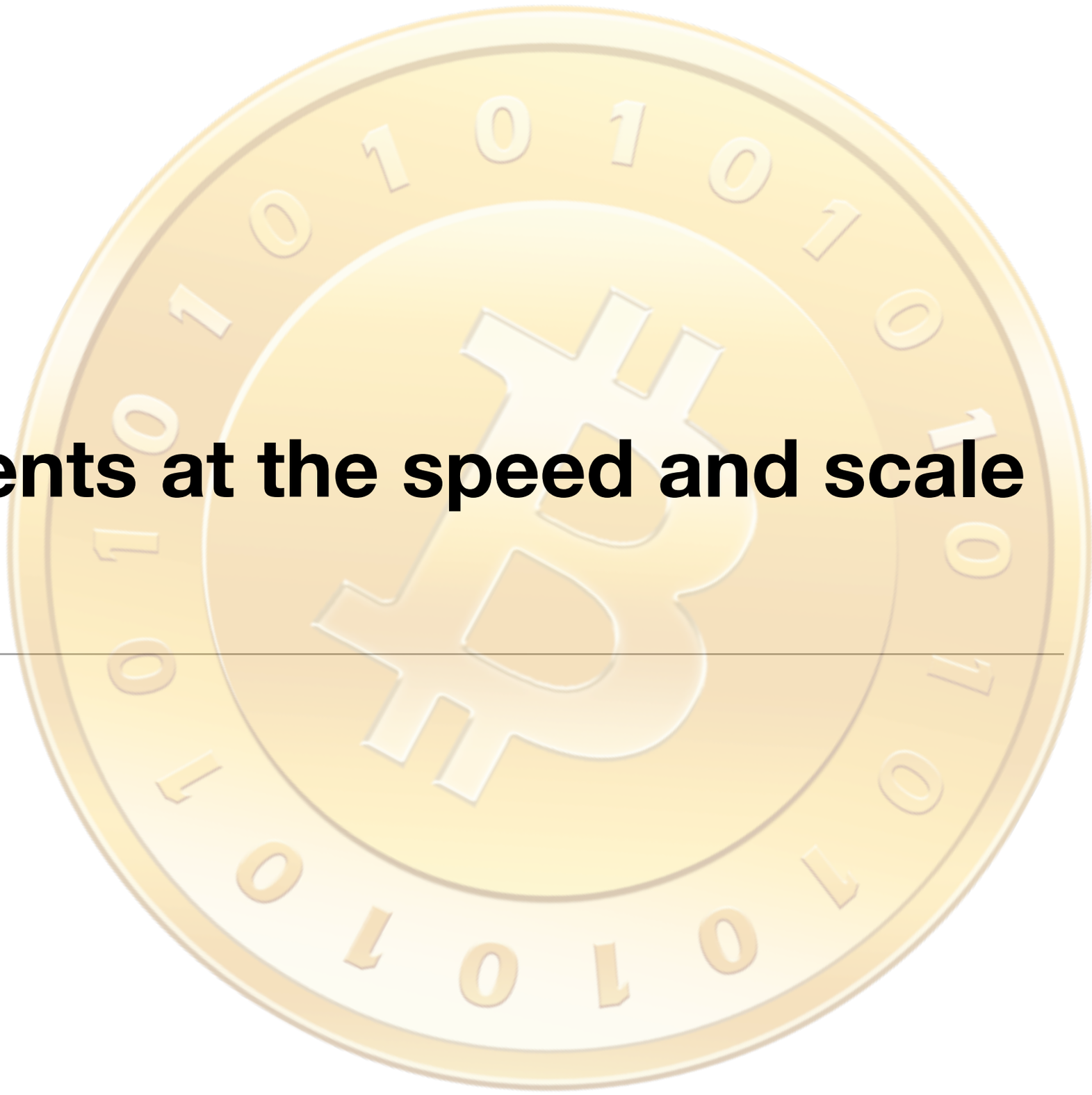
Bitcoin: payments at the speed and scale of the Internet

Tom Van Cutsem



Vrije
Universiteit
Brussel

What is Bitcoin?

- Digital “money”
- A virtual currency
- Technically, a **cryptocurrency**

How much is a BTC worth?

"Bitcoin rose 722% in the first six months of 2013"
(source: The Genesis Block, 2013 Mid-year review)

Talk outline

- Why Bitcoin? What makes it unique?
- How are Bitcoins created?
- Under the Hood
- Bitcoin in practice

Why Bitcoin? What makes it unique?

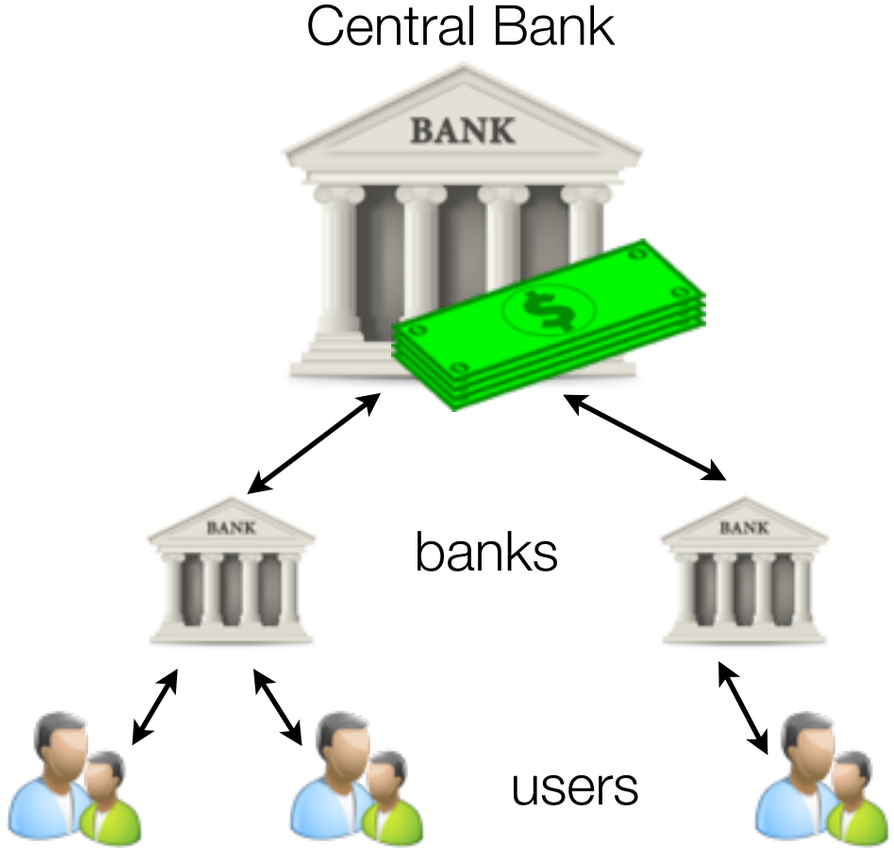
Virtual currencies are not new

- Cryptographic “e-cash” systems since the ‘80s
- Facebook Credits
- Linden Dollars (Second Life)
- …

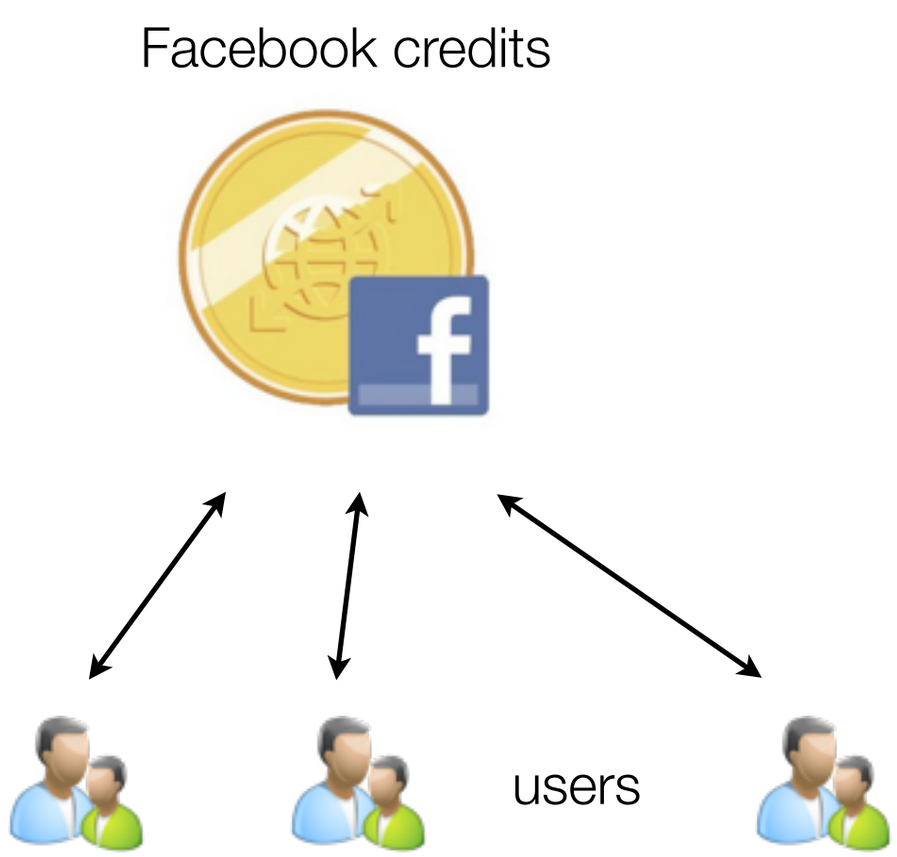
Fiat money and most virtual currencies are centralized

- Central point of trust
- Central “clearing house”: technically easy to verify double spending

Central Bank

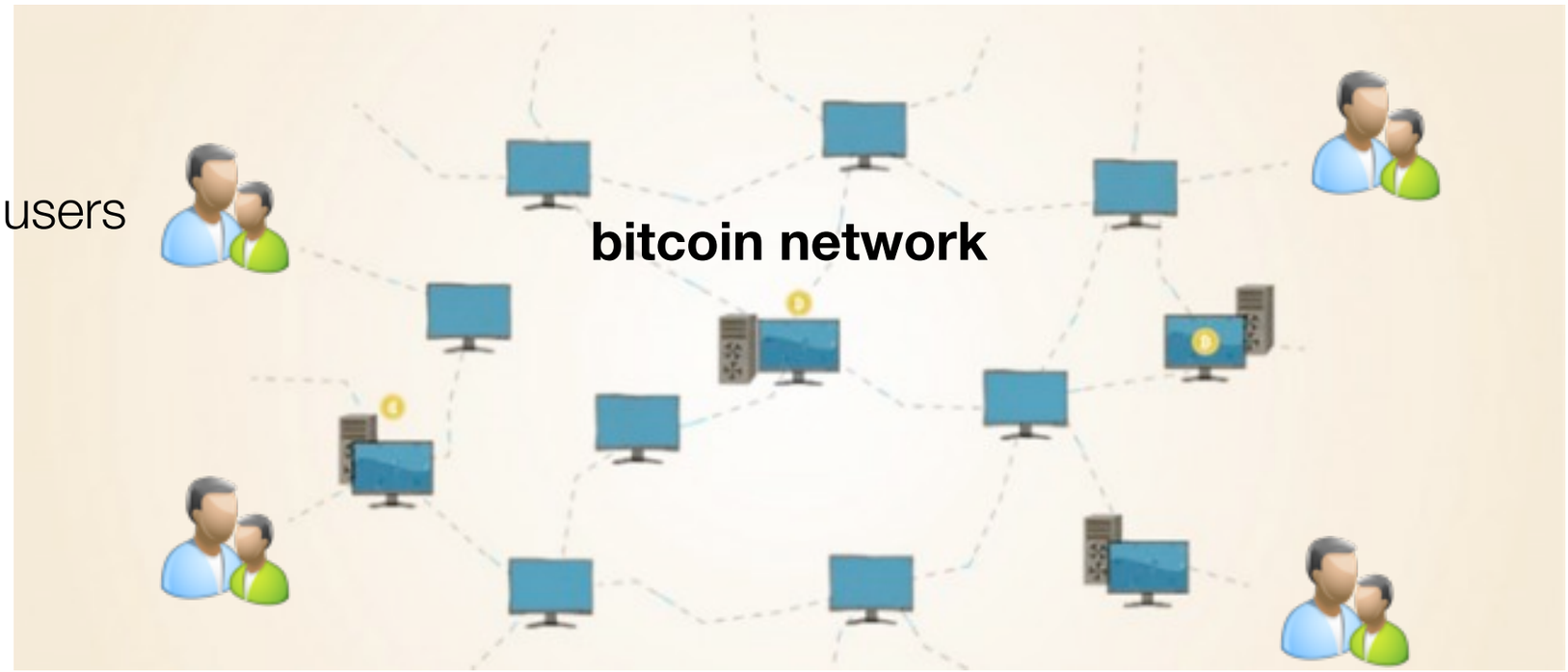


Facebook credits



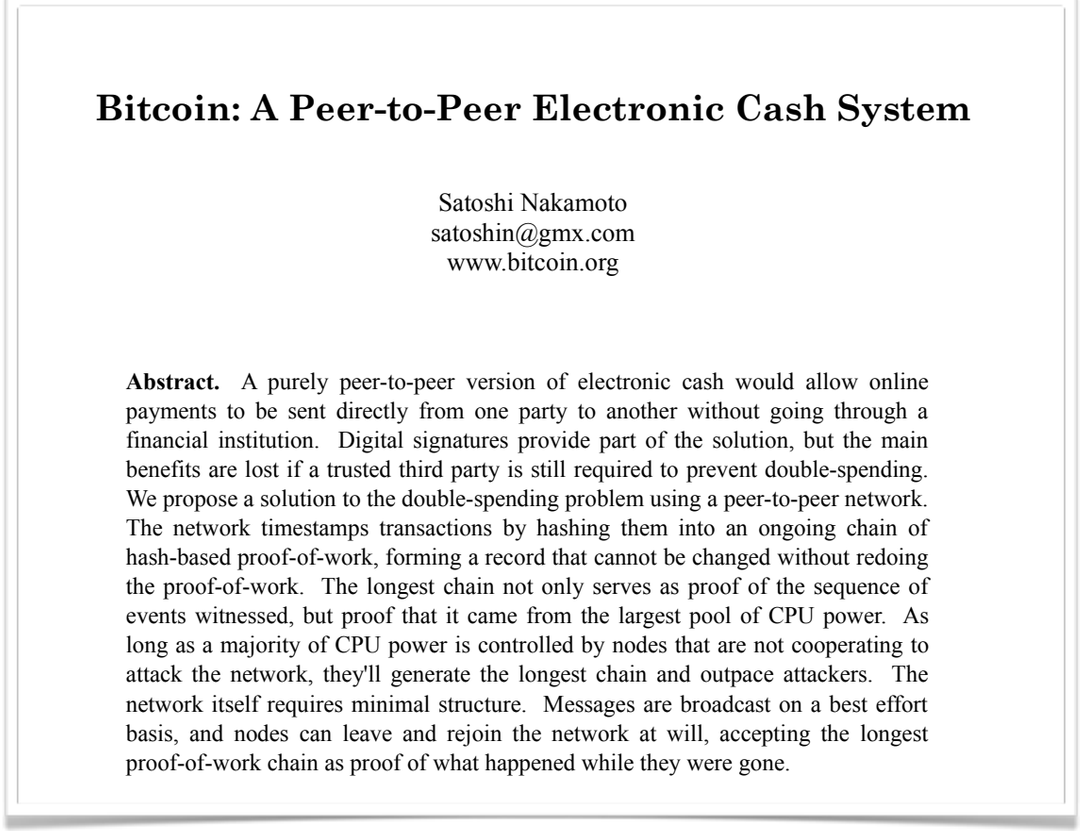
Bitcoin is decentralized

- Not issued or controlled by any single company or institution
- “Peer-to-peer” network
- All transactions are recorded in a single, distributed **public ledger**
- The network verifies transactions collectively.



Who is behind Bitcoin?

- 2008 white paper by “Satoshi Nakamoto”
- Today, Bitcoin codebase maintained as an open source project on GitHub



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

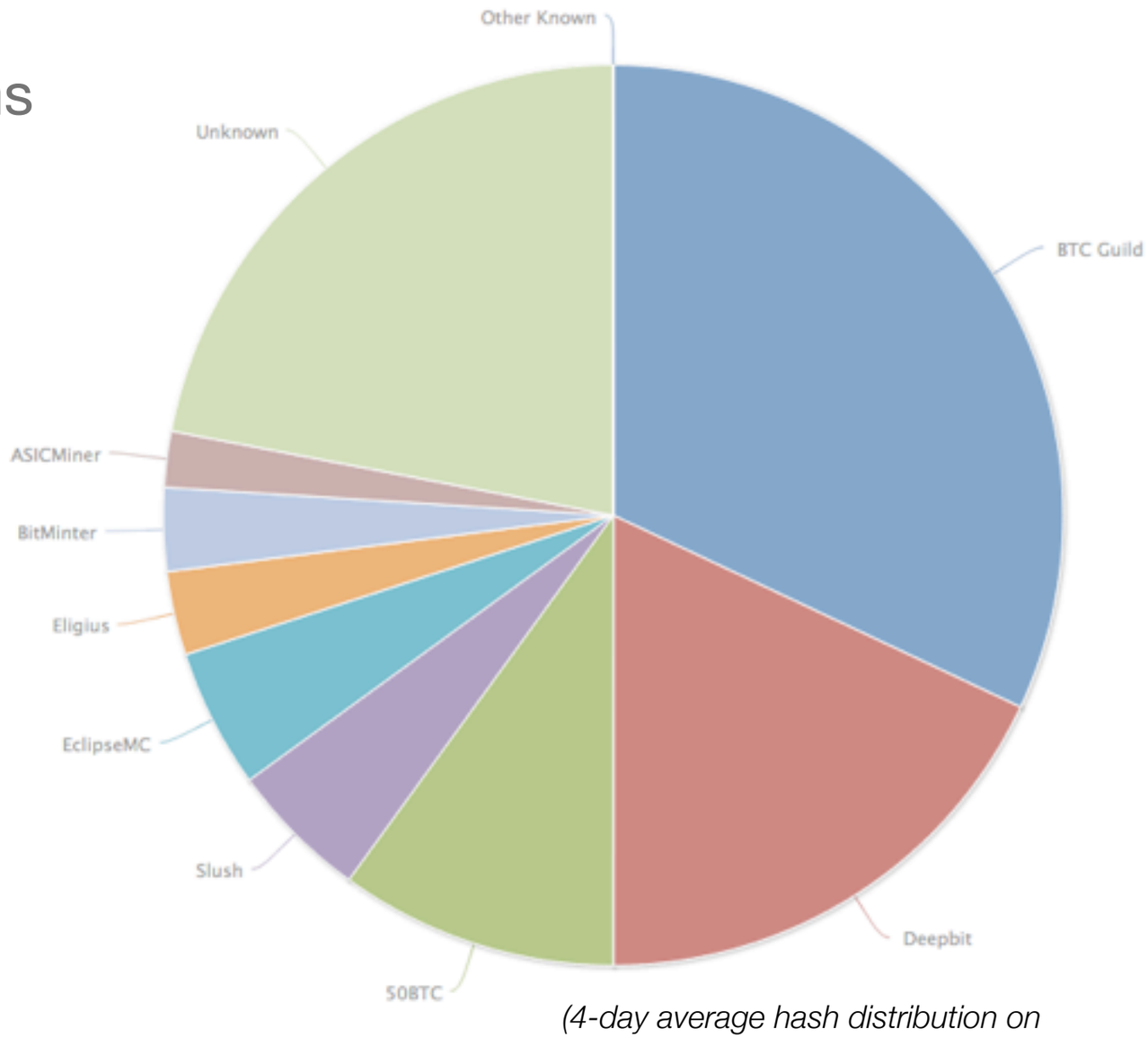
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required 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.

BTC Strengths

- **No central point of trust**, no central authority
- **No borders**: works the same across the planet
- Transactions are typically carried out within **minutes** (compare to banking transactions taking days)
- Transaction **fees are low** to non-existent. This makes BTC suitable for **micro-transactions**.
- Transactions are **irreversible**
- **Limited supply**: controlled inflation

BTC Weaknesses

- Technical Risks:
  - **Relies on crypto**graphic algorithms not being broken
  - If a **single party controls > 50%** of compute power in the network, it can rewrite transaction history



(4-day average hash distribution on 26-09-2013, source: blockchain.info)

BTC Weaknesses

- Non-technical Risks:
  - Not sure **who invented it**. Have to place trust in the network.
  - **End-user** is **responsible for safe-keeping** of his/her coins
    - blockchain.info slogan: “be your own bank”
      - Reliance on online wallets reintroduces third-party risk
  - **Lack of** a **legal framework** (taxation, ...)
  - Governments cannot manipulate the currency, but can **coerce companies** that serve as entry-point into the Bitcoin economy

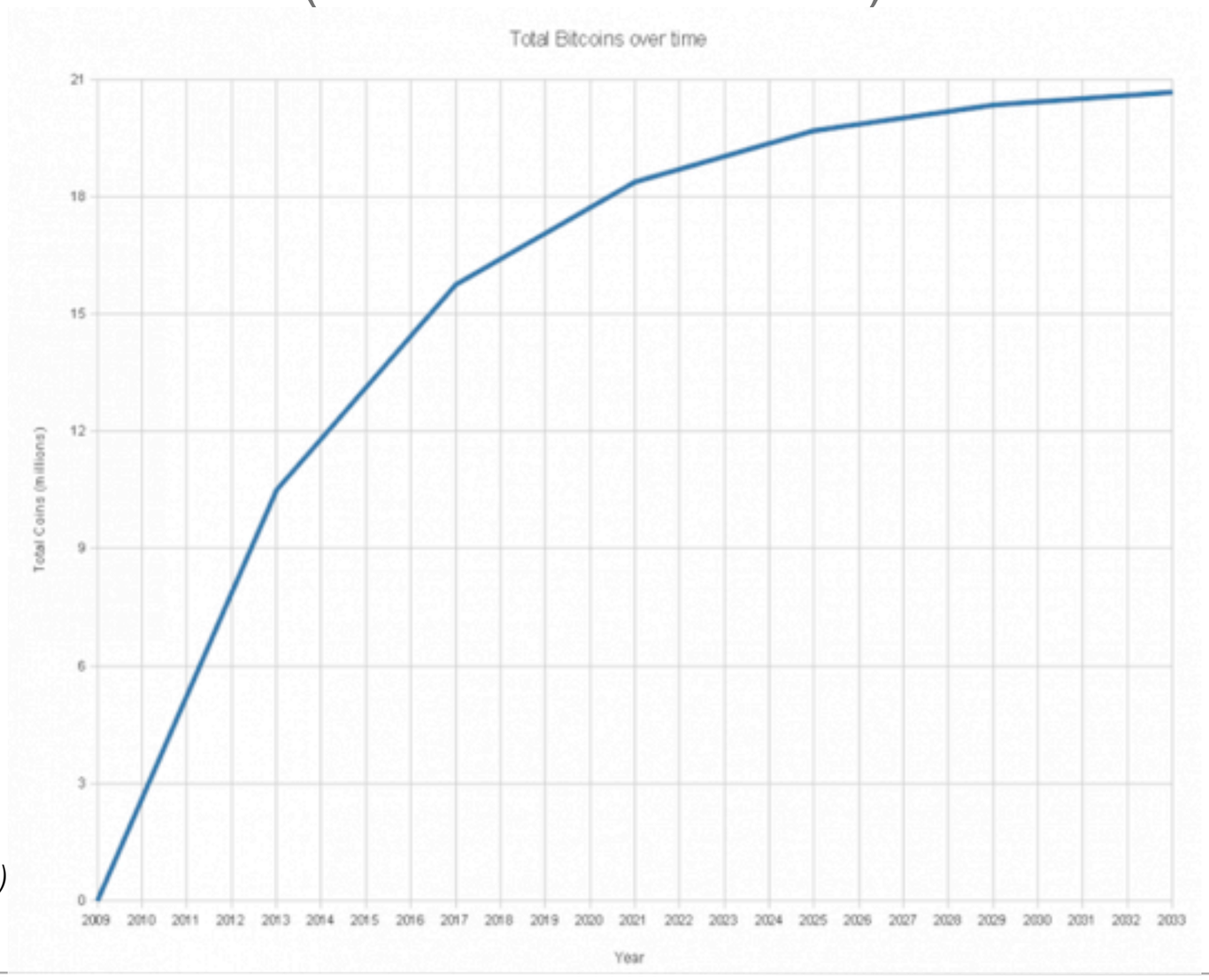
How are Bitcoins created?

Bitcoin mining

- Computers that aid in processing transactions get a “reward”
- **Incentive** to become part of the network and help transaction processing
- Analogy with mining gold.
- New bitcoins born by solving a cryptographic puzzle

Bitcoin mining: controlled inflation

- The mining “reward” is halved every 4 years
- Asymptotic limit of 21 Million bitcoins (to be hit around 2140)
- 11.7 Million mined so far



(source: Wikipedia)

Mining Rigs

Under The Hood

Bitcoin wallet

- To create a bitcoin wallet, generate a new public/private key pair
- Access to public key allows you to query the account balance
- Access to private key allows you to spend
- Example Bitcoin address:

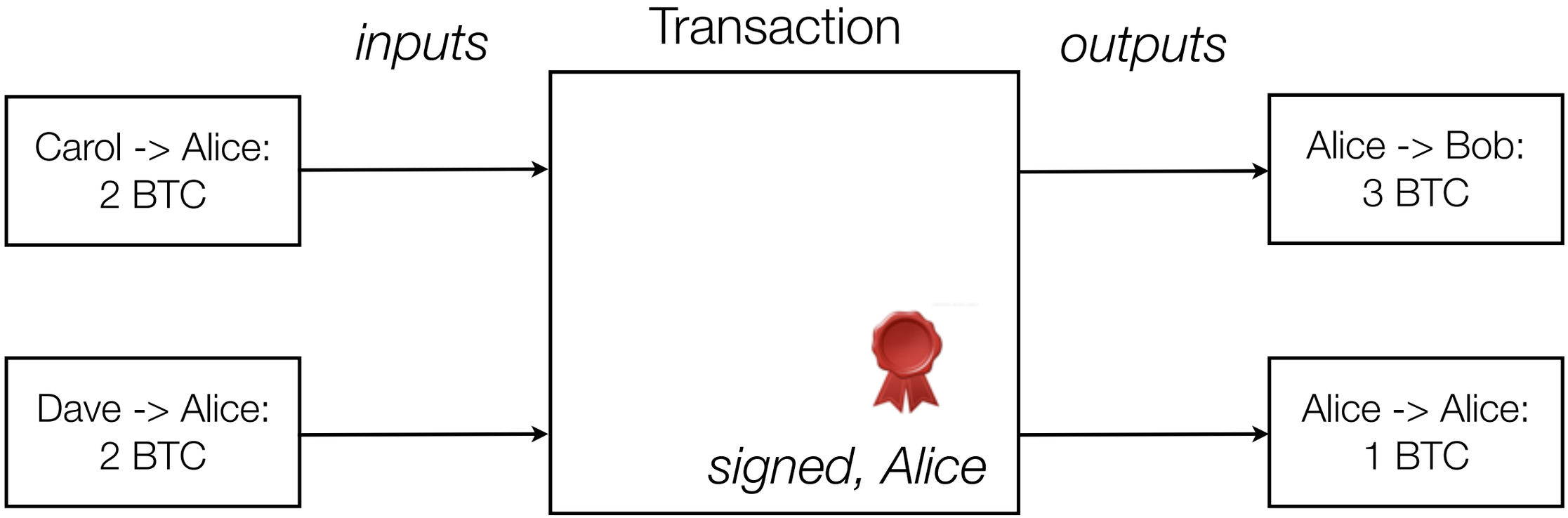
31uEbMgunupShBVTewXjtqbBv5MndwfXhb

Where are Bitcoins stored?

- The wallet is just a pair of keys (large numbers)
- Bitcoins are *not* stored physically on your computer.
- Your coins “reside” implicitly in prior transactions that designate your public key as a beneficiary

Example

- Alice wants to pay Bob 3 BTC
- She “owns” 4 BTC by proving that she previously received 2 BTC from Carol and 2 BTC from Dave

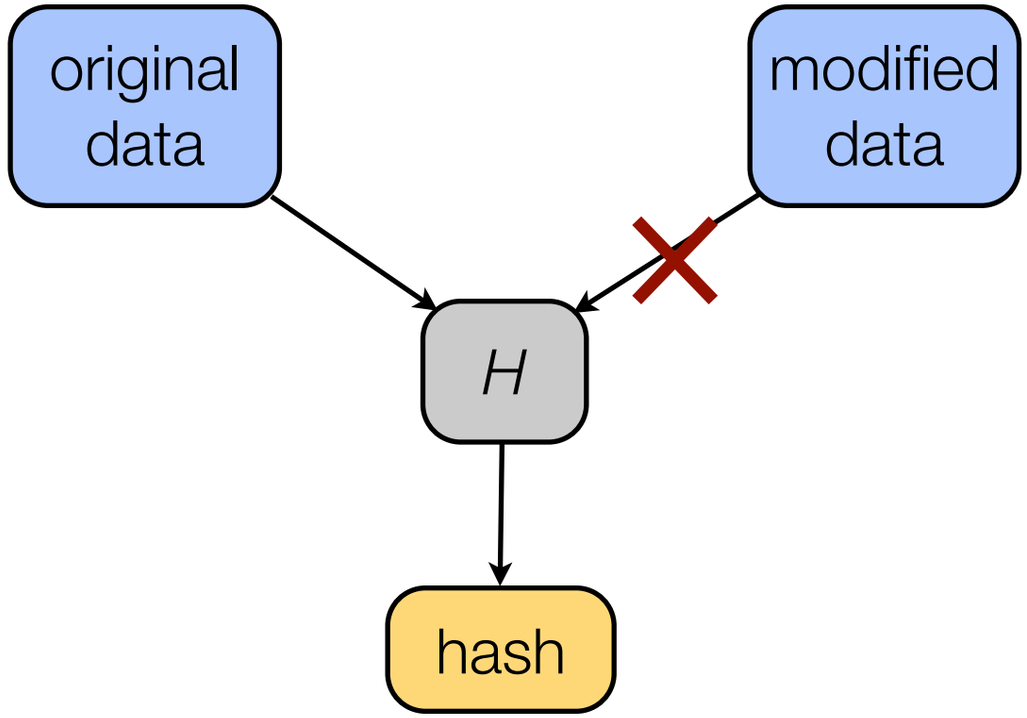


The double spending problem

- How does Bob know the received coin has not been spent before?
- Did the previous owner not sign any earlier transactions with the coin?
- Solution: make all transactions **public**
  - So everyone can verify what transactions happened first and detect double spending
  - But, all participants must **agree on a single history** of the order in which transactions were made
  - This is a **technically hard** problem in distributed systems (known as **consensus**)

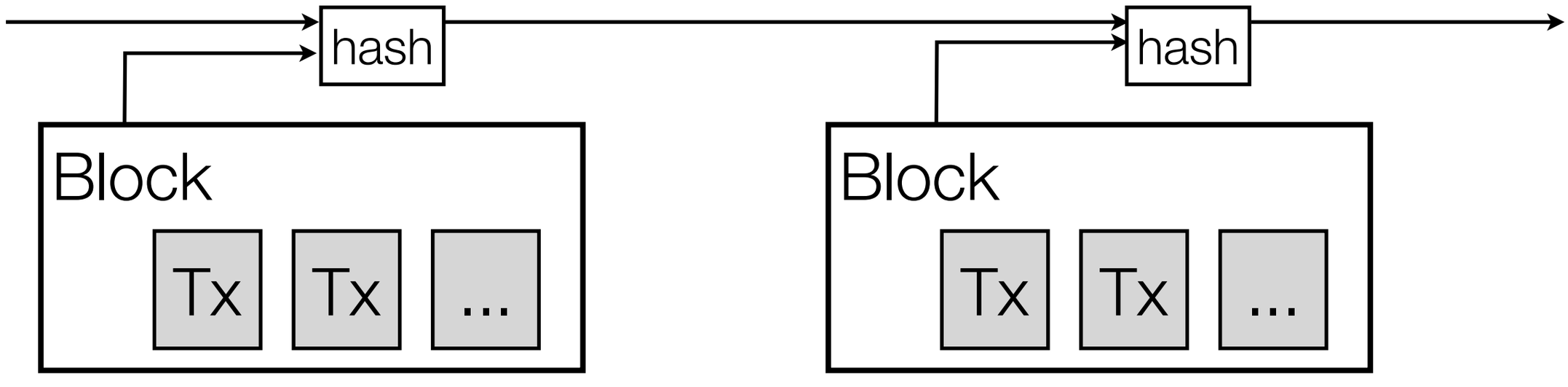
Cryptographic hashing 101

- Hashing protects against tampering with Bitcoin transaction data
- Given output hash, impossible to construct modified input data that hashes to the same output



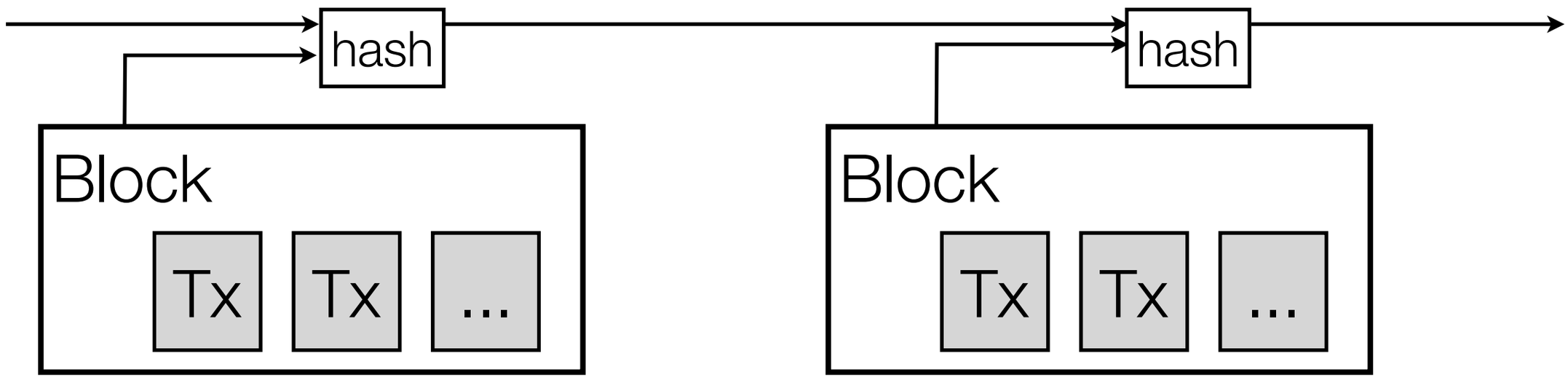
Hashing and Bitcoin

- Node in the Bitcoin network *hashes* a block of transactions to be timestamped and widely publishes the hash
- The timestamp proves that the data must have existed at the time, in order to get into the hash
- Each timestamp includes the previous hash in its hash, forming a chain
- This is called the **blockchain**



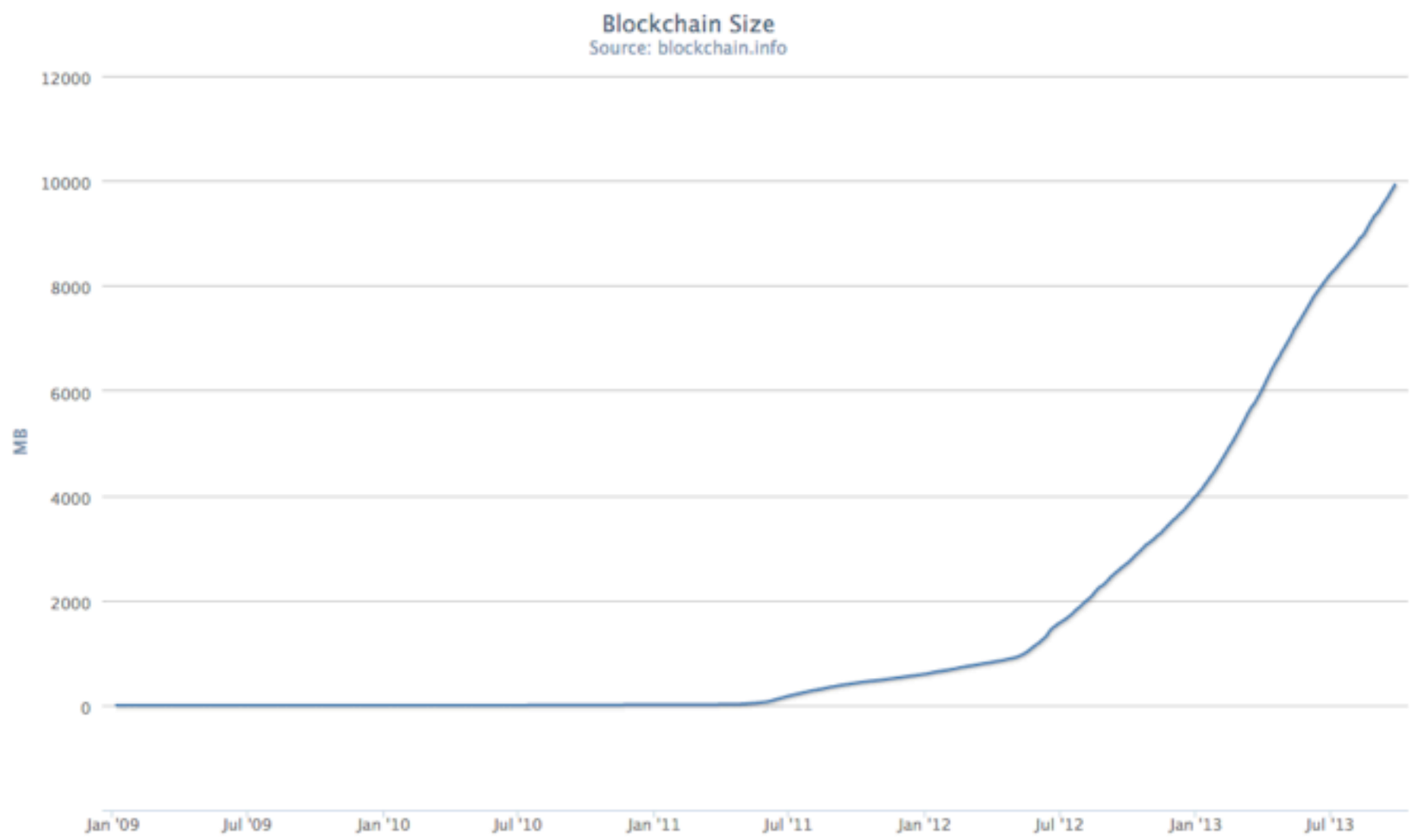
The Blockchain

- The blockchain is Bitcoin's **transaction ledger**, publicly recording *all* transactions
- Benefit of chaining: changing a single block would require changing all blocks after it as well



The real blockchain

- First block known as the “Genesis block” (Jan 3rd, 2009)
- The current longest blockchain: 10 GigaByte of transaction data



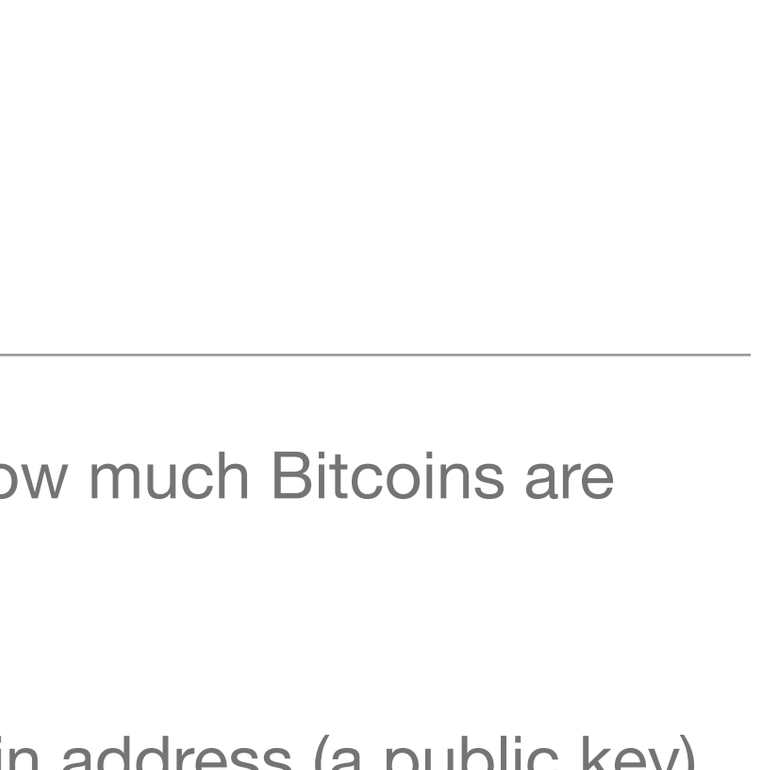
Privacy

- **Transactions are** entirely **public**: anyone can see how much Bitcoins are transferred between any 2 addresses

- But: there is no a priori relationship between a Bitcoin address (a public key) and a user's "identity"

- Keeping your public key anonymous keeps the transactions anonymous

- In practice, not that easy to remain truly anonymous



(source: silicon angle)

Bitcoin in practice

What can you buy with it?

- Initially used for anonymously buying questionable / illegal goods
- More and more merchants are accepting BTC
  - Attractive for online micro-payments

- For a list of merchants, see https://www.spendbitcoins.com/ and https://en.bitcoin.it/wiki/Trade

Exchanges

- Market places where BTC is bought/sold for EUR, USD, ...
- Typical “entry point” into the Bitcoin market
- Examples:

Merchant Processors

- Aim to make it easy for merchants to accept BTC
- Merchant processor accepts BTC and transfers USD/EUR to the merchant
- The merchant never has to deal with BTC
- Examples:

Software Wallets

- Download a piece of software known as a “bitcoin client”
- “Fat” clients: your computer becomes part of the Bitcoin network, requires downloading the blockchain.
  - Example: 

    Bitcoin-Qt
- “Thin” clients: only stores your wallet (public/private keys) and allows you to send/receive BTC. Does not download the blockchain.
  - Example: 

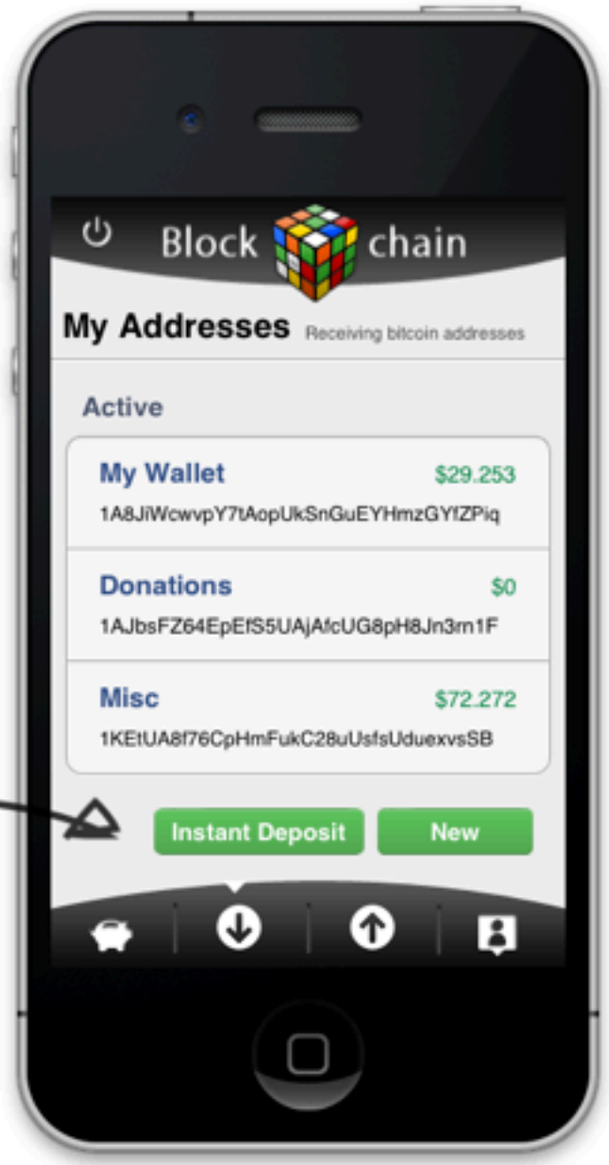
    Electrum

Online web-based Wallets

- Store your wallet for you
- Convenient but introduces third-party risk!
- Examples: blockchain.info
  - Wallet stored encrypted on server
  - Decrypts using JavaScript on the client

Click an address to show a QR Code

Instant Deposit. Right From your phone



Paper Wallets

- Offline wallet. To put your bitcoins in a physical safe.

- Basically a public and private key printed as a QR-code

(source: bitcointalk.org)

Concluding remarks

A word of warning

- Bitcoin is a young technology
- Highly volatile price
- High risk
- Storing money in online wallet: security issues

A glimpse at Money of the 21st Century?

- Bitcoin is money at the speed and scale of the Internet
- Rapidly growing list of financial services:
  - Currency exchanges
  - Offer or make loans in Bitcoin
  - Buy stock in Bitcoin
  - ...