Permissionless Innovation

The Dawn of Decentralized Computing

Marco <amadori@inbitcoin.it>

inbitcoin for Speck & Tech — `https://inbitcoin.it`

Trento — October, 24 - 2016

Definitions

Definiton of Bitcoin

Bitcoin is a peer-to-peer network that maintains a public distributed ledger of digital math-based assets known as bitcoins.

Definiton of Computer

A computer is a system that takes data in input, elaborate them via a mathematical model and outputs data without interpreting them.

How hard is to forecast applications like videogames and social network out of this definition?

Definitions

Definiton of Bitcoin

Bitcoin is a peer-to-peer network that maintains a public distributed ledger of digital math-based assets known as bitcoins.

Definiton of Computer

A computer is a system that takes data in input, elaborate them via a mathematical model and outputs data without interpreting them.

How hard is to forecast applications like videogames and social network out of this definition?

Definitions

Definiton of Bitcoin

Bitcoin is a peer-to-peer network that maintains a public distributed ledger of digital math-based assets known as bitcoins.

Definiton of Computer

A computer is a system that takes data in input, elaborate them via a mathematical model and outputs data without interpreting them.

How hard is to forecast applications like videogames and social network out of this definition?

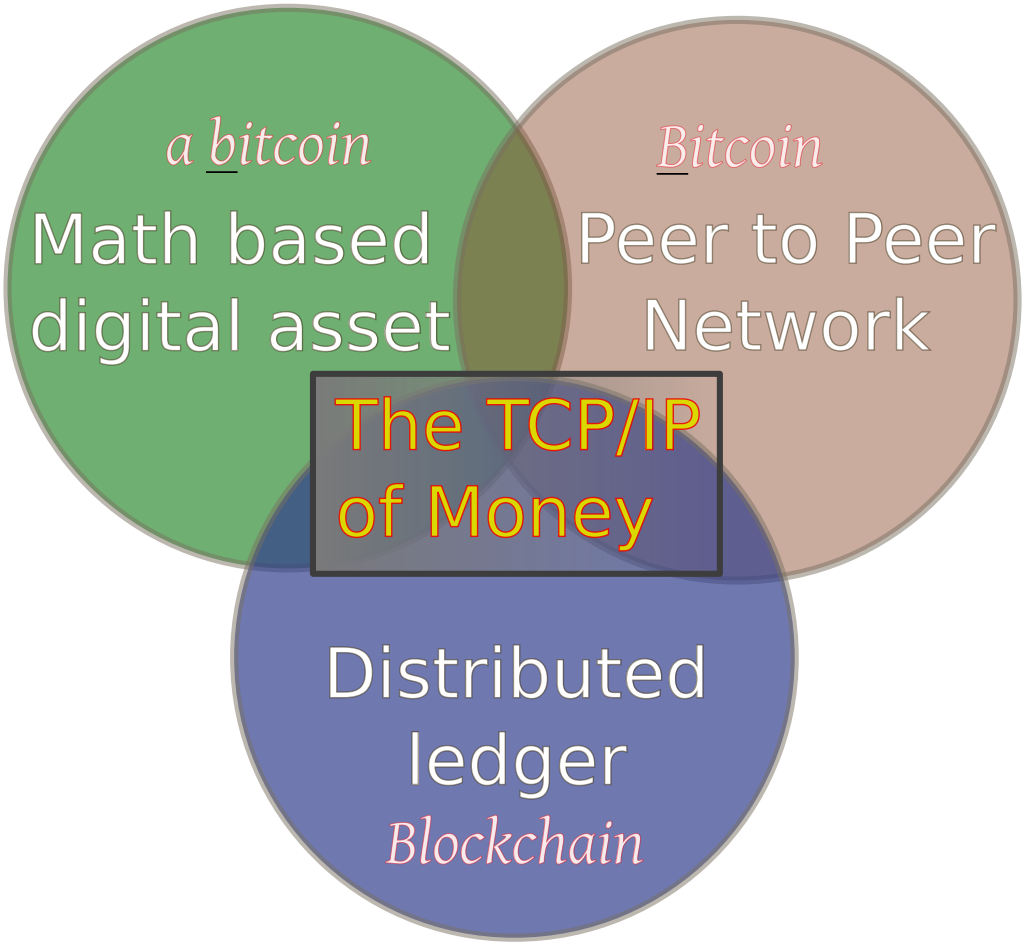
What is “Bitcoin”

A catchy but misleading name

- Bitcoin is a two words name (Bit Coin)
- it is a nice name for a Company or a Product, not for a Protocol (FaceBook, WalMart)
- TCP/IP is not called Bitflux or Netwire (Trasmission Control Protocol/Internet Protocol)
- Bitcoin could better indentified as P2P/DCP (Peer-to-Peer Digital Currency Protocol)

What is “Bitcoin”

The Currency, the Network, the Ledger



The currency
What is money?

Aristotle definition on money

1. It must be durable. Money must stand the test of time and the elements. It must not fade, corrode, or change through time.
2. It must be portable. Money hold a high amount of 'worth' relative to its weight and size.
3. It must be divisible. Money should be relatively easy to separate and re-combine without affecting its fundamental characteristics.
4. It must have intrinsic value. This value of money should be independent of any other object and contained in the money itself.

The currency
What is money?

Modern definition on money

- Exchange of value
- Unit of account
- Store of value

The Currency
The Grey Metal Metaphore

"As a thought experiment, imagine there was a base metal as scarce as gold but with the following properties:

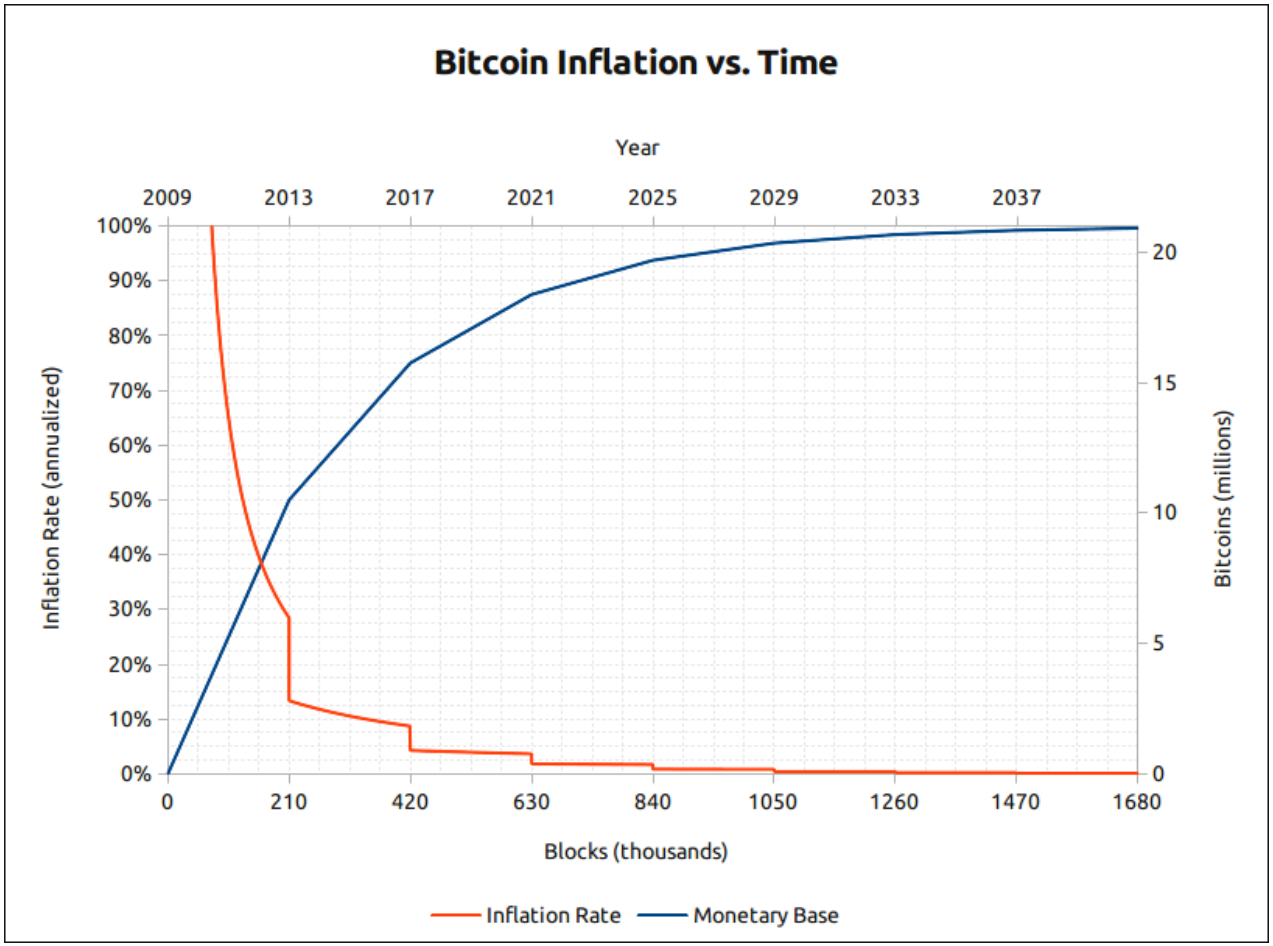
- boring grey in colour
- not a good conductor of electricity
- not particularly strong, but not ductile or easily malleable either
- not useful for any practical or ornamental purpose
- and one special, magical property:
  can be transported over a communications channel"

Satoshi Nakamoto – 27 August 2010

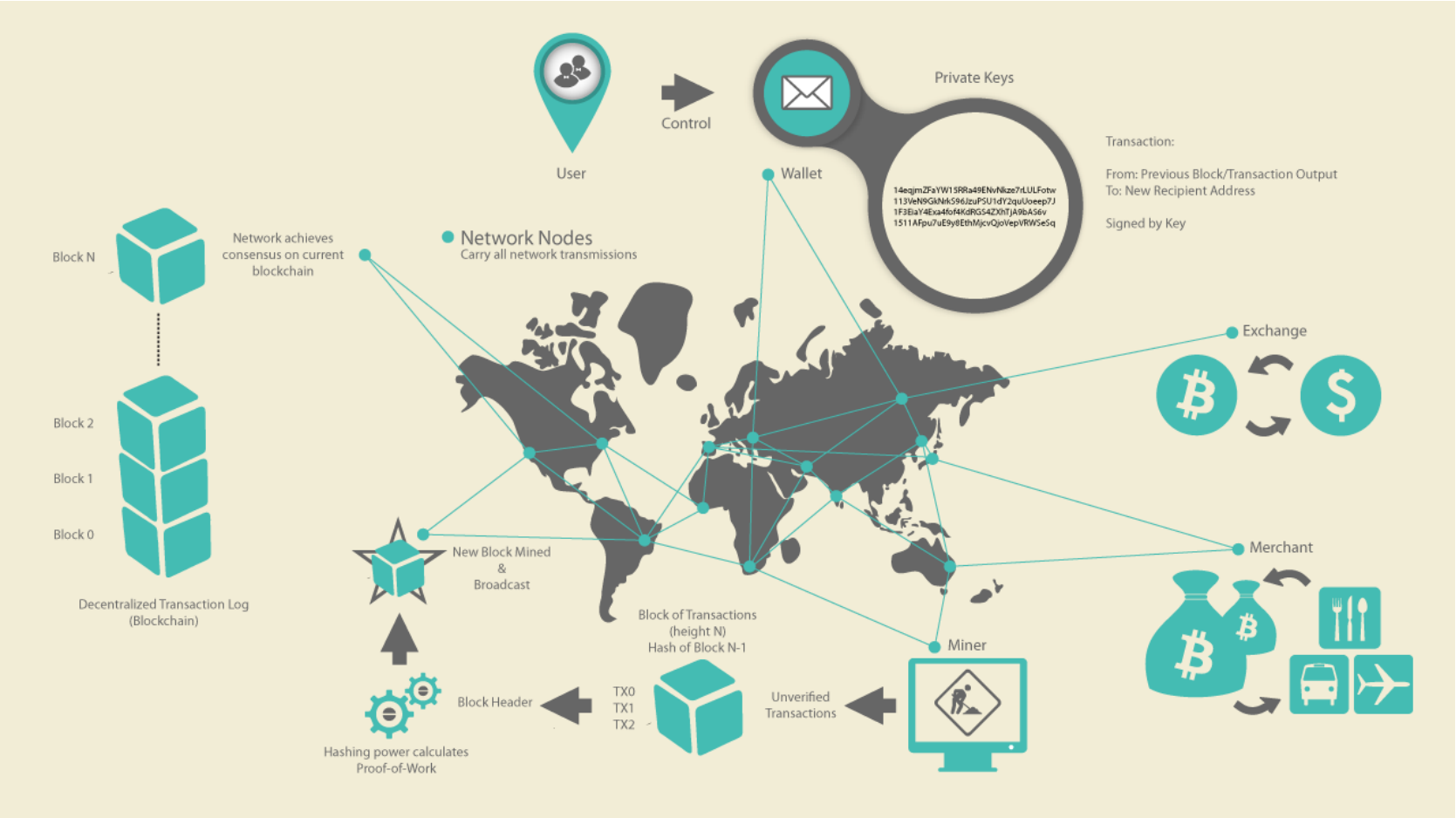
The Currency
Some information

- The supply of bitcoins is fixed at 21 millions, (now $\sim$16 M)
- Each bitcoin (BTC) can be divided in 10^8 units (1/100 000 000 is called one *satoshi*)
- The network tends to produce 12.5 new bitcoins every 10 minutes (block reward)
- The block reward is halved every $\sim$4 years (210 000 blocks)
- We are in the 3^{nd} reward era out of 34 (rewards ends in 2140)
- 1 BTC = 600 € on online exchanges

The Currency
Predictable Money Supply



Overview of the Network



Real time visuals: `http://bitcoinglobe.com/`

Who Invented Bitcoin?

Satoshi Nakamoto

- Satoshi Nakamoto, in 2008 publishes a white paper, “Bitcoin: a Peer-to-Peer Electronic Cash System” via “The Cryptography Mailing List”.
- In 2009–2011 he wrote a lot of posts (80000 words, the size of a novel) in flawless english with British colloquialisms (aside only the first post where he used American spellings).
- Satoshi is probably a pseudonym for a developer or a group, “vanished” from the web in April 2011 because he “moved to other things”
- If he is not a group, he is a world class programmer, with deep knowledge of C++, economics, cryptography and peer-to-peer networking.
- His timestamps speculation are about either east-coast US with a fairly normal sleep schedule or western Europe with a *coder* sleep schedule (probably not Japan)

Trusted third 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.""*
>
> — Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" – October 31, 2008

Trustless does not mean that we do not need to trust *anything*, but that we do not need to trust *anyone*.

Consensus in a decentralized system

The Byzantine Generals' problem

> *"A group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement."*
>
> — Marshall Pease, Robert Shosthak and Leslie Lamport, The Byzantine Generals Problem

Transactions

Transaction as Double-Entry Bookkeeping

Inputs	Value	Outputs	Value
Input 1	0.10 BTC	Output 1	0.10 BTC
Input 2	0.20 BTC	Output 2	0.20 BTC
Input 3	0.10 BTC	Output 3	0.20 BTC
Input 4	0.15 BTC		
Total Inputs:	0.55 BTC	Total Outputs:	0.50 BTC

	Inputs	*0.55 BTC*
-	*Outputs*	*0.50 BTC*
	Difference	*0.05 BTC (implied transaction fee)*

*"**spending** is signing a transaction which transfers value from a previous transaction over to a new owner identified by a bitcoin address"*

— Andreas M. Antonopoulos – Mastering Bitcoin – O'Reilly 2014

A Paper Wallet

Vires in numeris

Private Key

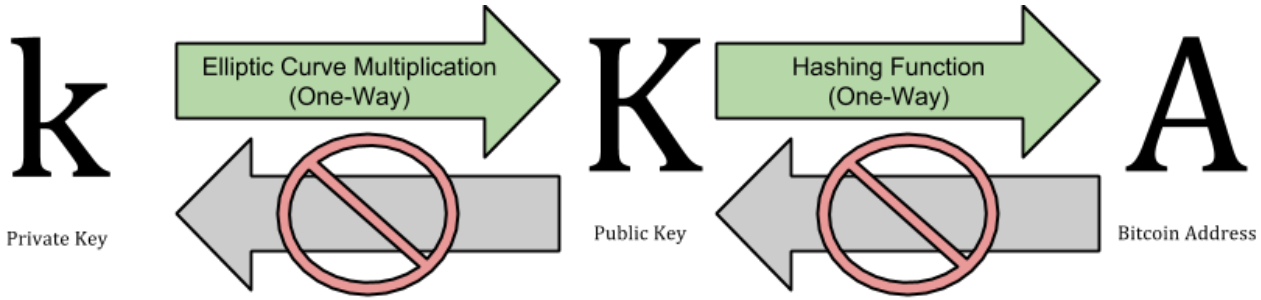
BIP38 Encrypted

6PRNsJqabLoT73aWNWfSa3hMcX6ML
mx779TPHbKzht4apwqsngkwFcBuKQ

Bitcoin Address

1fbk5AYjA7wLdwbru2CunWEuToBu1USsX

`https://blockchain.info/address/1fbk5AYjA7wLdwbru2CunWEuToBu1USsX`



Elliptic Curve Digital Signature Algorithm – secp256k1

Hash = RIPEMD160(SHA256(pubkey))

There are no transactions

just scripts

- A transaction (TX) is a script
  - the script language is called “Script” language
  - Script is a stack based language
  - Not Turing Complete by choice
  - A TX is valid if the script returns True
  - A TX has *k inputs* and *j outputs*
- Script P2PKH - Pay to Public Key Hash

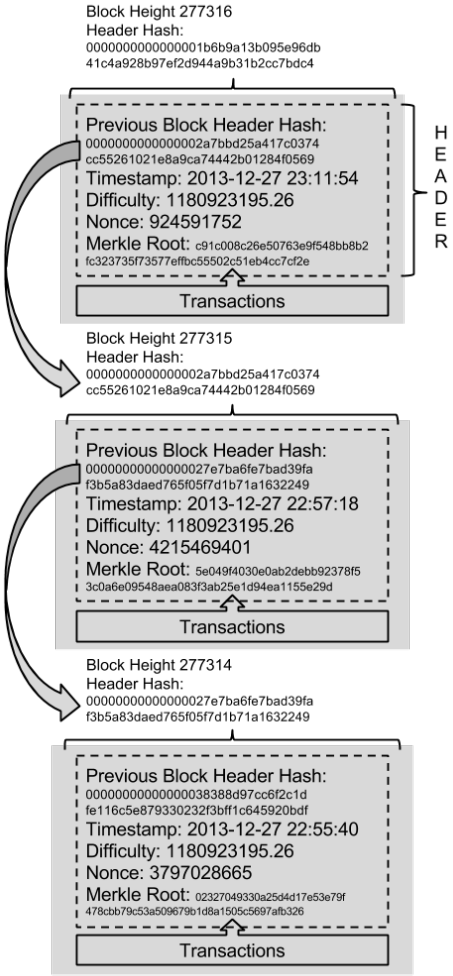
  `OP_DUP OP_HASH160 <pubKeyHash>`
  `OP_EQUALVERIFY OP_CHECKSIG`
- Script P2SH - Pay to Script Hash

  `OP_HASH160 <scriptHash> OP_EQUAL`

Wallet Types

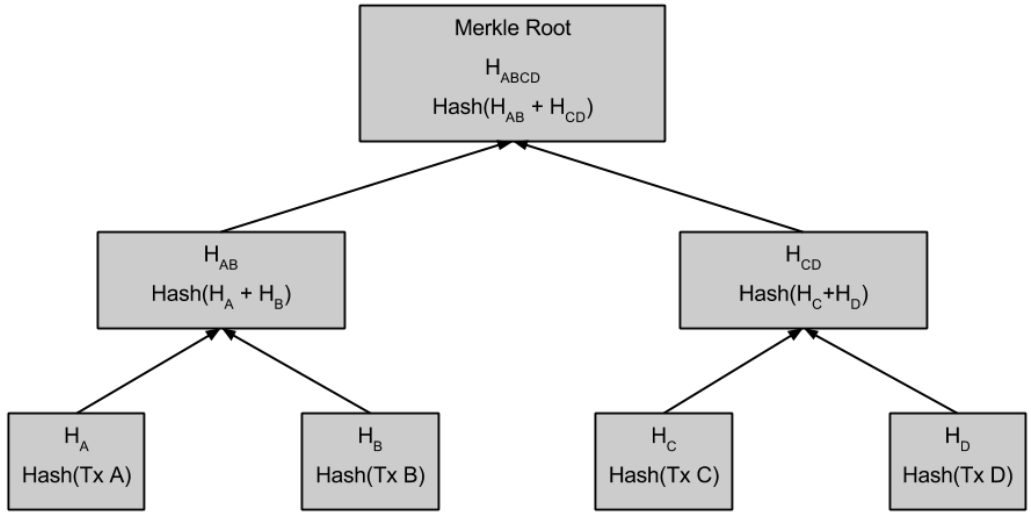
- Hot Wallet (online wallet)
  - Online Wallet without control of private keys
  - Online Wallet with control of private keys
  - Desktop PC wallet (Full node, SPV Wallets)
  - Smartphone Wallet
  - Multisig multiplatform Wallet (Altana)
- Cold Storage (disconnected wallet)
- Hardware Wallet (private keys not online)
- Brain Wallet (dangerous and powerful)

Chain of Blocks
A Distributed Ledger



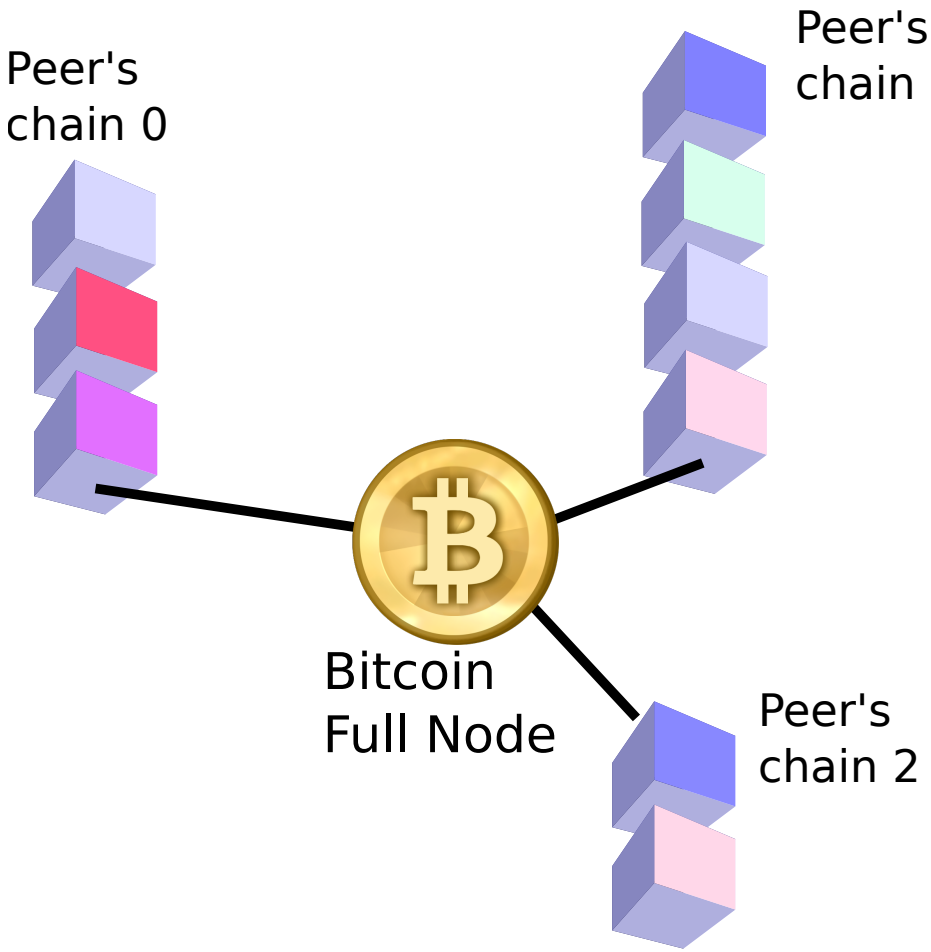
Secure Hash Algorithm – SHA256

The proof of work used in Bitcoin takes advantage of the apparently random nature of cryptographic hashes. A good cryptographic hash algorithm converts arbitrary data into a seemingly-random number.



Consensus via Proof of work

Longest chain wins



The "Work" is called "mining"

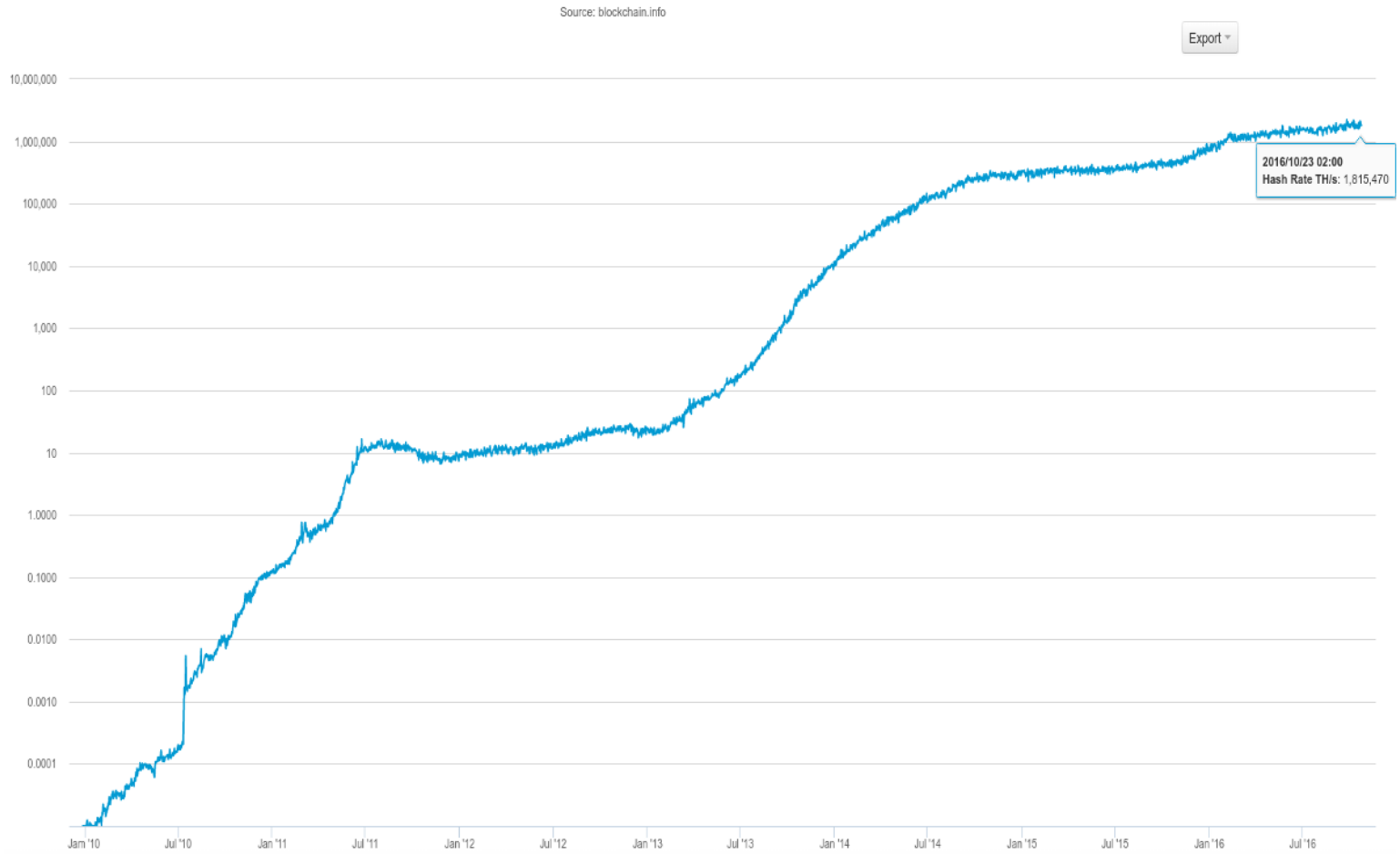
1. SHA256(SHA256(block header) + nonce) < *target* ?
2. The Bitcoin Network will reward me (25 BTC)

This is a new type of Cryptographic Signature, a **DMMS** — *Dynamic Membership Multi-party Signature*

Difficulty ("inverse" of target) will adapt to global hashrate every $\sim$ 2 weeks (2016 blocks)

Historycal Hashrate

Logarithmic Scale



Blockchain as DB

Permanent Storage

- You could write important data in the Blockchain (for a small bitcoin fee)
- What is written in the Blockchain is “forever”
- No one can remove or alter Blockchain information
- Example Application: Proof of Existence, Decentralization of Notary services

`http://www.proofofexistence.com/detail/`

`e3c21569e6ba5b488d5c416e8fc6ea166551cf64076f8f337ddc8cc8f9936bc0`

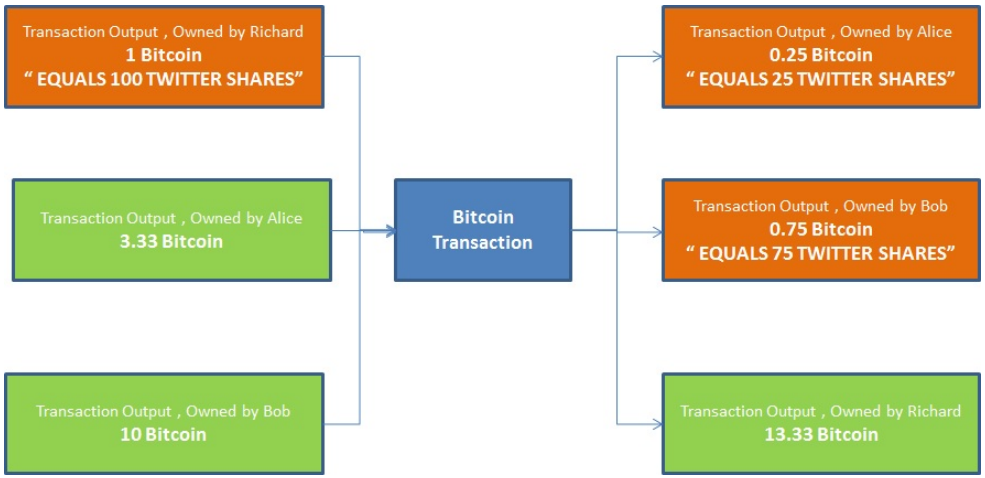
Permissionless Innovation

Bitcoin and Internet

- Before Internet, point-to-point communication between computers was available
- You needed a contract or permission from a Telco in order to innovate
- Low level of Innovation, fax-machine, poor video conferences, not much more
- Bitcoin opens an era of financial Innovation (programmable money)
- The Blockchain permits Decentralized Computing

Generic Asset Ledger
Coloring Coins

- Tracking bitcoin transaction to allow generic asset trading
- “coloring coins” enables innovation on top
- anyone can issue a colored coin



Multisignatures
Enabling Smart Contracts

- Wallets that need more than one signature to send a transaction
- k/n multisignatures are available in Bitcoin since 2012
- Smart Contracts are Trustless Unbreakable Agreements
- Example: micro and nanopayments trustless channels
- Example: decentralized escrow (OpenBazaar is a decentralized Ebay)
- Example: Smart Properties

Scaling Bitcoin
Need space?

- a typical TX is 300 bytes, 1Mb each 10 minutes
- **On chain TX are limited to 3 tps**
- Paypal like scaling (Coinbase users)
- Smaller TX (Segregated Witness, Schnorr signatures)
- Blocksize increase (Hard Fork required)
- Payment Channels
  - already available
  - exchange of presigned TX
  - TX not published on blockchain, just Open/Close CH

Scaling Bitcoin
Need speed?

- Lightning Networks
  - Payment Channels on steroids with Routing
  - Offchain Trustless Contracts > 1B tps
  - Smart contract and Game Theory based
- Sidechains
  - an altchain with BTC as the currency
  - bitcoin are locked in a chain to appear in the other chain
  - chain can have different rules and features
  - merged mining, federated mining

Security Issues
Bitcoin attacks

- 51% attack (50% +1)
- Finney or “Block Withholding” Attack
- The Race Attack
- Key Guessing / Collision Attacks
- Non-Bitcoin / Infrastructure Attacks
- Non-Technical Attacks / Scams

Why Cybersecutity and Bitcoin?

- **Money is Data, Data is Money**
- This dramatically increases the security requirements
- Keys must be stored safely
- New motivations (10 B$ Bounty) for hacking of desktop and smarphone devices
- Security in a decentralized system

What Next?
Questions?

- Which topic needs more care?
- Security and Wallets handling
- Protocol security issues
- Cryptographic underliyng protocols security
- Trustless Smart Contracts
- New applications brainstorming

These slides

`http://goo.gl/BbzhTT` [github: mammadori, branch “speck”]