
Bitcoin:
The Who, What, How, and What of a Decentralized Digital Currency

Update:

https://www.youtube.com/watch?v=siUQrEfyh1s

…and don’t forget to grab some pizza!

Game Plan

- A Little About The Presenter

Game Plan

- A Little About The Presenter
- Past (Who?)
  - 10,000 ft, layman's view of banking
  - Satoshi Nakamoto (anonymous creator)

Game Plan

- A Little About The Presenter
- Past (Who?)
- Why Bitcoin?
  - A digital, trustless, (safe?) store of value
  - Payments as bytes
  - Privacy (pseudo-anonymous transactions)
  - A new source of technological innovation

Game Plan

- A Little About The Presenter
- Past (Who?)
- Why Bitcoin?
- What is Bitcoin?
  - Cryptographic one-way hash functions
  - Elliptic curve digital signatures
  - The blockchain

Game Plan

- A Little About The Presenter
- Past (Who?)
- Why Bitcoin?
- What is Bitcoin?
- How does Bitcoin Work?
  - Mining
  - Wallets

And if you haven't left by then…

And if you haven't left by then…

- Multisignature Wallets
- Lightning Network
- Altcoins
- Ethereum
- 21 computer
- Prediction Markets
- Silk Road + OpenBazaar
- Bitcoin Development

Warning to the Wise

- Bitcoin is still a wildly new technology (v0.12)

Warning to the Wise

- Bitcoin is still a wildly new technology (v0.12)
- We are all still early adopters, don't be stupid!

Warning to the Wise

- Bitcoin is still a wildly new technology (v0.12)
- We are all still early adopters, don't be stupid!

- It's used for wholesome things such as:
  - Illegal gambling
  - Black market trades
  - Funding terrorists
  - Sex trade
  - Online Extortion

Warning to the Wise

- Bitcoin is still a wildly new technology (v0.12)
- We are all still early adopters, don't be stupid!

- It's used for wholesome things such as:
  - Illegal gambling
  - Black market trades
  - Funding terrorists
  - Sex trade
  - Online Extortion
- …(psssst! So is cash!)

Thanks!

Balaji Srinivasan

Jameson Lopp

Donn Lee

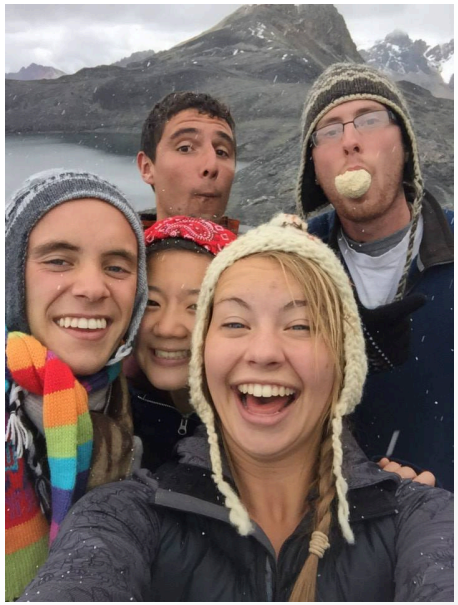
A favor, please

A Little About the Presenter

Alex Melville

Computer Science ‘15

BitGo Software Developer



My Bitcoin Journey

- Discrete Math and RSA crypto

My Bitcoin Journey

- Bitcoin projects with Josh Jones

My Bitcoin Journey

- Software Engineer at BitGo

The Who

History of banking from 10,000 ft.

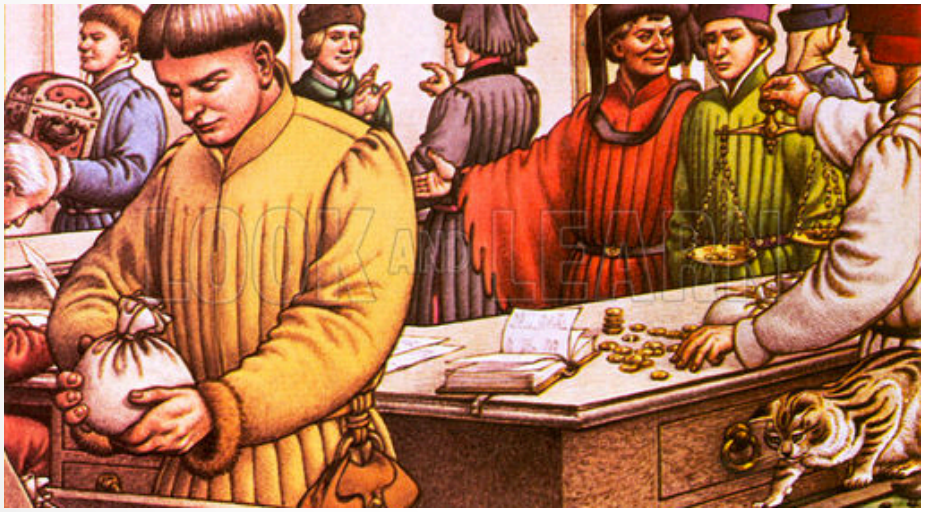
No banks!

History of banking from 10,000 ft.

No banks!

History of banking from 10,000 ft.

Early banks arise



Medici

History of banking from 10,000 ft.

Modern banking

- Images of bank of america and citi

The “T” Word

Trust

Trust

Why was Bitcoin invented?

To understand the progression of ideas, begin with physical cash.

1 PHYSICAL CASH

A hands **B** physical cash.

Implicit property: **A** no longer has the bill, and **B** knows **A** has transferred it.

Trust

Many tried to create a "digital cash"

But naively transplanting cash to the digital world doesn't work.

2 NAIVE DIGITAL CASH

A emails **B** the serial numbers on a bill.

But **A** still has those serial numbers — and temptation to “double spend”.

Trust

Banks solve this in a centralized way

Each transaction is recorded in a central database, with update permitted only by a short list of trusted financial intermediaries.

3 **CENTRALIZED DIGITAL CASH**

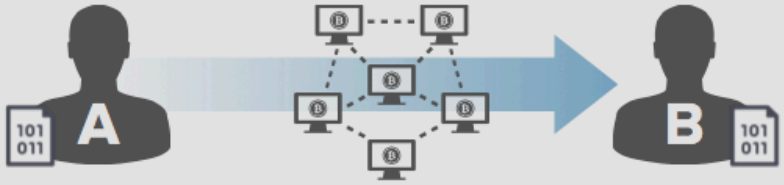
A sends **B** money.

C, a centralized bank, records debit/credit.

Trust

Bitcoin solves in a decentralized way

Each transaction is pushed out to a distributed database (the Blockchain), updated by a decentralized network of miners.



4 **DECENTRALIZED DIGITAL CASH**

A sends **B** money.

A global network of “miners” now records the debit/credit.

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.

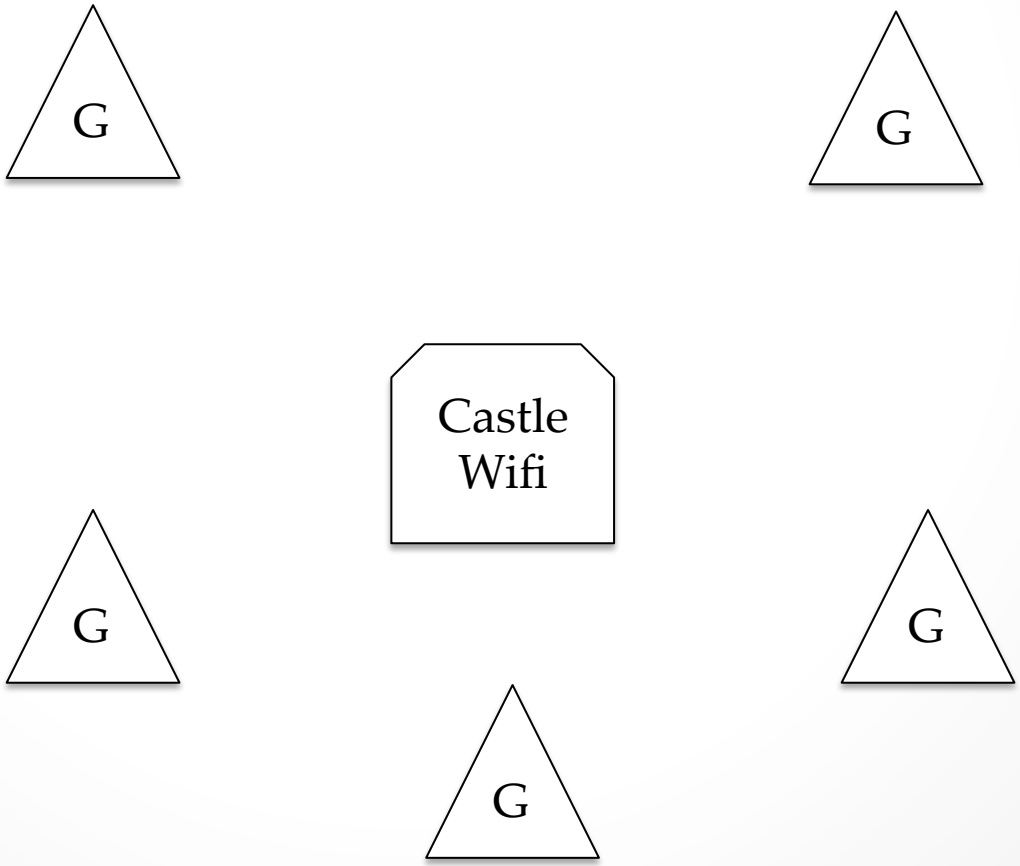
Public Append-Only Ledger

Payments As Bytes

- TCP/IP + HTTP -> information by the byte

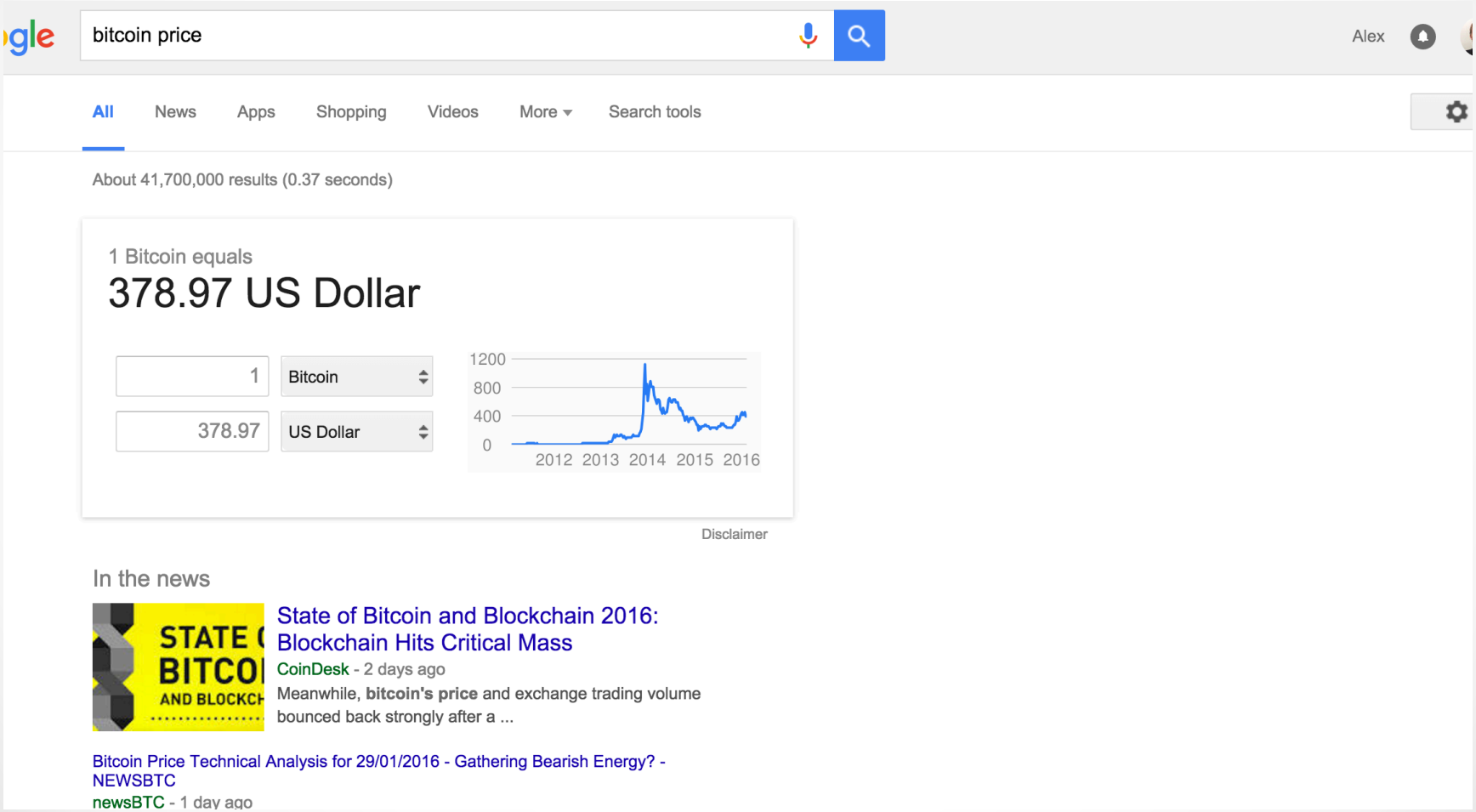
- Bitcoin -> payment by the byte

Solution to (a form of) the Byzantine General's Problem



The Why

A digital, trustless (safe?) store of value



Privacy

Alice: From 3NENLy72np5Gcb33YzDVvqaopapxx7voaDD **sends 1BTC**

Bob: Receives 1BTC at 3N5kutZzYCzyPoAcMxxUmSNHDTNDCKqC8xN

Privacy

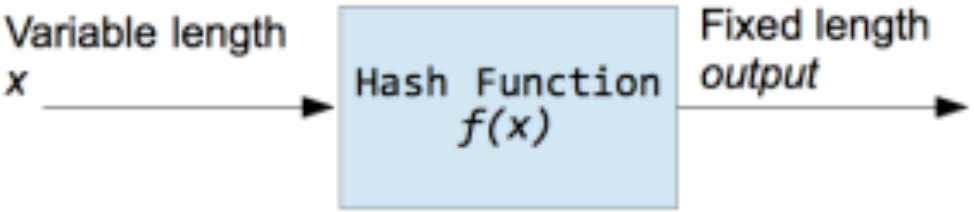

joe@gmail.com
Anyone can send you email if they know your public email address.
****
But **only you** can send email from that account with your private email password.
15qSxP1SQcUX3o4nhkfdbgyoWEFMomJ4rZ
Anyone can send you Bitcoin if they know your public Bitcoin address.
****
But **only you** can send Bitcoin from that address with your private Bitcoin key.

A New Source of Technological Innovation

- Identity and Reputation Services (BitID, Bitrated, OneName)
- Notary and Timestamping Services (CoinSpark, Factom)
- Decentralized Apps (Ethereum, Mastercoin, Counterparty)
- Decentralized Markets (OpenBazaar)
- Decentralized Prediction Markets (Augur)
- Decentralized Crowd Funding (LightHouse)
- Decentralized Crowd Storage (HiveDrive, StorJ, MaidSafe)
- Decentralized Asset Exchange (Bitshare, Medici)
- On-Demand Internet (Bitmesh)
- IoT device contract autonegotiation (IBM's ADEPT)

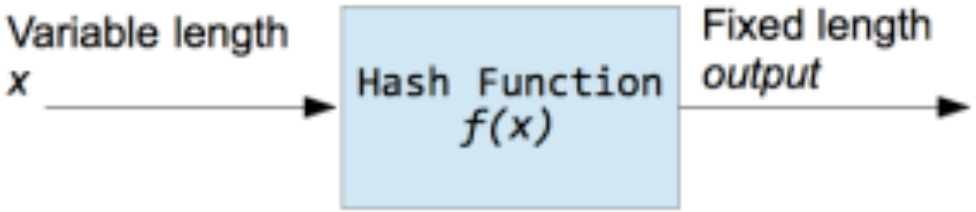
The How

Cryptographic One-Way Hash Functions



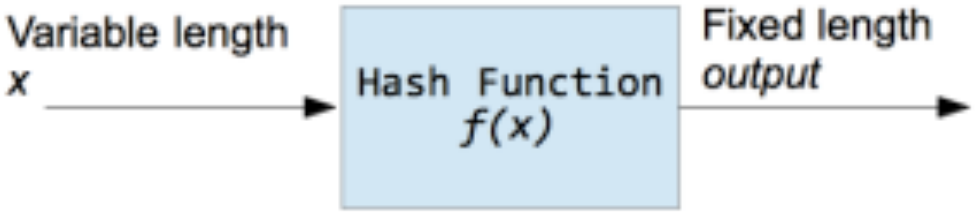
- Essential to mining (more on that later!)

Cryptographic One-Way Hash Functions



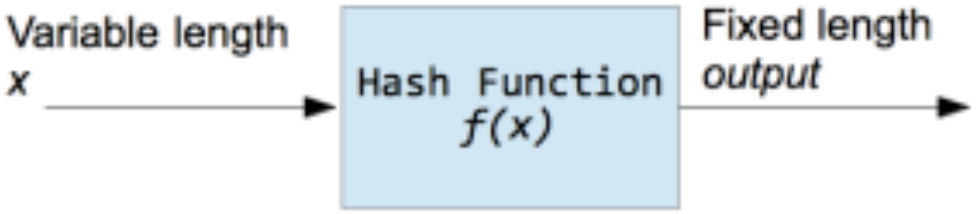
- Essential to mining (more on that later!)
- Prove existence without revealing information

Cryptographic One-Way Hash Functions



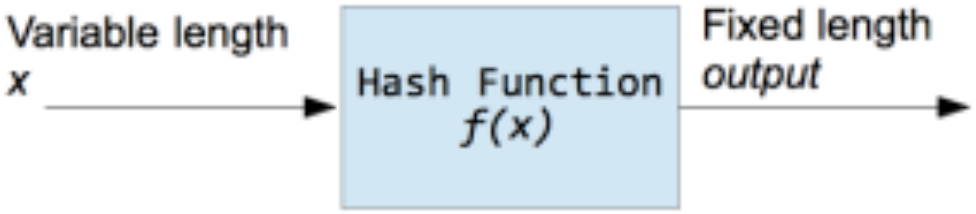
- Essential to mining (more on that later!)
- Prove existence without revealing information
- Also called trapdoor functions

Cryptographic One-Way Hash Functions



- MD5
  - Broken!
- SHA Family (Secure Hashing Algorithm)
  - SHA1
  - SHA256

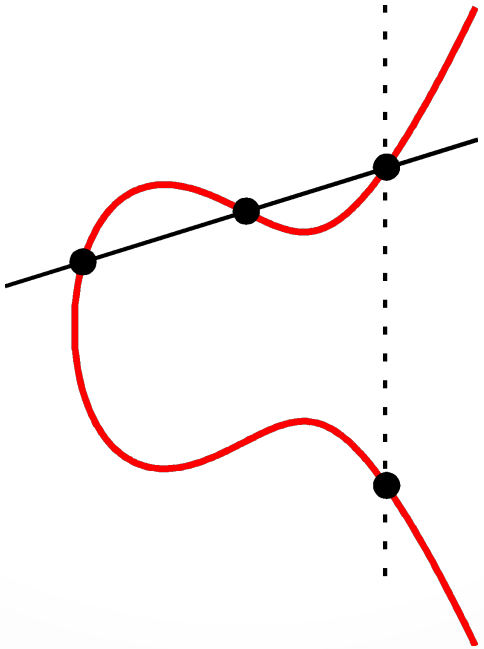
Cryptographic One-Way Hash Functions



Let's see it for ourselves!

Elliptic Curve Digital Signatures

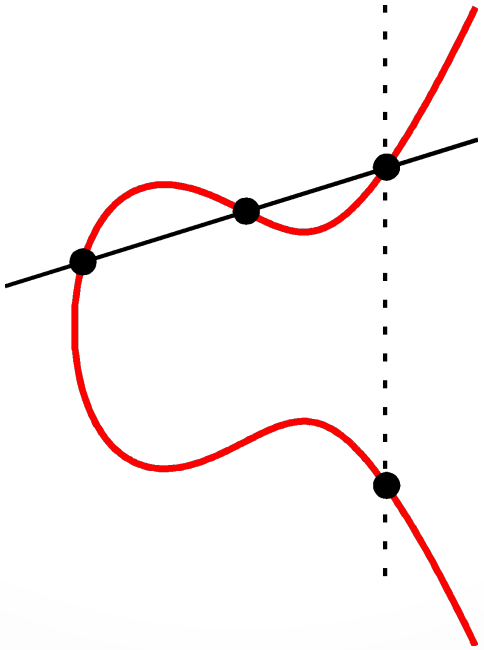
Used by Bitcoin to securely send transactions



Elliptic Curve Digital Signatures

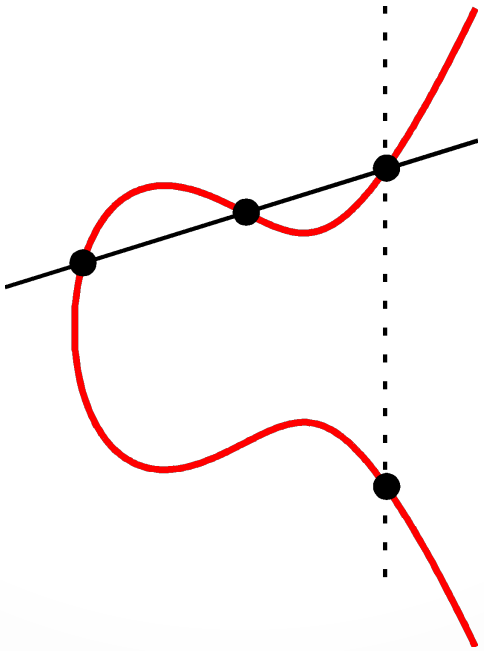
Believed to take exponential time to crack

Discrete Log Problem: **b^x = g**

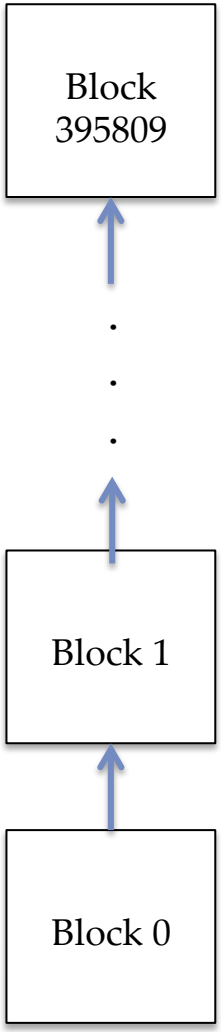


Elliptic Curve Digital Signatures

- See board for further explanation

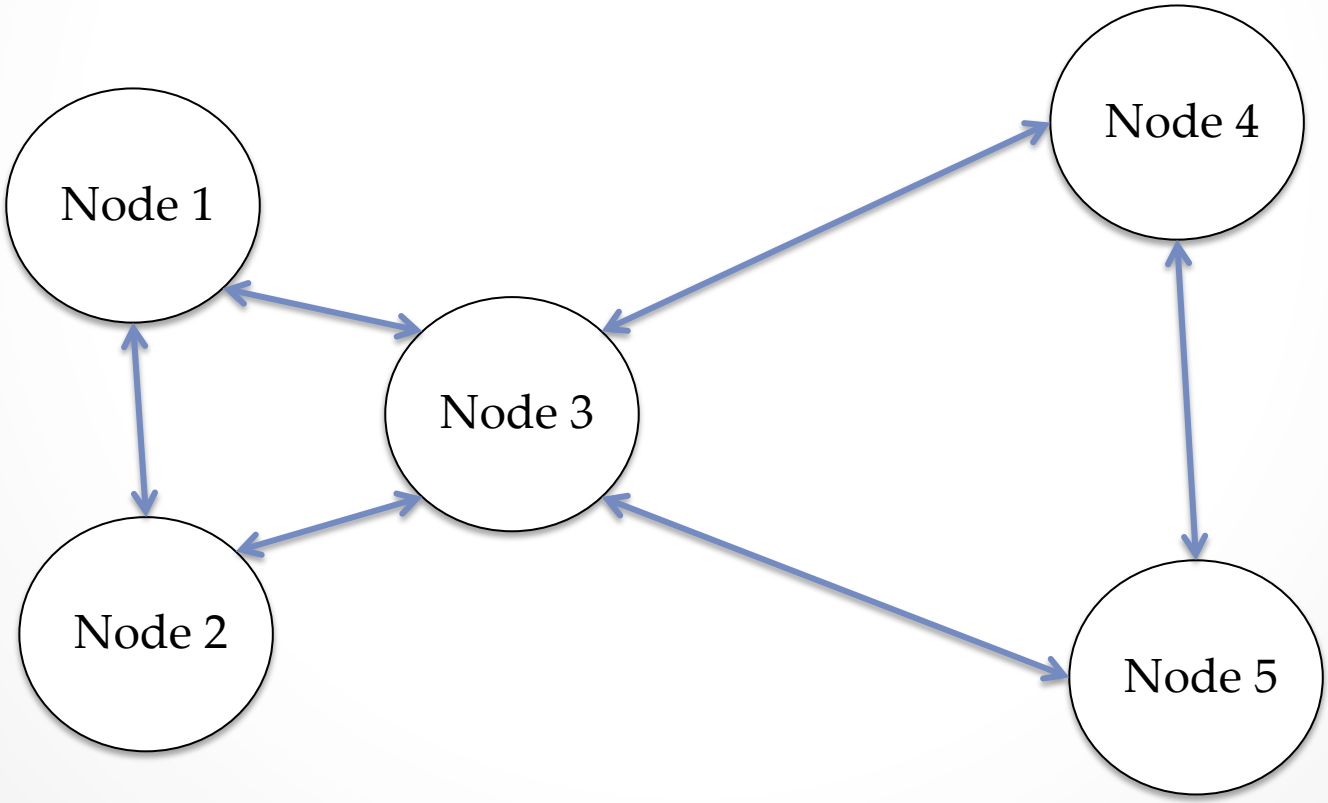


The Blockchain



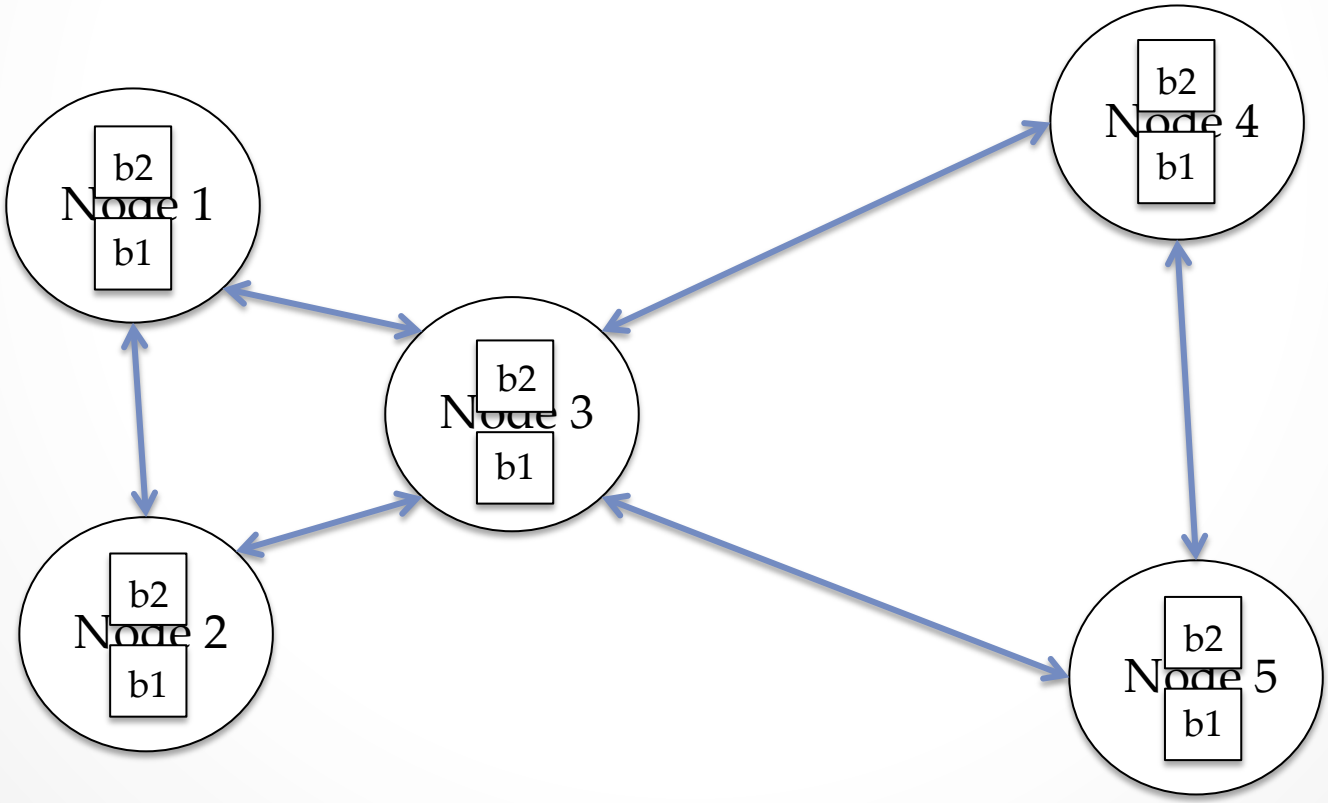
The Blockchain

Peer-to-peer system



The Blockchain

Peer-to-peer system



The Blockchain

Block header

- **Previous block head hash**: 0000…0002za9d20
- **Timestamp**: 2015 – 12 – 27 – 23 – 11 – 54
- **Difficulty:** 11293958399
- **Nonce:** 93958998
- **Merkle Root:** c91d93k9d…d93kdls

The Blockchain

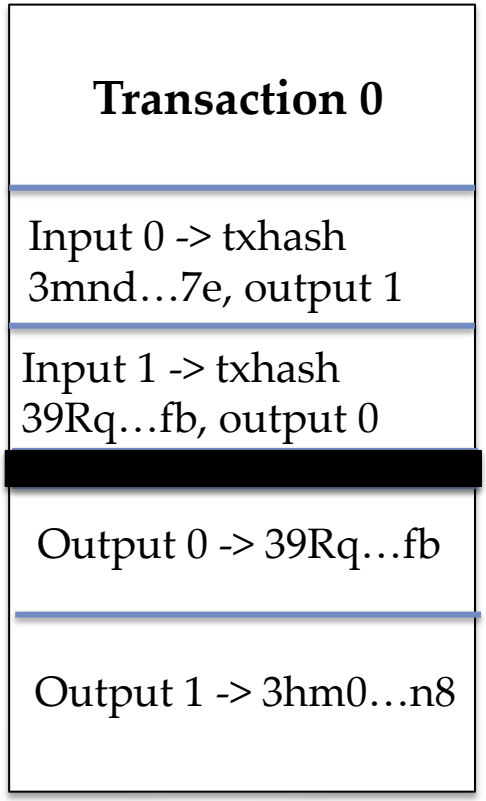
Addresses

152f1muMCNa7goXYhYAQC61hxEgGacmncB

3MENLy72np5Gcb33YzDVvqaopapxx7voaDD

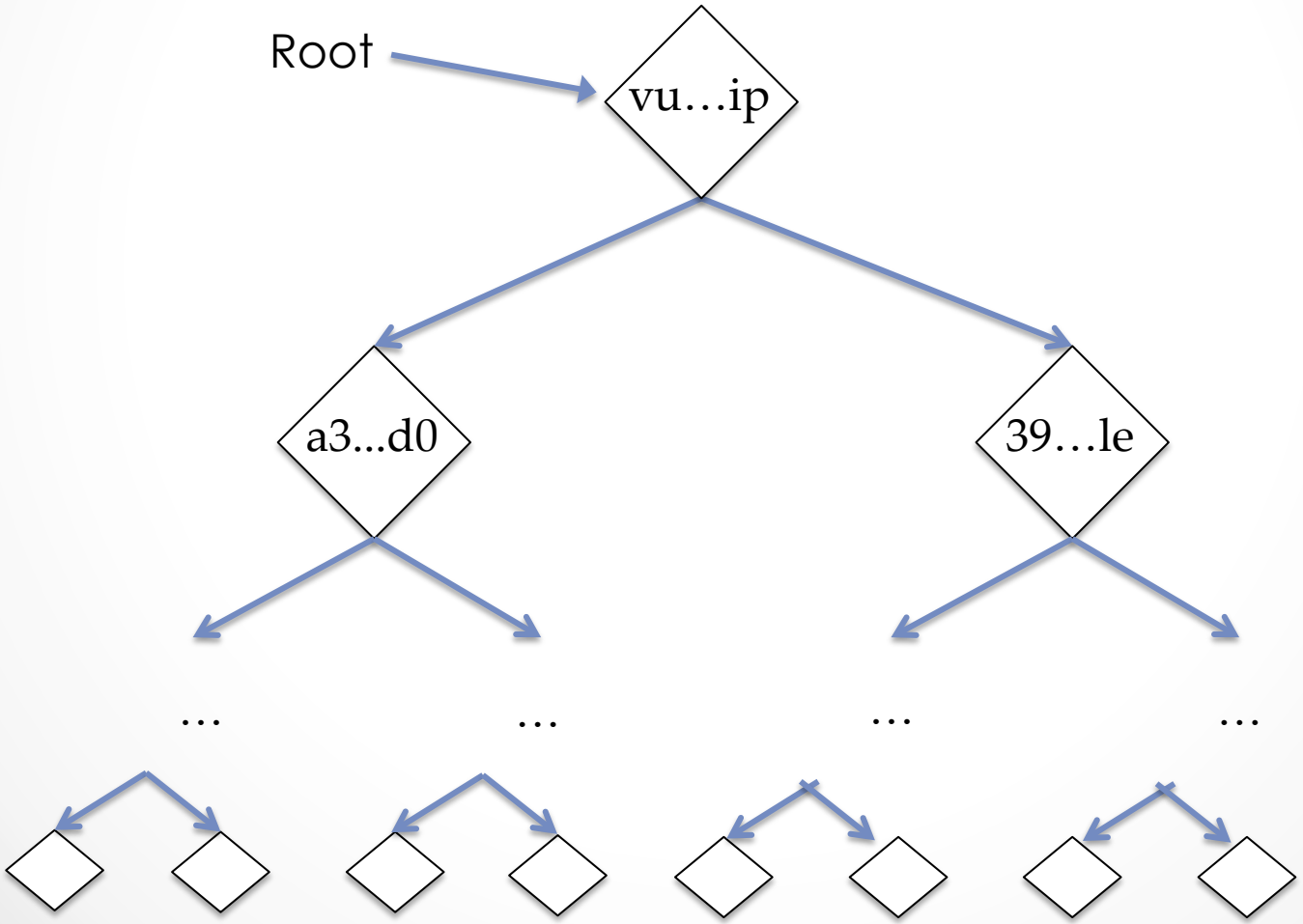
The Blockchain

Transactions

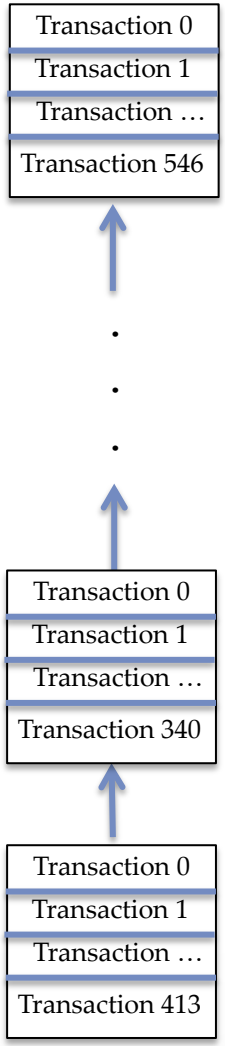


The Blockchain

Merkle Tree

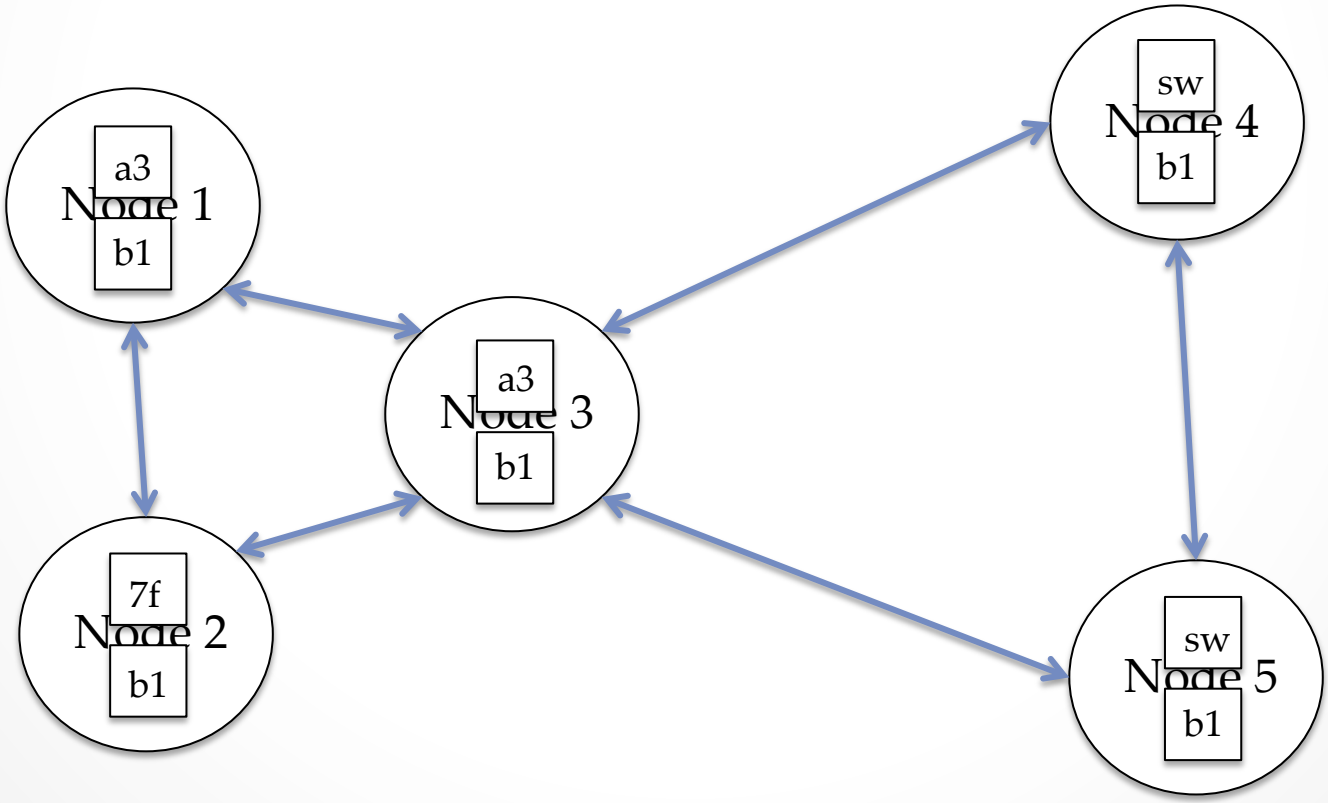


The Blockchain



The Blockchain

Remember! Everyone has a copy



Mining

It's all about **Proof of Work**

Mining

It's all about **Proof of Work**

Proof of Work = Showing the network that you have run sufficient computation to be awarded a block

Mining

It's all about **Proof of Work**

Proof of Work = Showing the network that you have run sufficient computation to be awarded a block

Proof of Work = sha256(sha256(blockheader)) < target

Mining

It's all about **Proof of Work**

Proof of Work = Showing the network that you have run sufficient computation to be awarded a block

Proof of Work = sha256(sha256(blockheader)) < target

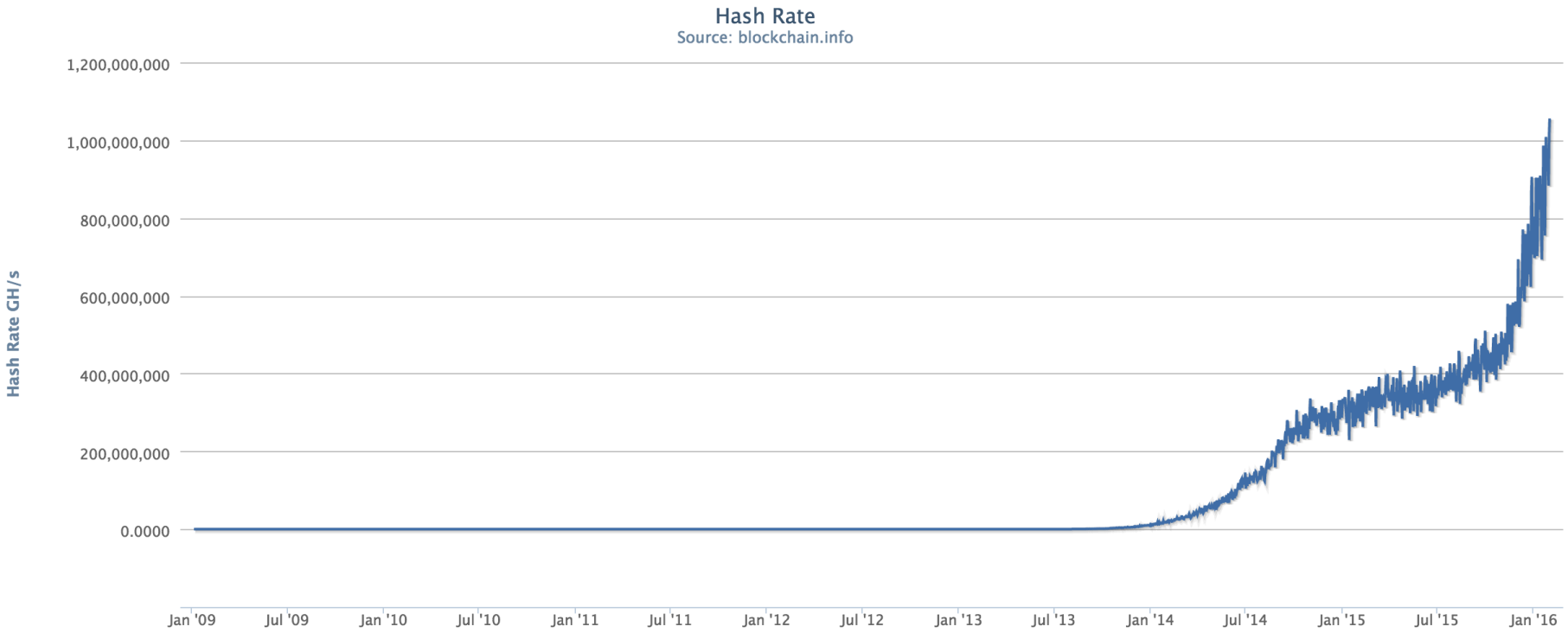
Proof of Work = Solving a difficult mathematical problem

Mining

Time + Electricity = 25 BTC

Mining

Mining


Hash Rate
Source: blockchain.info
Hash Rate GH/s
1,200,000,000
1,000,000,000
800,000,000
600,000,000
400,000,000
200,000,000
0.0000
Jan '09
Jul '09
Jan '10
Jul '10
Jan '11
Jul '11
Jan '12
Jul '12
Jan '13
Jul '13
Jan '14
Jul '14
Jan '15
Jul '15
Jan '16

Mining

- Let's mine!

Wallets

- Let's just go ahead and make a wallet