hard to find X s.t. hash(X) = Y
- **Collision resistant:** given hash(W) = Z, hard to find X such that hash(X) = Z



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

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

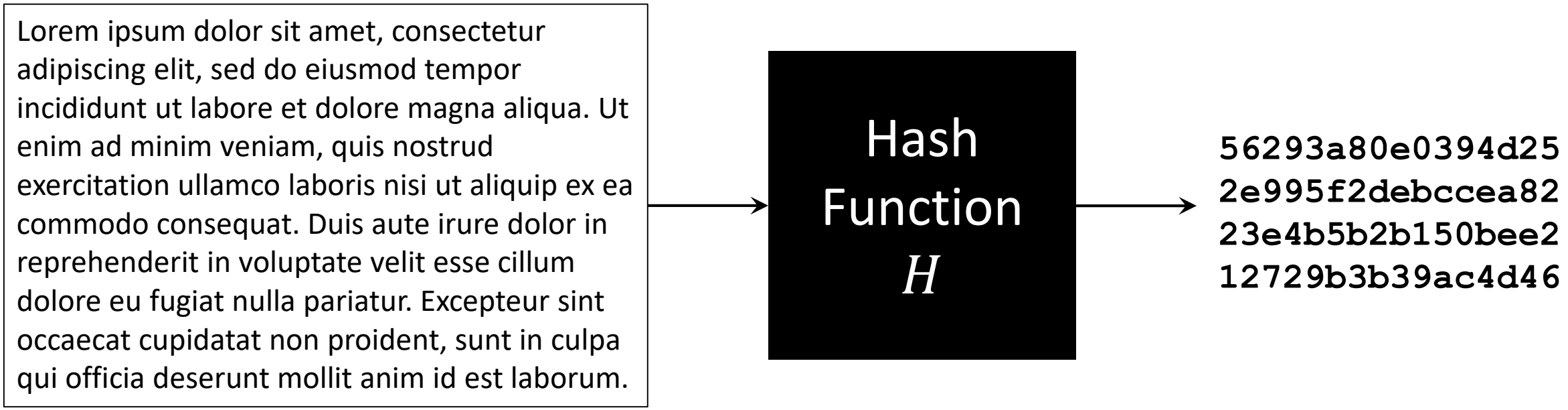
Security in Bitcoin

- Authentication
  - Am I paying the right person? Not some other impersonator?
- Integrity
  - Is the coin double-spent?
  - Can an attacker reverse or change transactions?
- Availability
  - Can I make a transaction anytime I want?
- Confidentiality
  - Are my transactions private? Anonymous?

Security in Bitcoin

- Authentication → Public Key Crypto: Digital Signatures
  - Am I paying the right person? Not some other impersonator?
- Integrity → Digital Signatures and Cryptographic Hash
  - Is the coin double-spent?
  - Can an attacker reverse or change transactions?
- Availability→ Broadcast messages to the P2P network
  - Can I make a transaction anytime I want?
- Confidentiality→ Pseudonymity
  - Are my transactions private? Anonymous?

60 Seconds on Cryptographic Hashing



String input

256 bit number (for example)

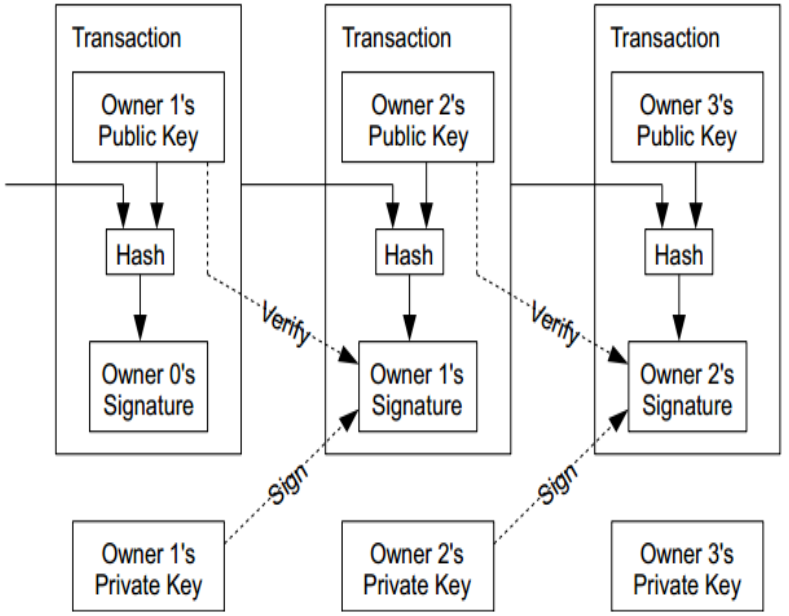
Given a 256bit number h, one cannot find an input string that results in h faster than repeatedly guessing inputs x and calculating $H(x)$.

Slide courtesy of Ittay Eyal

Bitcoin

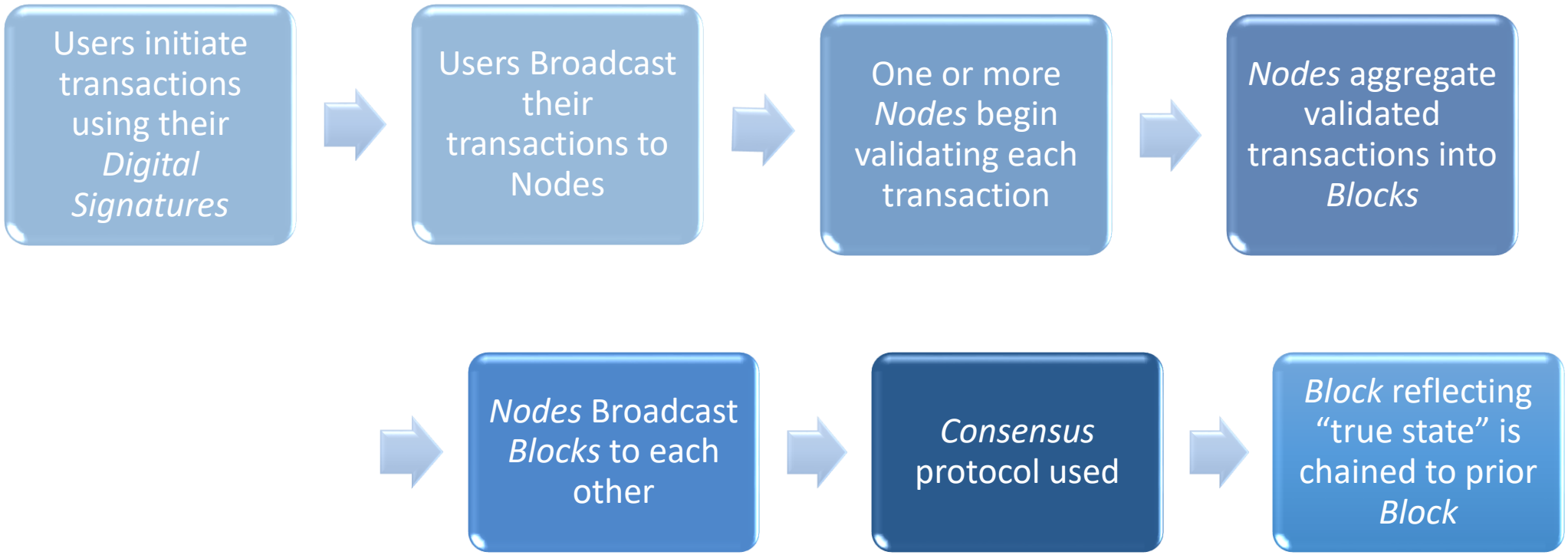
- Electronic coin == chain of digital signatures
- BitCoin transfer: Sign(Previous transaction + New owner's public key)
- Anyone can verify (n-1)th owner transferred this to the nth owner.
- Anyone can follow the history

Given a BitCoin



Blockchain terminologies

- **Distributed ledger – How it works?**

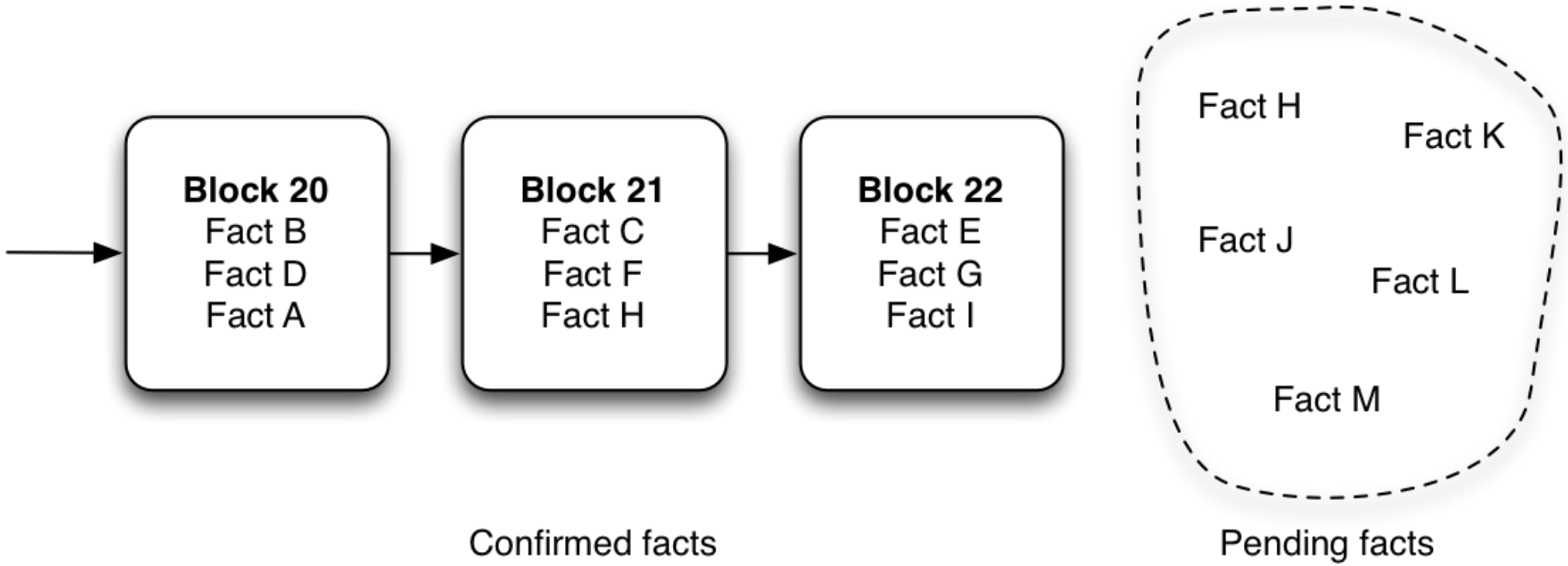


Source:
https://ccl.yale.edu/sites/default/files/files/A%20Brief%20Introduction%20to%20Blockchain%20(Final%20without%20Notes).pdf

Specific issues

Blockchain terminologies

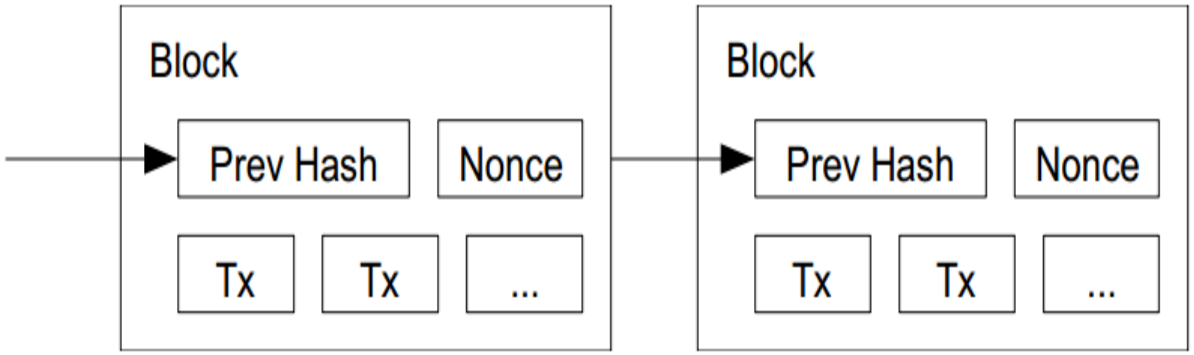
- **Mining**
  - This process of solving cryptographic problems using computing hardware also triggers the release of cryptocurrencies



Source: https://marmelab.com/blog/2016/05/12/blockchain-expliquee-aux-

Use of Cryptographic Hashes

- Proof-of-work
  - Block contains transactions to be validated and previous hash value.
  - Pick a nouce such that **H(prev hash, nounce, Tx) < E**. E is a variable that the system specifies. Basically, this amounts to finding a hash value who's leading bits are zero. The work required is exponential in the number of zero bits required.
  - Verification is easy. But proof-of-work is hard.



BitCoin

- Validation
  - Is the coin legit? (proof-of-work) → Use of Cryptographic Hashes
  - How do you prevent a coin from double-spending? → consensus based verification
- Creation of a virtual coin/note
  - How is it created in the first place? → Provide incentives for miners
  - How do you prevent inflation? (What prevents anyone from creating lots of coins?) → Limit the creation rate of the BitCoins

Preventing Double-spending

- The only way is to be aware of all transactions.
- Each node (miner) verifies that this is the first spending of the Bitcoin by the payer.
- Only when it is verified it generates the proof-of-work and attach it to the current chain.

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

Slide courtesy of Ittay Eyal

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

Who runs the public key infrastructure?

Who maintains the public ledger?

Who gives money for puzzles?

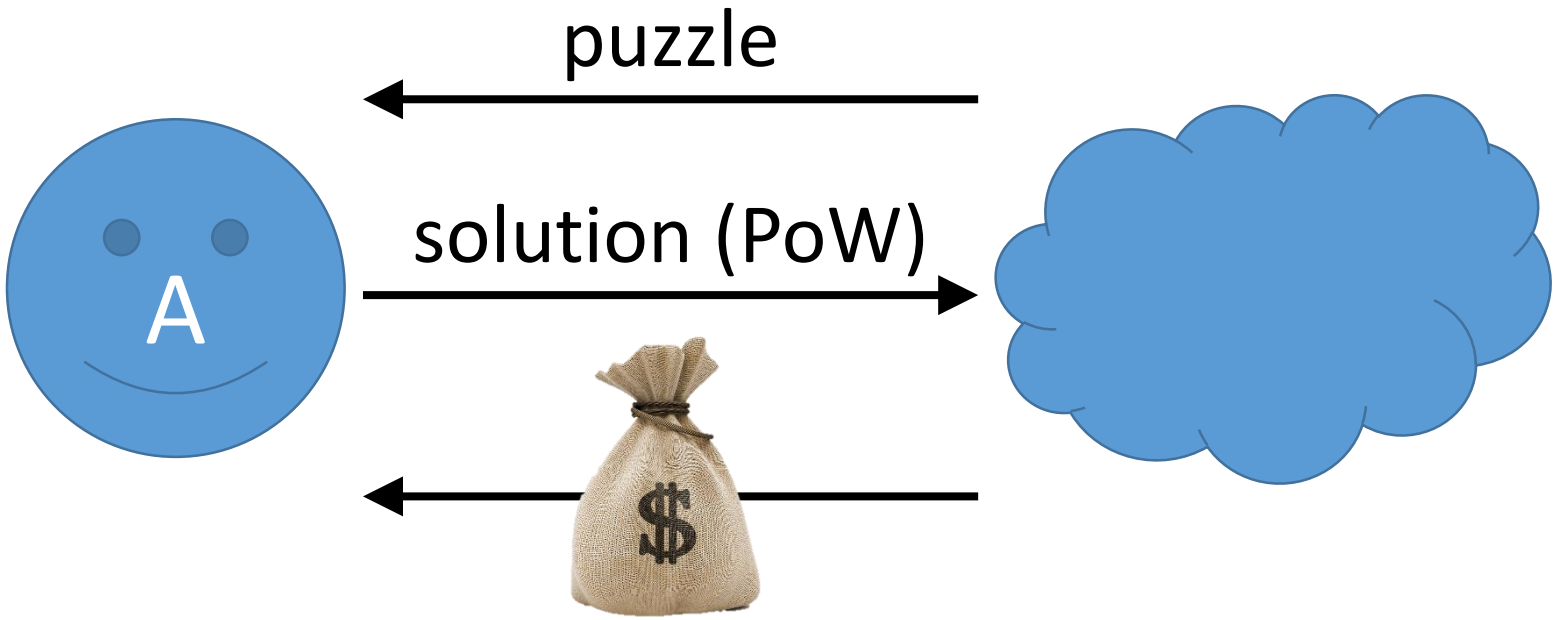
Can this be decentralized?

Slide courtesy of Ittay Eyal

BitCoin Economics

- Rate limiting on the creation of a new block
  - Adapt to the “network’s capacity”
  - A block created every 10 mins (six blocks every hour)
    - How? Difficulty is adjusted every two weeks to keep the rate fixed as capacity/computing power increases
- N new Bitcoins per each new block: credited to the miner → incentives for miners
  - N was 50 initially. In 2013, N=25.
  - Halved every 210,000 blocks (every four years)
  - Thus, the total number of BitCoins will not exceed 21 million. (After this miner takes a fee)

Mining – Minting for Proof of Work



Mining – Minting for Proof of Work

Computationally difficult puzzle:

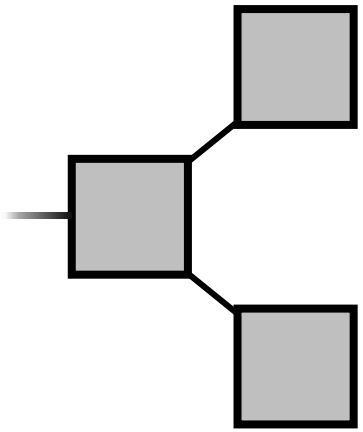
$$\text{Find } x \text{ such that } H(x|y) < t$$

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

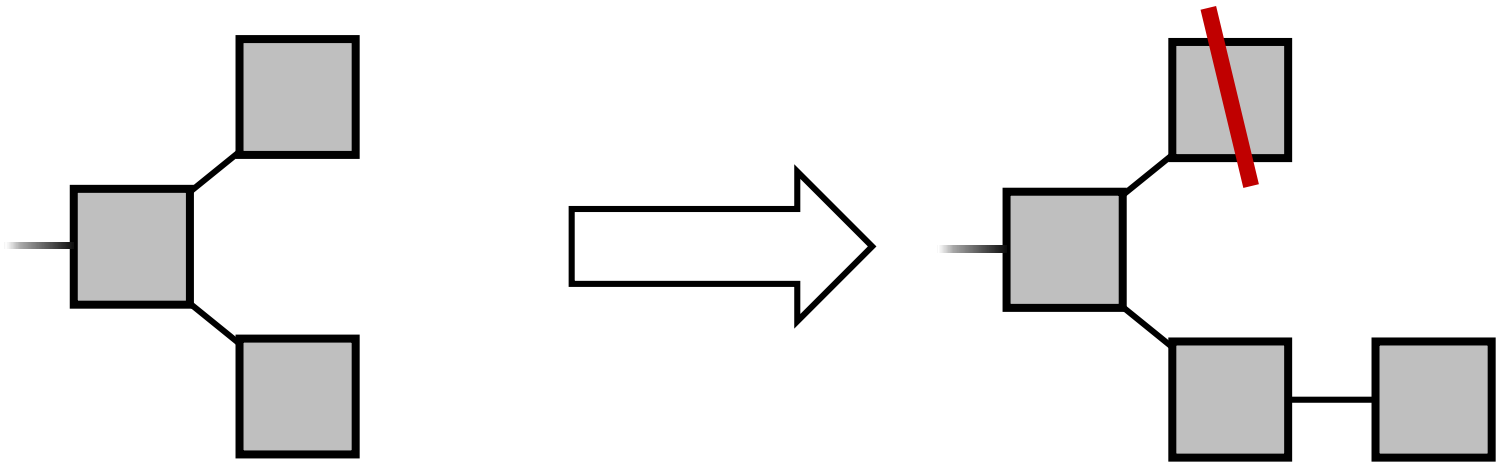
Slide courtesy of Ittay Eyal

Forks



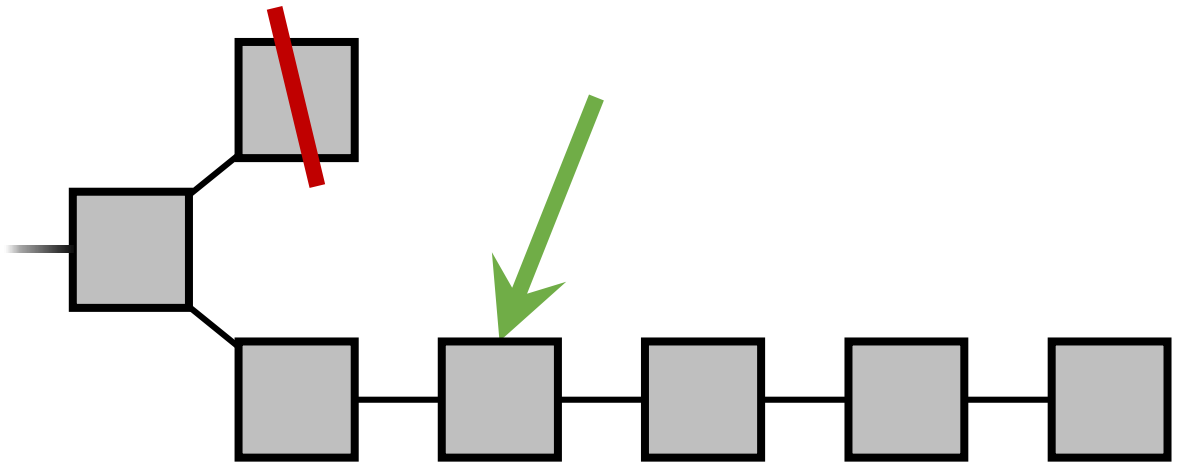
- Natural in a distributed system

Fork Resolution



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

Fork Resolution



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