

# Permissionless Innovation

## Bitcoin Research Challenges

### The Dawn of Decentralized Computing

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

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

Trento — 10 October 2014



# 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

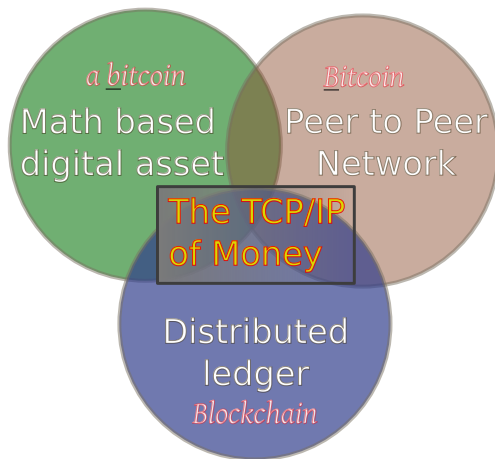
A computer is a system that takes data in input, elaborate them via a mathematical model and outputs data without interpreting them.

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



# What is “Bitcoin”

The Currency, the Network, the Ledger



# 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

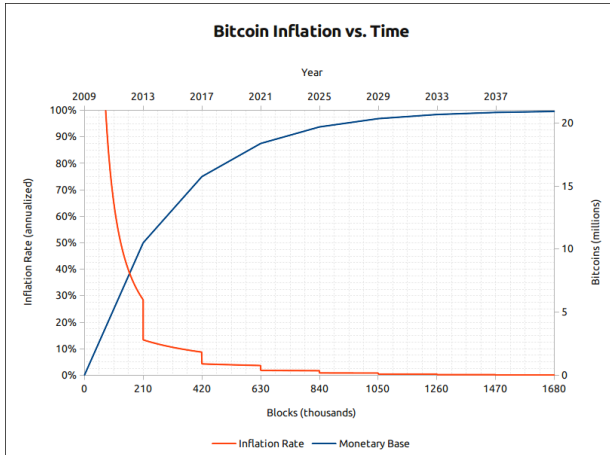
## Some information

- The supply of bitcoins is fixed at 21 millions, (now  $\sim 13$  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  $\sim 4$  years (210 000 blocks)
- We are in the  $2^{nd}$  reward era out of 34 (rewards ends in 2140)
- 1 BTC = 310 € on online exchanges



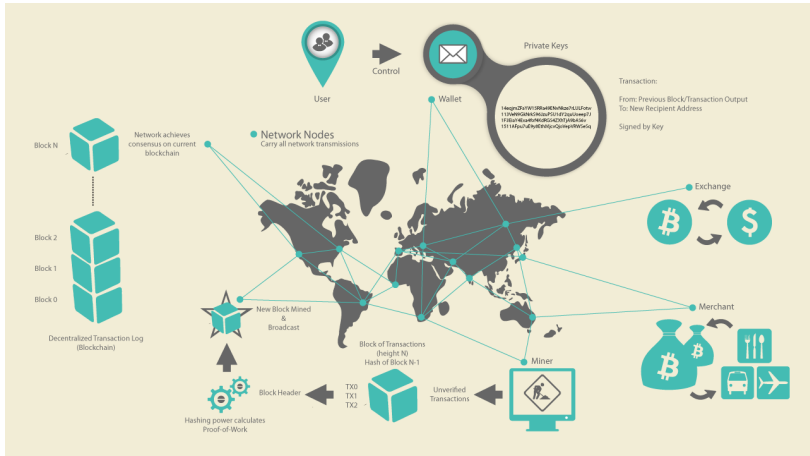
# The Currency

## 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 Shostak and Leslie Lamport, The Byzantine Generals Problem





# A Paper Wallet

Vires in numeris

## Private Key

BIP38 Encrypted



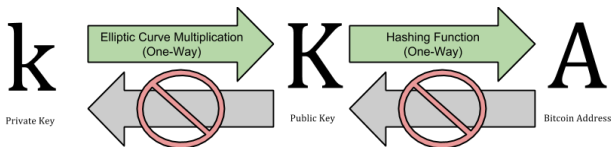
6PRNsJqabLoT73aWNWfSa3hMcX6ML  
mx779TPHbKzht4apwqsngkwFcBuKQ

## Bitcoin Address



1fbk5AYjA7wLdwbru2CunWEuToBu1USsX

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



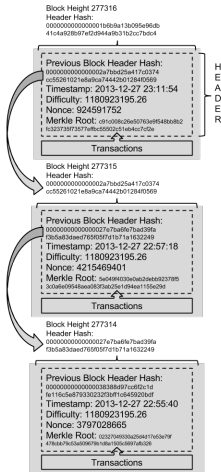
Elliptic Curve Digital Signature Algorithm – secp256k1

Hash = RIPEMD160(SHA256(pubkey))



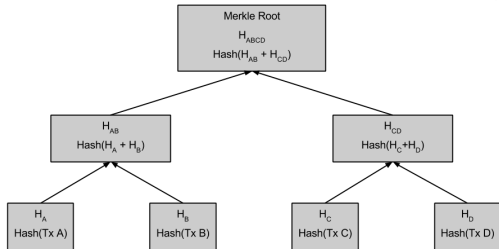
# Chain of Blocks

## A Distributed Ledger



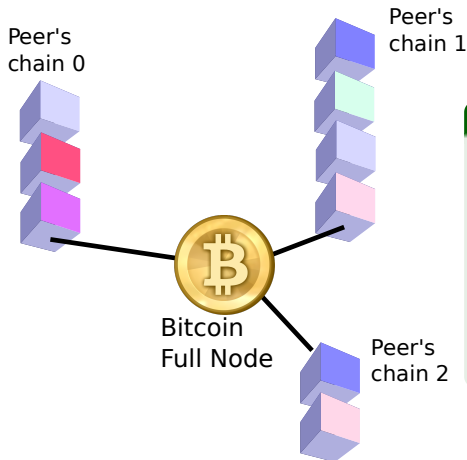
### Secure Hash Algorithm – SHA256

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  $\text{SHA256}(\text{SHA256}(\text{block header}) + \text{nonce}) < \text{target}$  ?
- 2 The Bitcoin Network will rewards me (25 BTC)

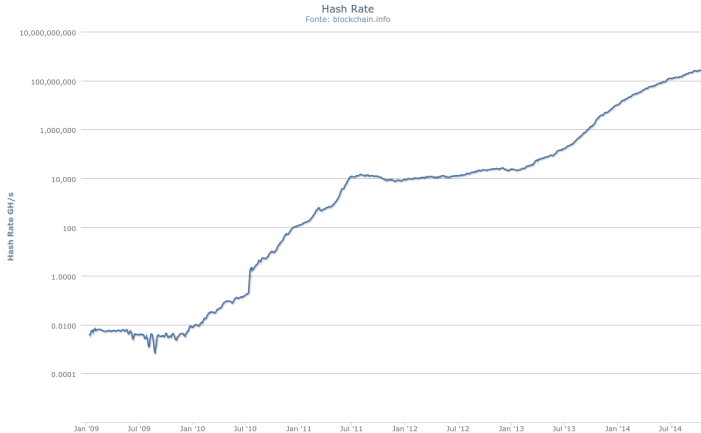
Difficulty ("inverse" of target) will adapt to global hashrate every  $\sim 2$  weeks (2016 blocks)





# Historical 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."*

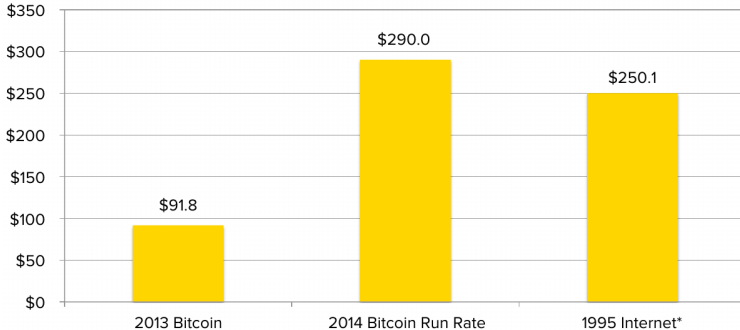
— Paul Robin Krugman – Nobel Memorial Prize in Economic Sciences (1998)



# What is happening?

## Status of Venture Capitals

Bitcoin vs Early Internet VC Investment (millions)



\*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](#)



# Usage Metrics

Latest quarter

	Quarterly			Last 12 Months	
	Sep-14	Jun-14	Q/Q Δ	Sep-13	Δ
<b>Commerce</b>					
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
<b>Industry</b>					
All-time VC investment (\$m)	317.0*	225.3	41%	30.4	10x
Number of VC-backed startups	66*	50	32%	14	5x
<b>Media</b>					
Mainstream media mentions	9,398	9,024	4%	1,794	5x
<b>Technology</b>					
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
<b>Valuation</b>					
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/>



# Crypto currencies

640 currencies should be enough for everyone

Currencies - Assets - All - EUR -					
#	Name	Market Cap	Price	Available Supply	Volume (24h)
1	 Bitcoin	€ 4.168.162.966	€ 311.35	13,387,225 BTC	€ 22.221.961
2	 Ripple	€ 110.681.882	€ 0.003818	28,989,252,282 XRP *	€ 194.176
3	 Litecoin	€ 105.133.859	€ 3.19	32,832,451 LTC	€ 3.966.589
4	 BitSharesX	€ 42.124.211	€ 0.021083	1,999,883,512 BTSX *	€ 180.969
5	 Dogecoin	€ 19.773.050	€ 0.000210	94,244,476,277 DOGE	€ 828.391
6	 Nxt	€ 19.128.976	€ 0.019129	999,997,096 NXT *	€ 65.025
7	 Peercoin	€ 18.198.085	€ 0.834301	21,812,384 PPC	€ 93.463
8	 Counterparty	€ 10.522.277	€ 3.97	2,647,485 XCP *	€ 12.598
9	 Namecoin	€ 8.398.133	€ 0.834142	10,066,000 NMC	€ 55.712
10	 Darkcoin	€ 7.825.255	€ 1.85	4,750,837 DRK	€ 76.044
11	 BitShares PTS	€ 3.929.134	€ 2.23	1,760,544 PTS	€ 17.594
12	 Monero	€ 3.263.531	€ 0.806039	4,048,849 XMR	€ 85.809
13	 BitcoinDark	€ 2.938.637	€ 2.47	1,187,858 BTCD	€ 22.983
14	 CannabCoin	€ 2.563.214	€ 0.027997	91,552,650 CANN	€ 172.939
15	 BlackCoin	€ 2.524.265	€ 0.033796	74,691,307 BC *	€ 21.669



# Bitcoin is difficult

Why FBK?

- ICT is about data, communication and technologies
- Money is Data, Data is Money (Big Data, Secure computing)
- Cryptography is hard
- Peer-to-peer is hard
- Enterprenuers need Technology partners



# What Next?

- FBKcoin – The “Kessler”®
- PATcoin – meal vouchers, *glocal* social credits
- Trentino as the new “Bitcoin Valley”
- Deep social and economic impact papers
- The Bitcoin Research Center
- ~~A new Research Unit~~

These slides

<http://goo.gl/BbzHTT> [github: mammadori]

