Permissionless Innovation

The Dawn of Decentralized Computing

Marco Amadori <amadori@fbk.eu>
<marco.amadori@gmail.com>

Fondazione Bruno Kessler — https://www.fbk.eu

Trento — 6 November 2014

FONDAZIONE
BRUNO KESSLER

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?

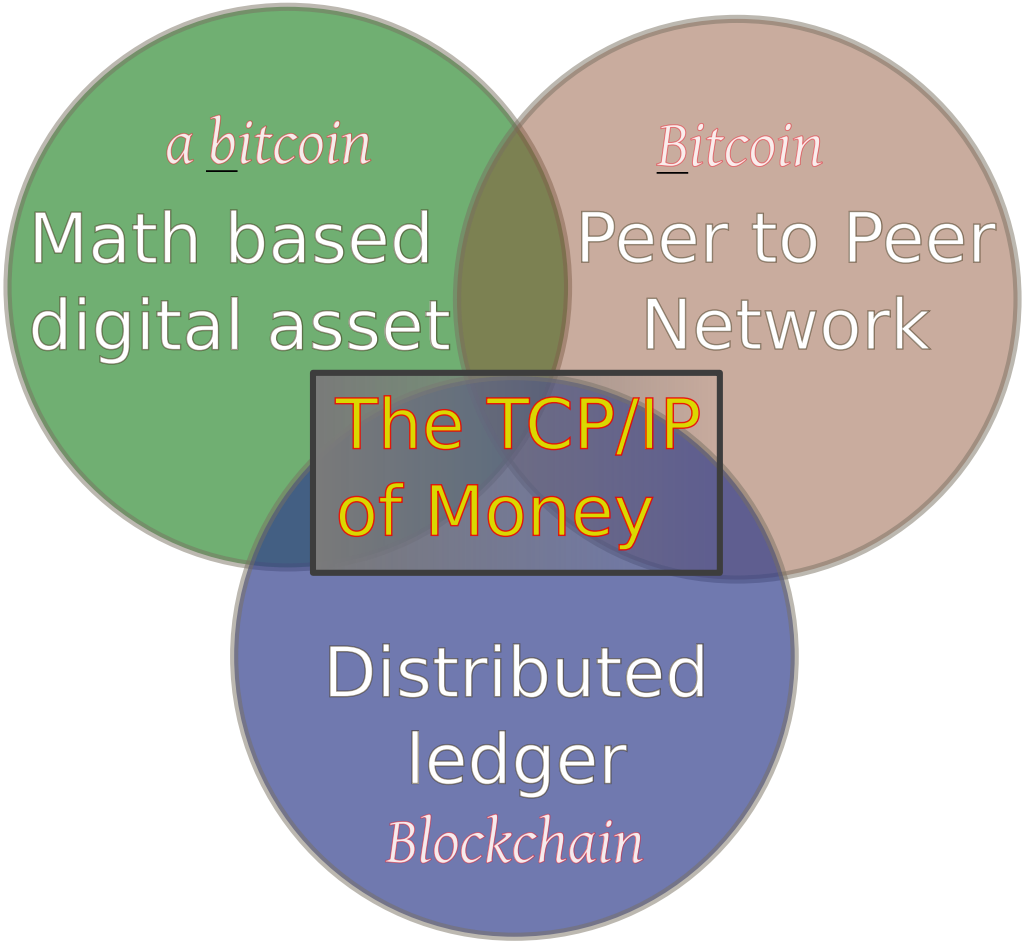
What is “Bitcoin”

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

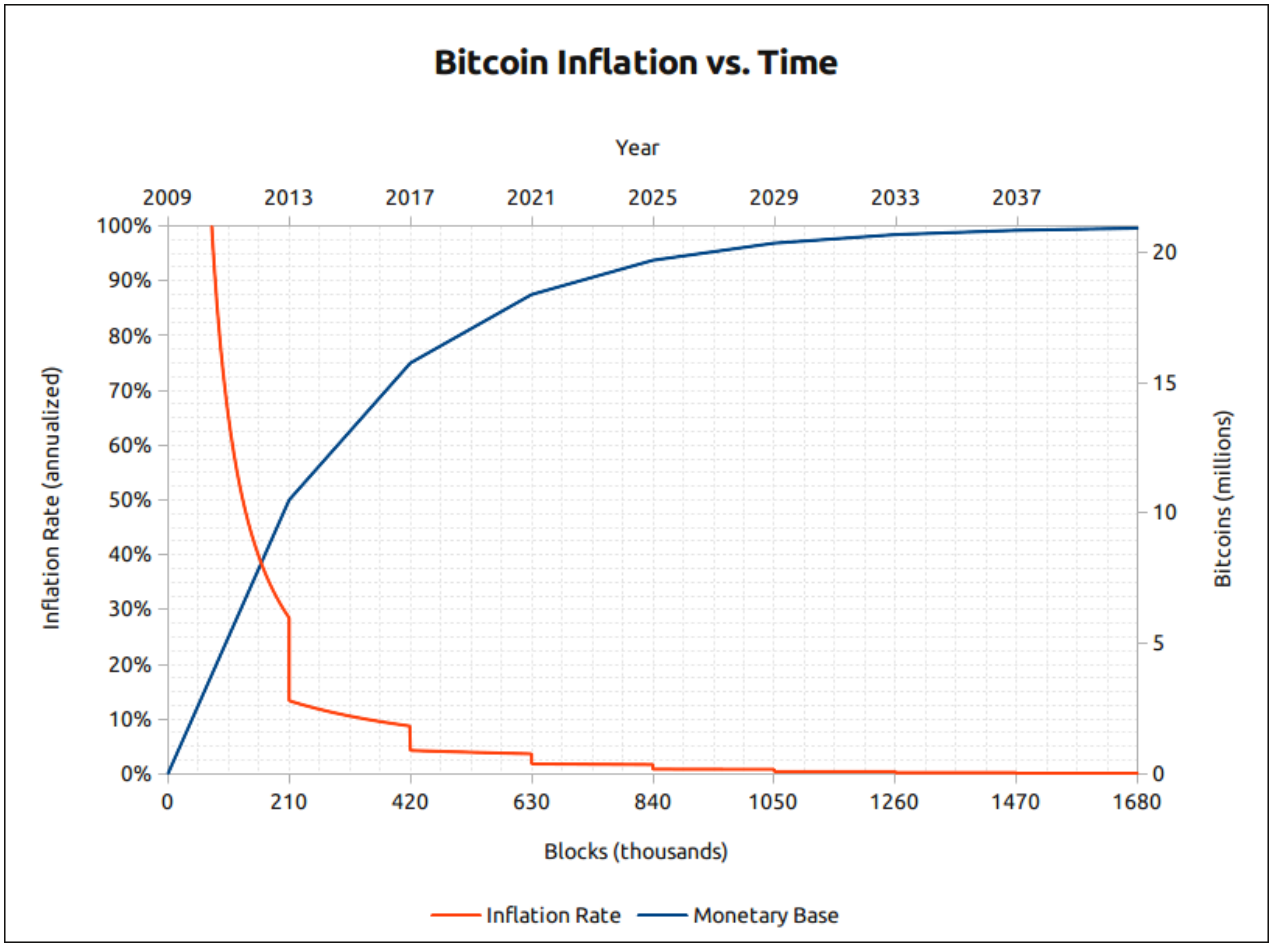
The Currency

Some information

- The supply of bitcoins is fixed at 21 millions, (now ∼13 M)
- Each bitcoin (BTC) can be divided in 10^8 units (1/100 000 000 is called one *satoshi*)
- The network tends to produce 25 new bitcoins every 10 minutes (block reward)
- The block reward is halved every ∼4 years (210 000 blocks)
- We are in the 2nd reward era out of 34 (rewards ends in 2140)
- 1 BTC = 310 € 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

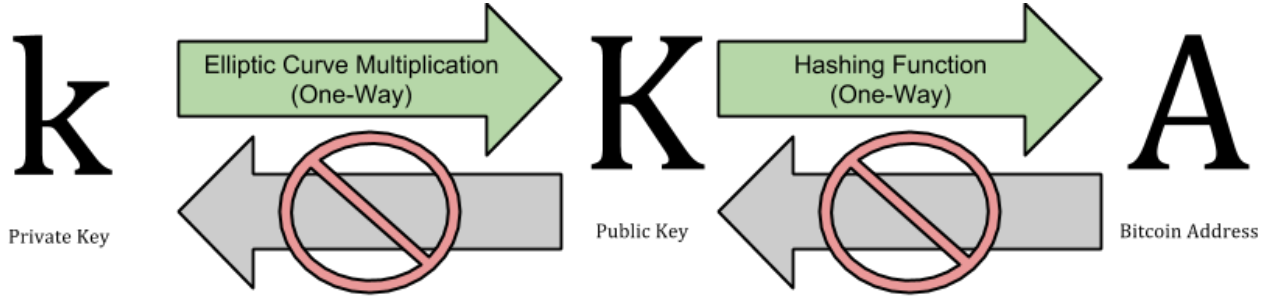
BIP38 Encrypted

6PRNsJqabLoT73aWNWfSa3hMcX6ML
mx779TPHbKzht4apwqsngkwFcBuKQ

Bitcoin Address

1fbk5AYjA7wLdwbru2CunWEuToBu1USsX

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



Elliptic Curve Digital Signature Algorithm – secp256k1

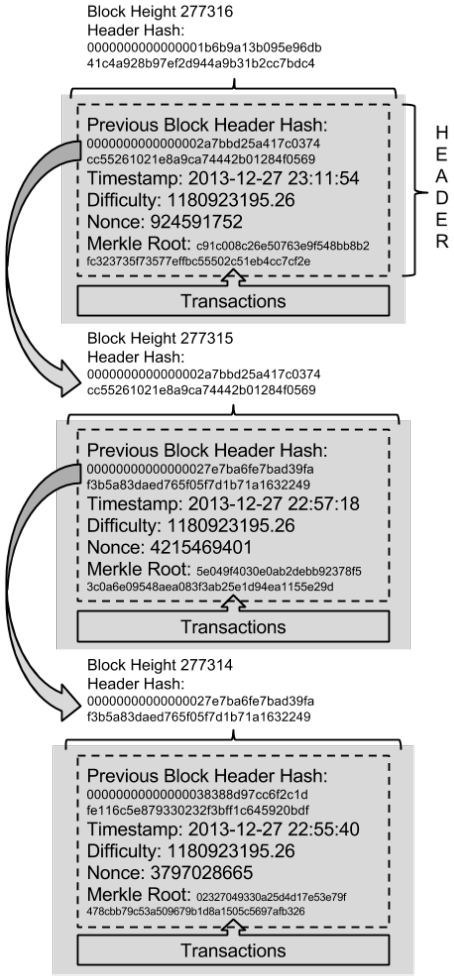
Hash = RIPEMD160(SHA256(pubkey))

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
- Cold Storage (disconnected wallet)
- Hardware Wallet (private keys not online)
- Brain Wallet
- HD Wallets (Masterkey $\Rightarrow$ multiple private keys)
- Multisignatures (p2hs)

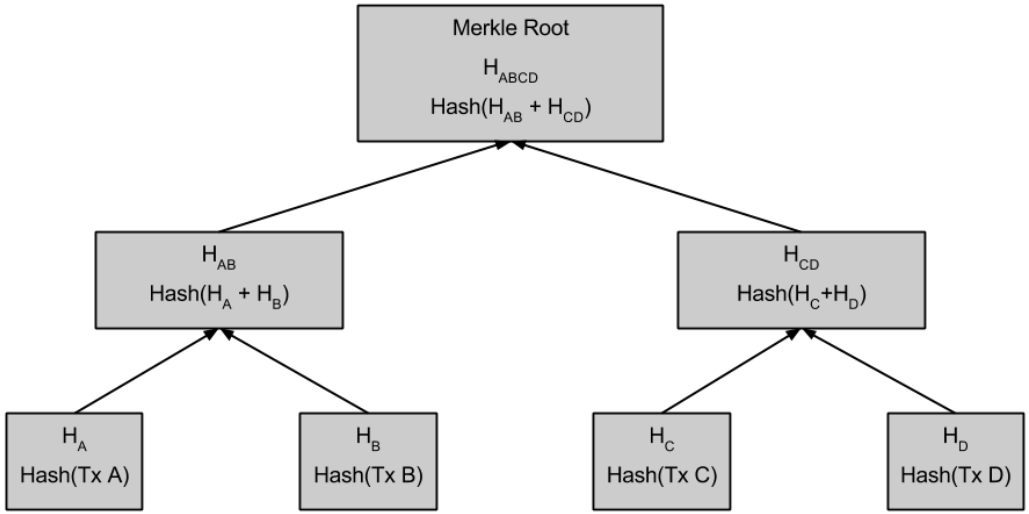
Chain of Blocks

A Distributed Ledger



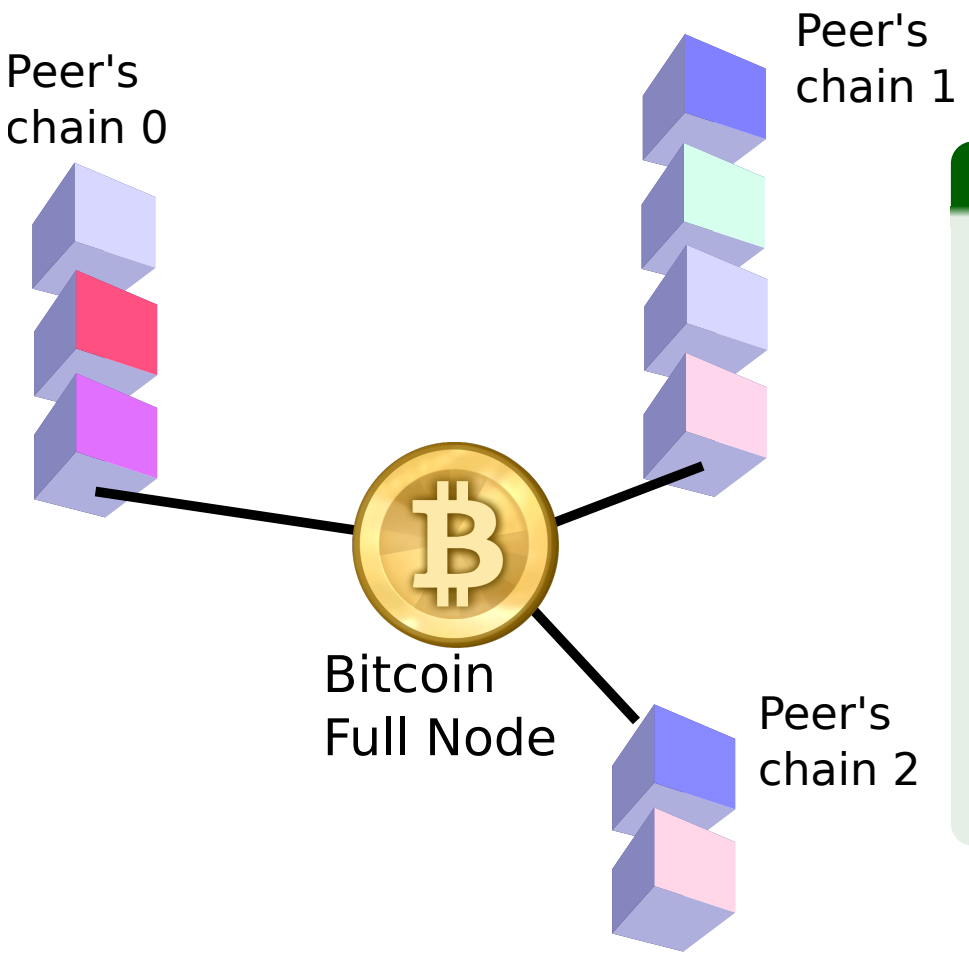
Secure Hash Algorithm – SHA256

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"

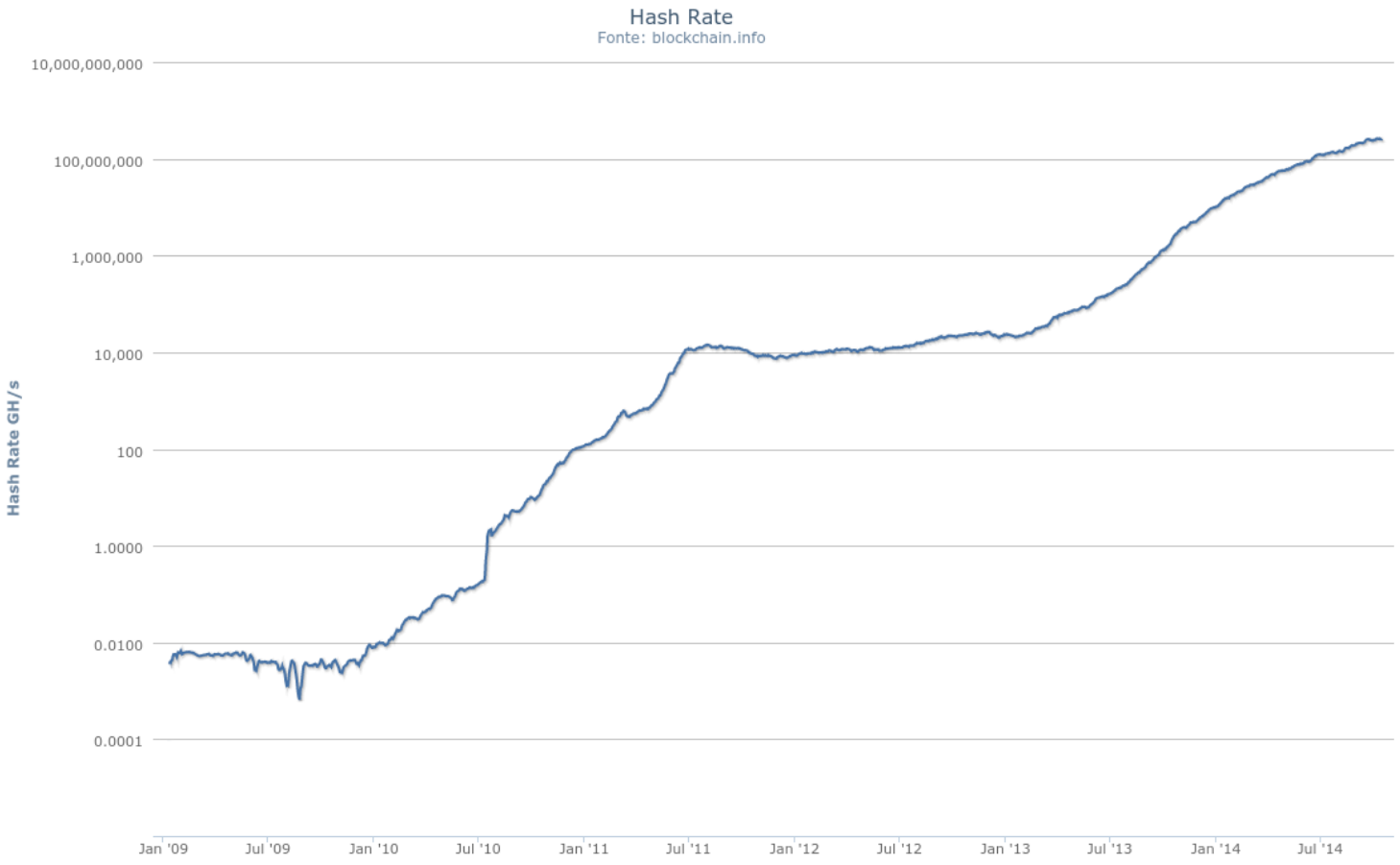
1. SHA256(SHA256(block header) + nonce) < *target* ?
2. The Bitcoin Network will reward me (25 BTC)

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



Random Quotes

Taking Breath

"Bitcoin is a remarkable cryptographic achievement and the ability to create something that is not duplicable in the digital world has enormous value."

— Eric Schmidt (Google's former CEO)

"Not having an internet strategy in 1995 is the equivalent of not having a bitcoin strategy now."

— Moe Levin (Bitpay CEO)

"By 2005 or so, it will become clear that the Internet's impact on the economy has been no greater than the fax machine's."

— Paul Robin Krugman – Nobel Memorial Prize in Economic Sciences (1998)

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

Usage Metrics

Latest quarter

	Quarterly			Last 12 Months	
	Sep-14	Jun-14	Q/Q Δ	Sep-13	Δ
Commerce					
Wallets	6,559,978	5,427,688	21%	1,353,201	5x
Merchants	76,000	63,000	21%	10,000	8x
Merchants' annual revenue ($bn)	86	29	196%	0	N/A
ATMs	251	103	144%	0	N/A
Unique bitcoin addresses	184,554	136,152	36%	61,734	3x
Industry					
All-time VC investment ($m)	317.0*	225.3	41%	30.4	10x
Number of VC-backed startups	66*	50	32%	14	5x
Media					
Mainstream media mentions	9,398	9,024	4%	1,794	5x
Technology					
Network Hash Rate (billion/second)	261,900,382	111,194,683	136%	1,213,246	216x
Github no. of updated repositories	18,753	15,109	24%	1,573	12x
Valuation					
Bitcoin market capitalization ($bn)	5.2	8.3	-37%	1.5	3x

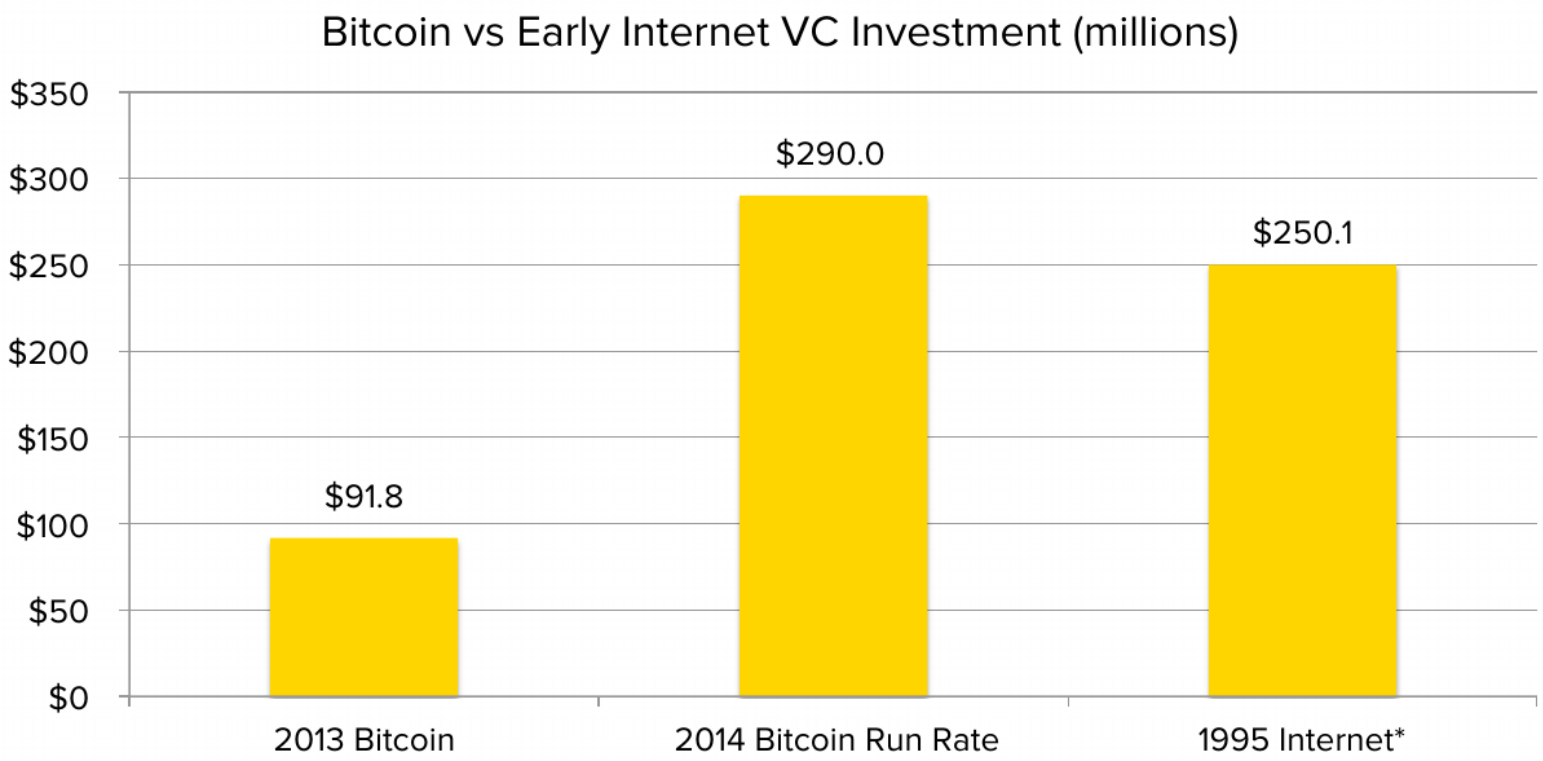
*Includes recent Q4 deals (eg Blockchain $30.5m).

Sources: CoinDesk, Blockchain.info, BitcoinPulse, Github, Coin ATM Radar. Figures used are as of end of quarter.

- http://coinmap.org/

What is happening?

Status of Venture Capitals



*Includes first sequence venture deals but excludes late-stage 1995 internet investments ($257.6m). For additional disclosure on methodology see http://www.coindesk.com/following-money-trends-bitcoin-venture-capital-investment/

Source: CoinDesk, PricewaterhouseCoopers

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
- Internet of Things: IBM's "Adept" will use the Blockchain

Blockchain as DB

Permanent Storage

- You could write important data in the Blockchain (for free or for a small 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

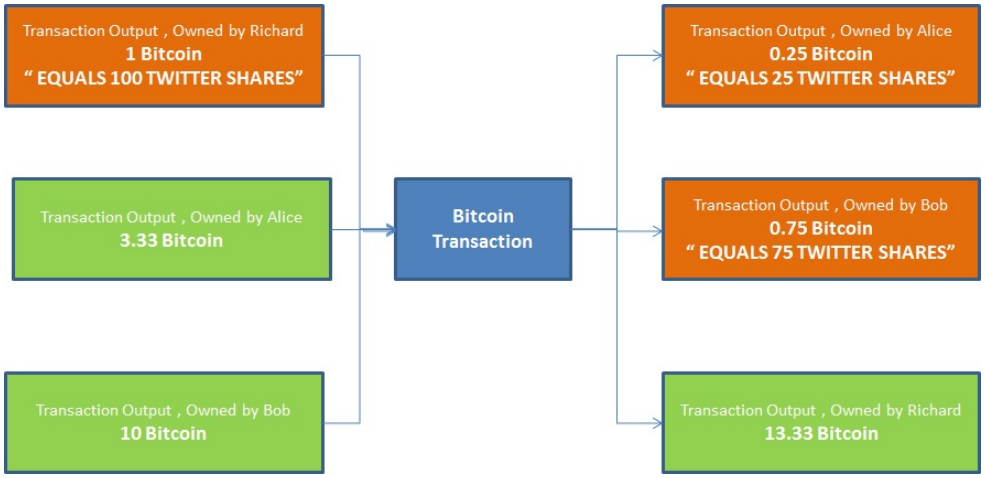
`http://www.proofofexistence.com/detail/`

`e3c21569e6ba5b488d5c416e8fc6ea166551cf64076f8f337ddc8cc8f9936bc0`

Generic Asset Ledger

Coloring Coins

- Tracking bitcoin transaction to allow generic asset trading
- “coloring coins” enables distributed exchanges
- 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

Crypto currencies

640 currencies should be enough for everyone

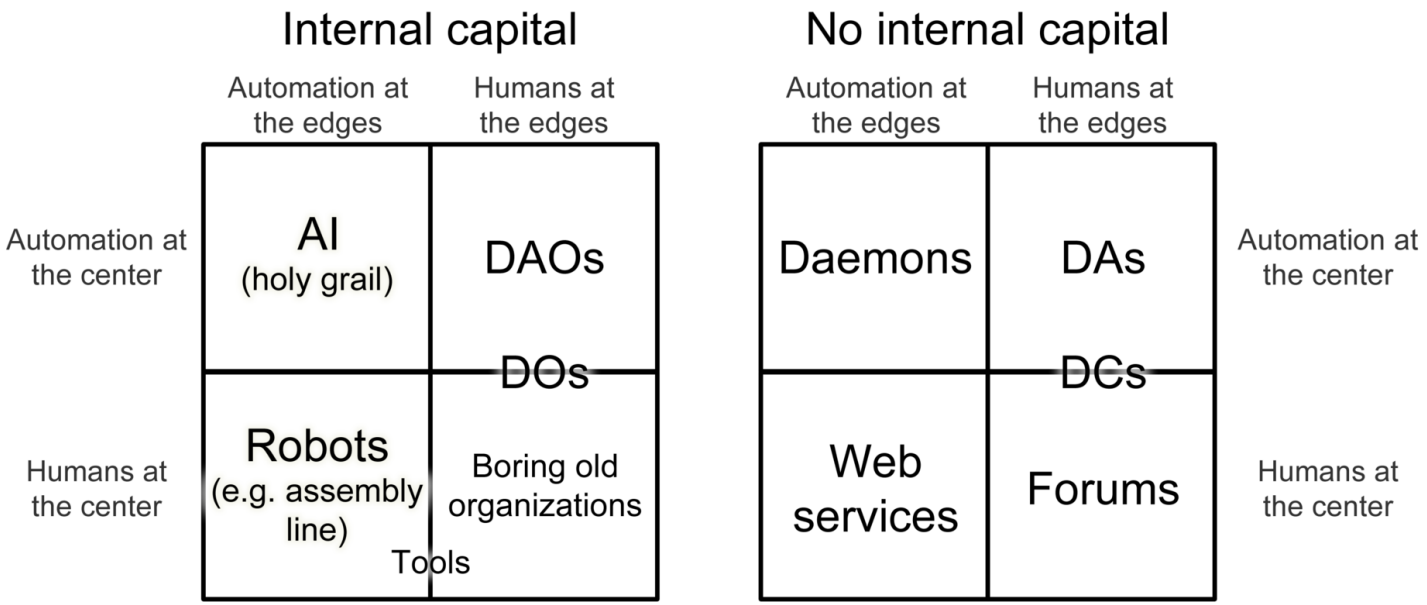
#	Name	Market Cap	Price	Available Supply	Volume (24h)
1	Bitcoin	€ 3.681.775.431	€ 273.33	13,470,025 BTC	€ 11.075.275
2	Ripple	€ 112.521.946	€ 0.003882	28,989,252,282 XRP *	€ 235.763
3	Litecoin	€ 97.392.370	€ 2.90	33,563,705 LTC	€ 2.052.311
4	BitSharesX	€ 27.824.896	€ 0.013913	1,999,883,512 BTSX *	€ 286.588
5	Dogecoin	€ 17.085.031	€ 0.000180	95,166,195,027 DOGE	€ 392.888
6	Nxt	€ 16.067.217	€ 0.016067	999,997,096 NXT *	€ 26.691
7	Peercoin	€ 13.629.943	€ 0.623657	21,854,853 PPC	€ 41.736
8	Counterparty	€ 9.303.871	€ 3.51	2,647,154 XCP *	€ 31.952
9	Namecoin	€ 7.163.043	€ 0.705097	10,158,950 NMC	€ 12.924
10	Darkcoin	€ 6.840.358	€ 1.42	4,832,408 DRK	€ 41.911

- Initially forks of bitcoin codebase
- Purpose-Specific or Experimental testbed
- Different parameters or hash Algorithm
- Due to being tied to bitcoin, they become real money too (crypto exchanges)
- Less network effect, no real threat to Bitcoin

Appcoins

Ethereum example

- Bitcoin full nodes execute a Non-Turing Complete script (handling of transactions, signatures)
- What if the script is Turing Complete?
- A platform for Smart Contracts `http://www.ethereum.org`
- Distributed Applications
- Distributed Autonomous Corporations



Bitcoin for good

Payment system for developing countries

- 50 % of the world is unbanked
- Kenya: 50 % of gdp is transacted via Mpesa, SMS money
- Remittances: $\sim$400 B$ market, 8% average fee
- Microcredits

Why Security and Trust?

- **Money is Data, Data is Money**
- This dramatically increases the security requirements
- Keys must be stored safely
- New motivation for hacking of desktop and smarphone devices
- Security in a decentralized system

What Next?
Questions?

- Which topic needs more care? (next 2 events)
- 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 “st”]