Bitcoin and Blockchain
An Introduction

April 9 2018, Fondazione Fiera Milano

ferdinando@ametrano.net

https://github.com/fametrano

https://twitter.com/Ferdinando1970

https://speakerdeck.com/nando1970

https://www.reddit.com/user/Nando1970/

https://www.slideshare.net/Ferdinando1970

https://it.linkedin.com/in/ferdinandoametrano

https://www.youtube.com/c/FerdinandoMAmetrano

Agenda

1. **Introduction**
2. How Does It Work? (i.e. the Double Spending Problem)
3. Bitcoin as Digital Gold
4. Bitcoin in The History of Money
5. Blockchain Beyond Bitcoin

Understanding Lags Well Behind the Hype

Understanding of the technology however lags well behind the hype, amongst practitioners, policy makers and industry commentators alike. <u>'Blockchain' technology seems to promise major change for capital markets and other financial services</u> – some say it may ultimately prove to be as important an innovation as the internet itself – <u>but few can say exactly how or why.</u>

Michael Mainelli, Alistair Milne (2016)
The Impact and Potential of Blockchain on the Securities Transaction Lifecycle
http://ssrn.com/abstract=2777404

Bitcoin Is Hard to Understand

At the crossroads of:

1. Cryptography
2. Distributed systems (networking and data transmission)
3. Game theory
4. Economic and monetary theory

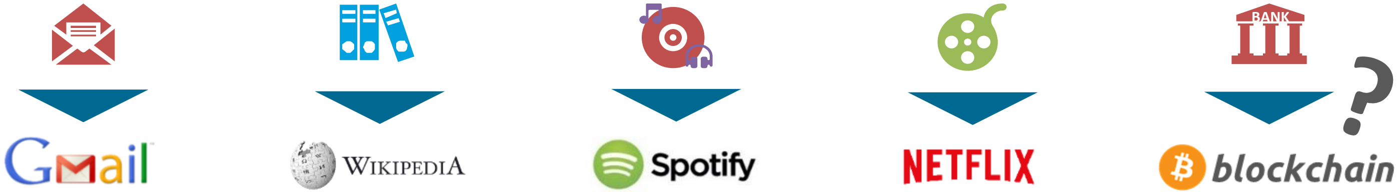
Mainly not a technology,
a cultural paradigm shift instead

bitcoin

- Decentralized digital currency
- Not backed by any government or organization
- No need for trusted third party
- Instantaneous peer-to-peer transactions
- Cryptographic security
- Synergic economic incentives
- Efficient low-cost banking for everybody everywhere

https://bitcoin.org/en/faq
http://www.coindesk.com/information/

The Information Economy



- Data is transferred with zero marginal cost
- Why pay a fee to move bytes representing wealth?
- Why only 9-5, Monday-Friday, two days settlement?
- Who (and when) will gift humanity with a global instantaneous free p2p payment network?

bitcoin

- Decentralized: no central authority, no intermediaries
- Permissionless: no regulator
- Censorship resistant: no frozen funds
- Open-access: no discrimination, no amount limits, 24/7, 365 days
- Free: negligible transaction costs
- Borderless: no geographic limits
- Transnational: no specific jurisdiction applies
- Secure: non falsifiable, non repudiable transactions
- Resilient: nothing has been able to stop it or break it

Agenda

1. Introduction
2. **How Does It Work? (i.e. the Double Spending Problem)**
3. Bitcoin as Digital Gold
4. Bitcoin in The History of Money
5. Blockchain Beyond Bitcoin

Double Spending Problem

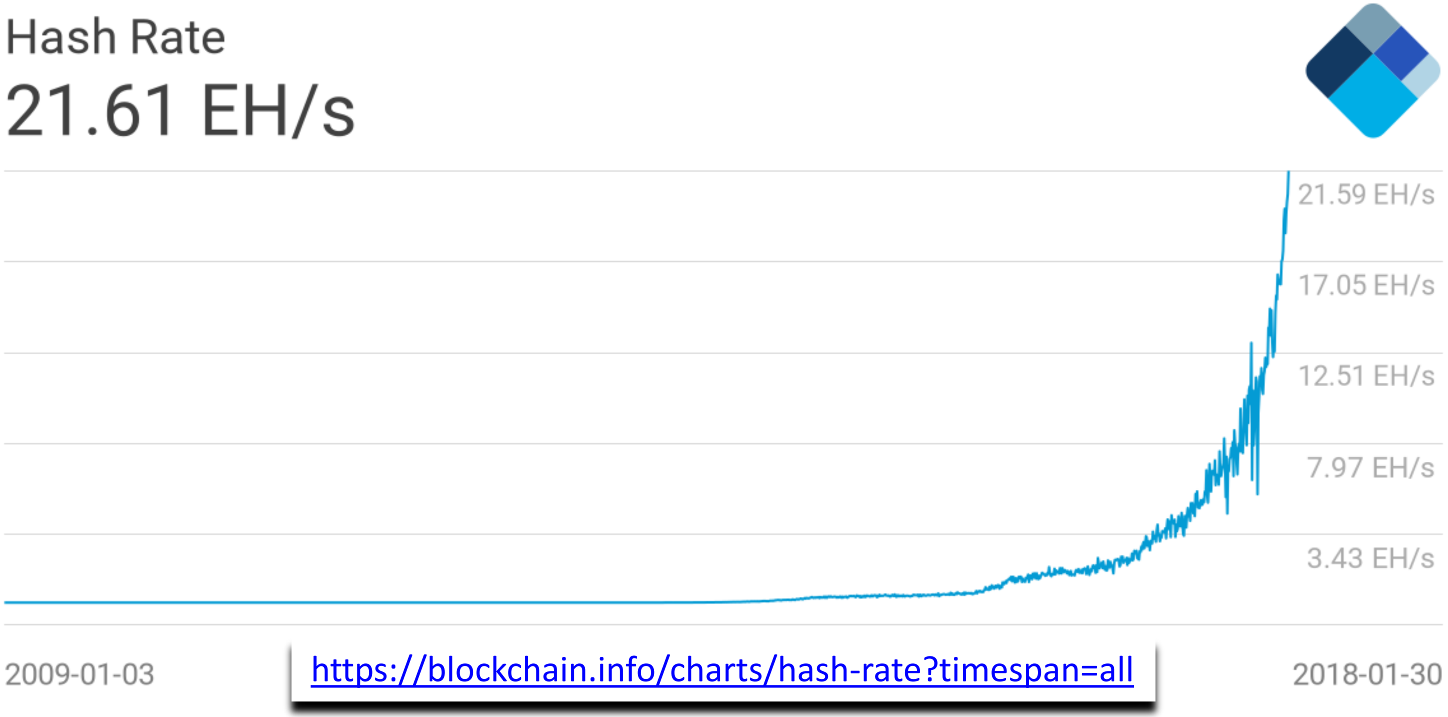
- To securely transfer value using digital means has been possible for decades
- In digital cash schemes, a single digital token, being just a file that can be duplicated, can be spent twice
- A centralized trusted party has always been required to prevent ***double spending***

Mining

- All network nodes validate all transactions; those also providing the computational power for clearing and settlement are called miners
- Miners compete to validate a new block of transactions: the winner providing *proof-of-work* is rewarded with the issue of new bitcoins in a special *coinbase* transaction included in the block
- *Proof-of-work* mining solves the double spending problem:
  - conflicting transactions spending the same coins would invalidate the block
  - an invalid block would be rejected from the network
  - the bitcoin reward would be removed from transaction history
  - miner would have wasted his work

Network Hashing Power

- 100,000s times more powerful than the world top 500 supercomputers
- To manipolate blocks 51% of the Hash Rate is required

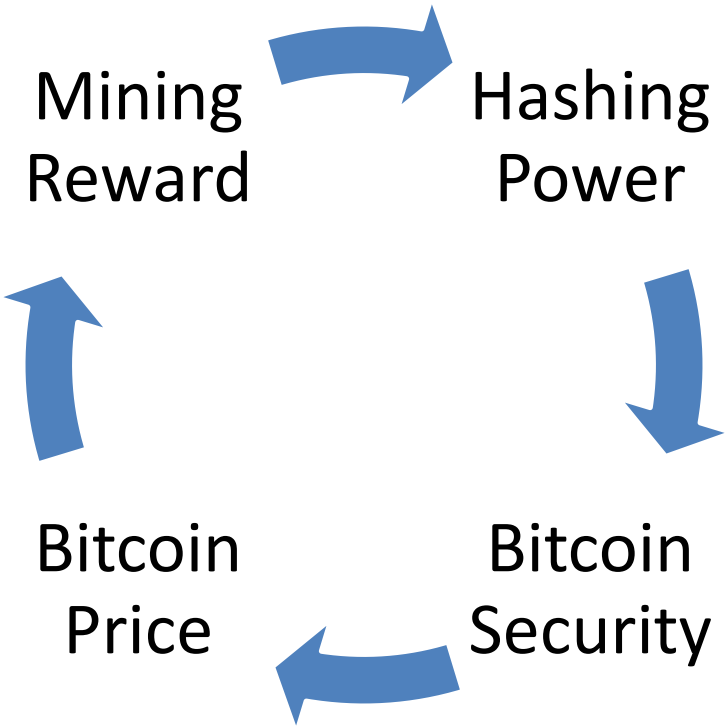


https://blockchain.info/charts/hash-rate?timespan=all

Nakamoto Consensus

- Nakamoto achieves Practical Byzantine Fault Tolerant (PBFT) *distributed consensus* using *(game theory) economic incentive* for the mining nodes to be honest.
- Bitcoin solves double spending without a central trusted party
- Bitcoin can resist attacks of malicious agents, as long as they do not control network majority
- Miners are compensated for their *proof-of-work* using seigniorage revenues, i.e. with issuance of new bitcoins
- Seigniorage revenues subsidize the network, covering consensus costs and making transactions cheap

Virtuous Cycle



Mining Reward

Hashing Power

Bitcoin Security

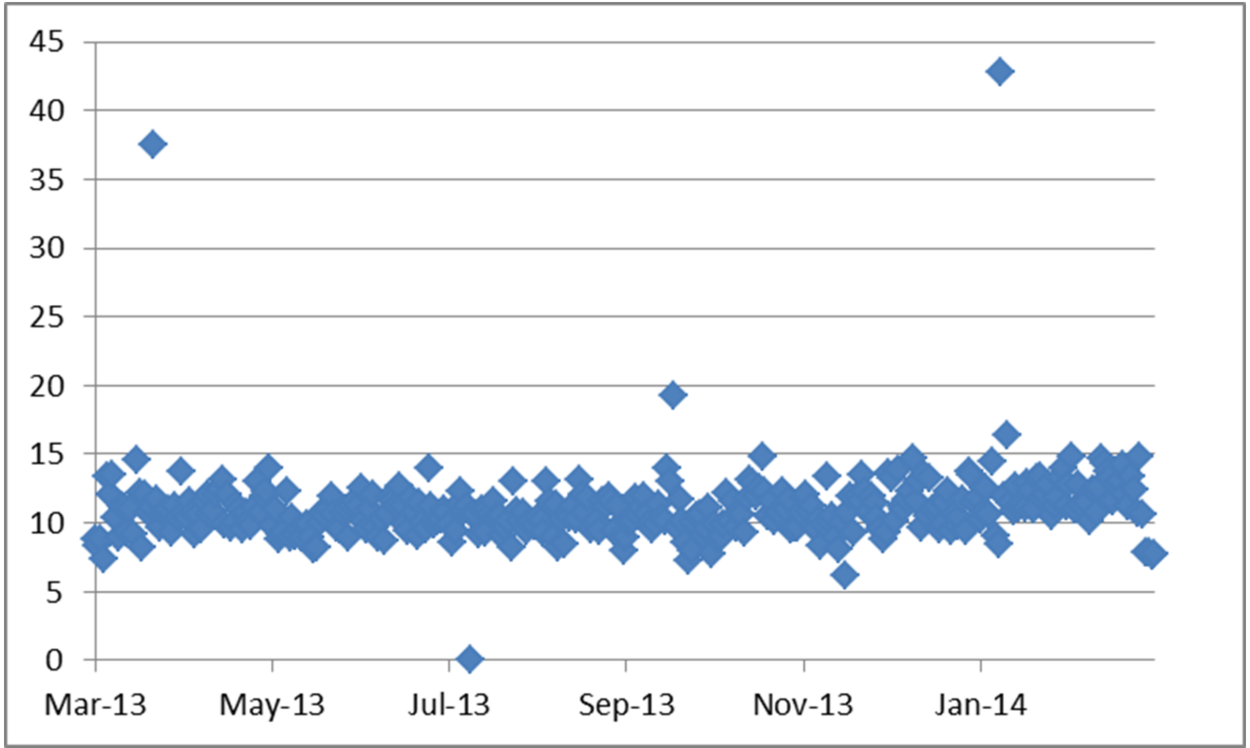
Bitcoin Price

Agenda

1. Introduction
2. How Does It Work? (i.e. the Double Spending Problem)
3. **Bitcoin as Digital Gold**
4. Bitcoin in The History of Money
5. Blockchain Beyond Bitcoin

Validation Process: Block Generation

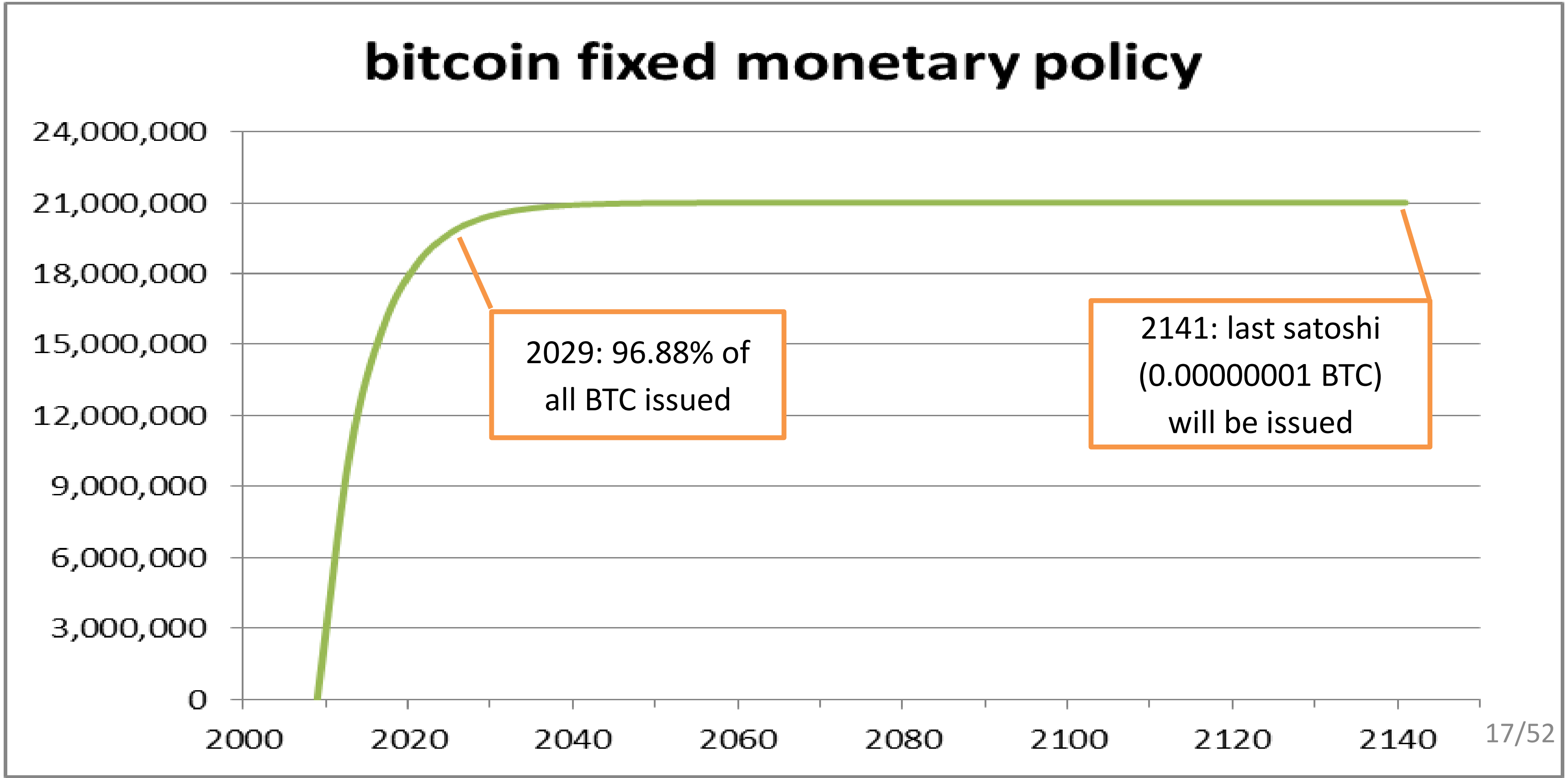
Proof-of-work difficulty is adapted (every 2016 blocks) to the overall available computing power to ensure an average of one block every ten minutes



Bitcoin Monetary Rule

- 2009: 50BTC per block, every 10 minutes
  - halving every 4Y
- This is the only way new bitcoins are released
- It is called mining because of its similarity with the progressive scarcity of gold extraction
- Supply free of discretionary intervention

Bitcoin Inelastic Supply: Deterministic Decreasing Rate



2029: 96.88% of all BTC issued

2141: last satoshi (0.00000001 BTC) will be issued

What Makes Bitcoin Special?

- Digital and scriptural: it only exists as validated transaction
- Asset, not liability
- Bearer instrument
- It can be transferred but not duplicated

  (i.e. it can be spent, but not double-spent)
- Scarce in digital realm, as nothing else before
- Mimicking gold monetary policy

Bitcoin is digital gold

this is the groundbreaking achievement by Satoshi Nakamoto

- More a crypto-commodity then a crypto-currency

Bitcoin Relevance

If one thinks about the role of physical gold in the history of civilization, money, and finance

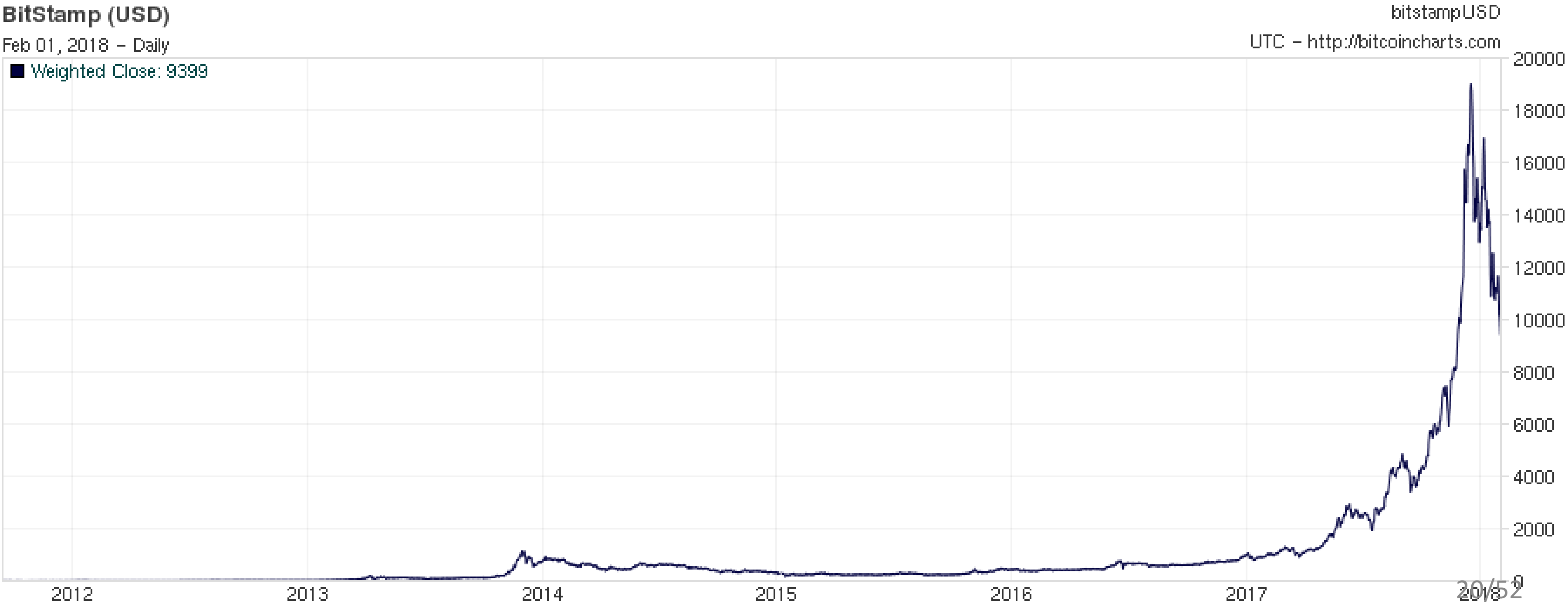
the digital equivalent of gold could be disruptive

in the current digital civilization and the future of money and finance

BTC/USD Exchange Rate

http://bitcoincharts.com/charts/bitstampUSD#tgWzm1g10zm2g25

- BTC Market Cap: about $150B (USD M0 1959-2017 average has been $680B)



Risk Measures

- Price dynamic is the discovery process of value, the value of digital gold being hard to grasp
- High return (x10,000 in 7 years) → high risks

Daily Returns, July 2010 – October 2017

	BITCOIN	GRAIN	WTI	IND.METALS	GOLD	MSCI BRIC	EUROSTOXX50	S&P500
	XBT Curncy	SPGSGRP Index	CLA Comdty	SPGSINP Index	XAU Curncy	MXBRIC Index	SX5EWK Index	SPX Index
Mean	0,83%	-0,02%	-0,03%	0,00%	0,01%	0,00%	0,01%	0,04%
Standard deviation	6,99%	1,41%	1,29%	1,24%	1,02%	1,12%	1,57%	0,92%
Volatility	133,61%	26,87%	24,67%	23,60%	19,44%	21,47%	29,97%	17,62%
Skewness	123,36%	20,68%	3,89%	-13,38%	-58,48%	-26,23%	-3,53%	-37,00%
Excess kurtosis	1482,10%	245,42%	421,23%	240,23%	566,63%	252,24%	522,26%	478,54%
Minimum return	-45,17%	-5,88%	-6,86%	-6,49%	-8,97%	-6,69%	-11,02%	-6,66%
Maximum return	67,71%	7,35%	7,17%	5,69%	5,20%	4,87%	11,81%	4,74%
Value-at-Risk at 99% confidence	17,27%	3,69%	3,46%	3,19%	2,83%	3,20%	4,39%	2,67%
Expected Shortfall at 99% confidence	25,99%	4,80%	4,66%	4,36%	3,95%	3,97%	5,67%	3,60%
Worst Absolute Drowdown	-93,07%	-61,27%	-59,51%	-57,82%	-44,58%	-51,05%	-44,33%	-19,39%

A New Uncorrelated Asset Class

Field = Last Price, Data Type = Pct Chg (1D), Log Type = None, Periodicity = 1D, Currency = Dflt,
Start Date = 24/07/2010, End Date = 13/10/2017

	BITCOIN	GRAIN	WTI	IND.METALS	GOLD	MSCI BRIC	EUROSTOXX50	S&P500
	XBT Curncy	SPGSGRP Index	CLA Comdty	SPGSINP Index	XAU Curncy	MXBRIC Index	SX5EWK Index	SPX Index
XBT Curncy	100%	4%	1%	4%	0%	1%	5%	4%
SPGSGRP Index	4%	100%	19%	22%	14%	16%	15%	16%
CL1 Comdty	1%	19%	100%	37%	15%	31%	31%	36%
SPGSINP Index	4%	22%	37%	100%	32%	44%	48%	37%
XAU Curncy	0%	14%	15%	32%	100%	12%	9%	-1%
MXBRIC Index	1%	16%	31%	44%	12%	100%	58%	49%
SX5EWK Index	5%	15%	31%	48%	9%	58%	100%	63%
SPX Index	4%	16%	36%	37%	-1%	49%	63%	100%

Bitcoin Potential Upside

- Asset Under Management, Worldwide: $100T
  - If 2% is invested in BTC, price should be $100,000
- Gold capitalization: $8T
  - if BTC reaches a similar level, its price should be $400,000
- Metcalfe's law: the value of a network is proportional to the square of the number of users
  - Estimated BTC investors is about 50 millions; with a forecast to 350 millions price might increase x49

Agenda

1. Introduction
2. How Does It Work? (i.e. the Double Spending Problem)
3. Bitcoin as Digital Gold
4. **Bitcoin in The History of Money**
5. Blockchain Beyond Bitcoin

Money As A Social Relation Instrument

1. Human beings are born into a gift economy
2. Enlarged relationship circle requires exchange economy
3. Barter economy: coincidence of wants
4. Trade economy: money as medium of exchange
5. Global information economy: supranational digital money

Friedrich August von Hayek Denationalisation of Money

- history of coinage is an almost uninterrupted story of debasements; history is largely a history of inflation engineered by governments for their gain
- why government monopoly of the provision of money is regarded as indispensable? It deprived public of the opportunity to discover and use a better reliable money

Blessed will be the day when it will no longer be from the benevolence of the government that we expect good money but from the regard of the banks for their own interest

A Free-Market Monetary System, Gold and Monetary Conference, New Orleans, Nov. 1977, https://mises.org/daily/3204

Hayek, F. A., Denationalisation of Money, The Institute of Economic Affairs, http://www.mises.org/books/denationalisation.pdf

Permissionless Innovation
Fast and Effective

- No centralized security mechanism, no barrier to enter, no editorial control
    - Email has not been designed by a consortium of postal agencies
    - Internet has not been developed by a consortium of telcos

- Will a decentralized transactional economy be shaped by a consortium of banks?

Trade Economy
From Gold Standard to Fiat Money

- Gold: the commodity money standard
  - scarce
  - pleasant color, i.e. resistant to corrosion and oxidation
  - high malleability
  - relative easiness of its purity assessment
- Gold purity certification
- Representative money
- Fractional receipt money
- *Fiat* money and legal tender

Explain Money to an Alien

***fiat* money**

- No intrinsic value (legal tender, social contract)
- Currency based on paper/ink security
- Discretionary governance
- Wicksellian interest-rate approach

bitcoin

- No intrinsic value (digital gold)
- Currency based on math/cryptographic security
- Algorithmic governance
- Deterministic supply

Unit of Account: Money as Numeraire

- Money is the unit of account against which the value of every other good is measured
- The price system measures the value of goods relative to the value of money

Good money should provide stable prices to best perform its role as unit of account

Money Comparison

	Medium of Exchange	*Store of ~~Constant~~ Value*	*Unit of Account*
Live cattle	★	★	★
Diamonds	★	★★★★	★★★
Gold	★★★	★★★★	★★★
Fiat coins and notes	★★★★	★★★★	★★★★
Bitcoin	★★★★★	★★★★ ?	★★

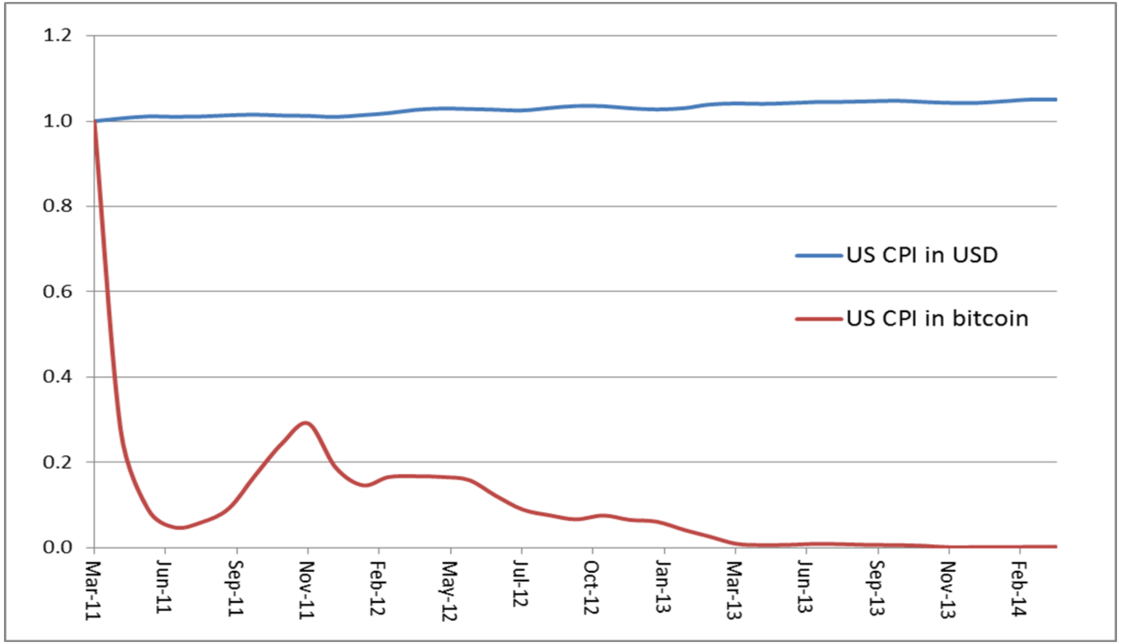
- swappable
- fungible
- portable
- divisible
- recognizable
- resistant to counterfeiting

- reliably saved, stored, and retrieved
- retain usefulness over time
- Maintain its storage properties
- non-perishable or with low preservation cost

- relative worth unit of measure
- stable value for stable price comparison
- supply must be controlled in some way

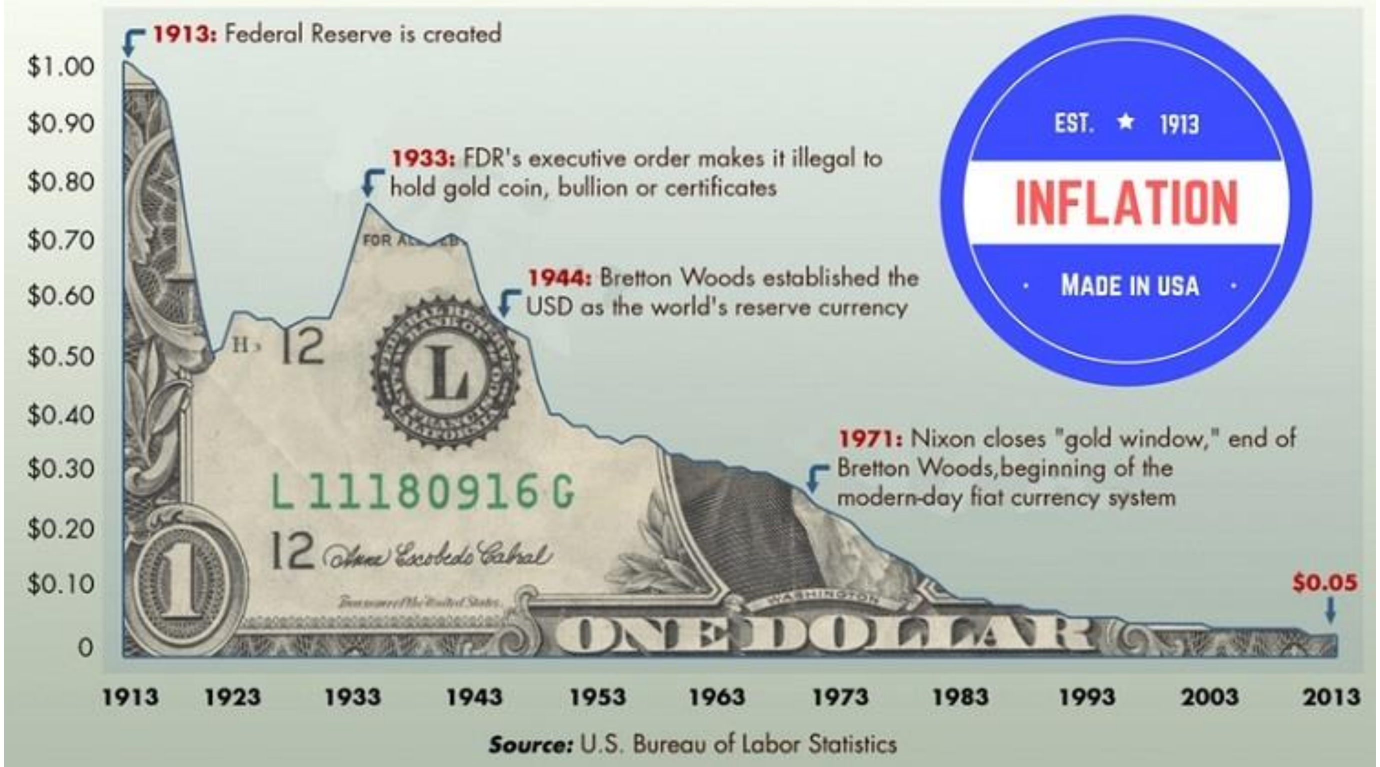
Bitcoin is Digital Gold
Not a Good Unit of Account

- no salaries, no mortgages, no stable purchasing power
- *successful at getting rid of a centralized monetary authority, it has given up the flexibility of an elastic supply of money*



There Are Worse Situations…

Since the establishment of Federal Reserve in 1913 the US dollar has lost 96% of purchasing power



1913: Federal Reserve is created

1933: FDR's executive order makes it illegal to hold gold coin, bullion or certificates

1944: Bretton Woods established the USD as the world's reserve currency

1971: Nixon closes "gold window," end of Bretton Woods, beginning of the modern-day fiat currency system

Source: U.S. Bureau of Labor Statistics

Bitcoin as (Digital) Gold in the History of (Crypto)Money

gold

- Its adoption was not centrally planned
- For centuries it has been the most successful form of money
- It has bootstrapped all monetary systems we know of
- It has been surpassed by other kind of money without becoming obsolete

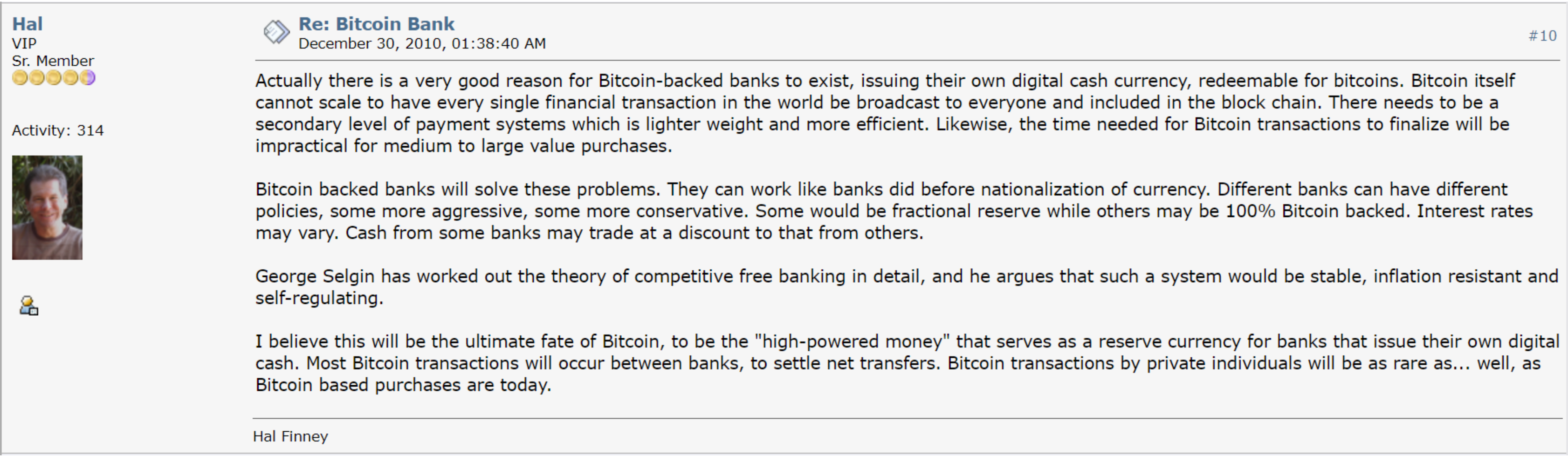
bitcoin

- Its adoption has not been centrally planned
- It is the most successful form of cryptocurrency
- It will bootstrap new monetary systems
- It might be surpassed by more advanced type of cryptocurrencies without becoming obsolete

Hayek Money: A New Generation of Cryptocurrencies

- The cryptocurrency monetary standard of **elastic non-discretionary** supply
- Price stability paradigm with respect to a given reference basket
- Concurrent cryptocurrencies will compete in monetary policy definition and reference basket choices

The Ultimate Fate of Bitcoin:
To Serve as a Reserve Currency



Hal
VIP
Sr. Member

Activity: 314

Re: Bitcoin Bank
December 30, 2010, 01:38:40 AM

#10

Actually there is a very good reason for Bitcoin-backed banks to exist, issuing their own digital cash currency, redeemable for bitcoins. Bitcoin itself cannot scale to have every single financial transaction in the world be broadcast to everyone and included in the block chain. There needs to be a secondary level of payment systems which is lighter weight and more efficient. Likewise, the time needed for Bitcoin transactions to finalize will be impractical for medium to large value purchases.

Bitcoin backed banks will solve these problems. They can work like banks did before nationalization of currency. Different banks can have different policies, some more aggressive, some more conservative. Some would be fractional reserve while others may be 100% Bitcoin backed. Interest rates may vary. Cash from some banks may trade at a discount to that from others.

George Selgin has worked out the theory of competitive free banking in detail, and he argues that such a system would be stable, inflation resistant and self-regulating.

I believe this will be the ultimate fate of Bitcoin, to be the "high-powered money" that serves as a reserve currency for banks that issue their own digital cash. Most Bitcoin transactions will occur between banks, to settle net transfers. Bitcoin transactions by private individuals will be as rare as... well, as Bitcoin based purchases are today.

Hal Finney

https://bitcointalk.org/index.php?topic=2500.msg34211#msg34211

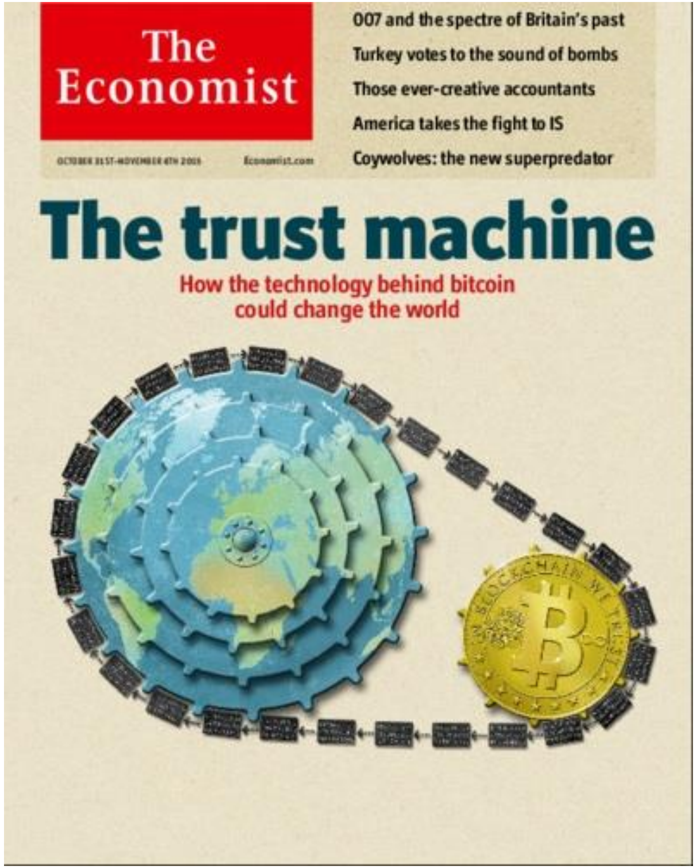
Hal Finney (1956–2014) was a noted cryptographic activist. He was the second PGP Corporation developer hired after Phil Zimmermann. He created the first reusable proof-of-work. He was an early bitcoin user and received the first bitcoin transaction from bitcoin's creator Satoshi Nakamoto.

Agenda

1. Introduction
2. How Does It Work? (i.e. the Double Spending Problem)
3. Bitcoin as Digital Gold
4. Bitcoin in The History of Money
5. **Blockchain Beyond Bitcoin**

Really?

“Blockchain – not bitcoin – will prove revolutionary in banking”



The Economist

OCTOBER 31ST–NOVEMBER 6TH 2015 Economist.com

007 and the spectre of Britain's past

Turkey votes to the sound of bombs

Those ever-creative accountants

America takes the fight to IS

Coywolves: the new superpredator

The trust machine

How the technology behind bitcoin could change the world

http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

A Dramatic Misunderstanding

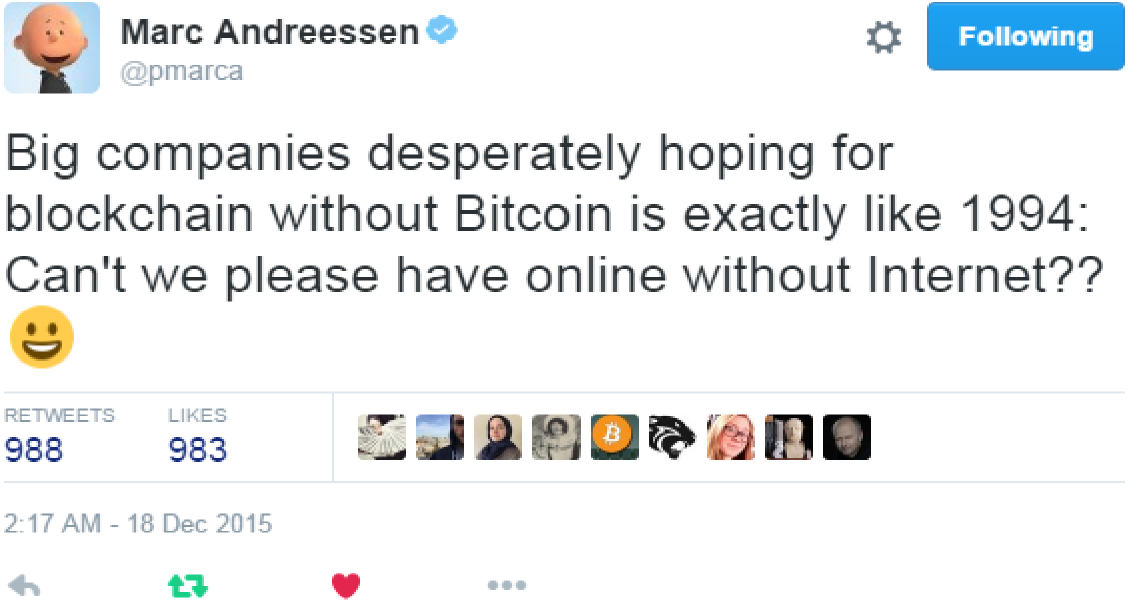
*“When a wise man points at the **moon** the fool examines the **finger**.”* (Confucius)

*“When a wise man points at the **bitcoin** the fool examines the **blockchain**.”* (Ametrano)

Bitcoin in 2014 Is Like Internet in 1994: Weird and Scary

Marc Andreessen: American entrepreneur, investor, and software engineer. Coauthor of Mosaic, cofounder of Netscape

https://twitter.com/pmarca/status/677658844504436737



Marc Andreessen
@pmarca

Big companies desperately hoping for blockchain without Bitcoin is exactly like 1994: Can't we please have online without Internet?? 😃

RETWEETS 988

LIKES 983

2:17 AM - 18 Dec 2015

The Walled Garden Model

- Controlled access to web content and services
- Offered in the late ‘90s and early ‘00s by Compuserve, AOL (and to some extent MSN)
- Corporates wanted to go online, but not in the wild unregulated internet, populated by anonymous agents
- They eventually realized that perceived risks, which are real, are outweighed by benefits

What is The Blockchain?

[A hash pointer linked list of blocks]

- An append-only sequential data structure
- New blocks can only be appended at the end of the chain
- To change a block in the middle of the chain, all subsequent blocks need to be changed
- <u>Very inefficient compared to a relational database</u>

Blockchain Without Bitcoin

Does it make sense?

No bitcoin

➡ No asset available to reward miners

➡ Appointed validator officials required

Central governance is required!

Why should validators use a blockchain,

i.e. a subpar data structure, instead of a database?

Blockchain Needs A Native Digital Asset

https://www.finextra.com/videoarticle/1241/blockchain-needs-a-native-digital-asset

Blockchain needs a native digital asset

01 June 2016 | 16619 views

Ferdinando Ametrano, Head of Blockchain and Virtual Currencies, Intesa Sanpaolo, discusses the relationship between bitcoin and blockchain, and outlines how banks can stay ahead of this evolving landscape.

Radioactive fallout

In the nuclear explosion of bitcoin, applied cryptography is the radioactive fallout

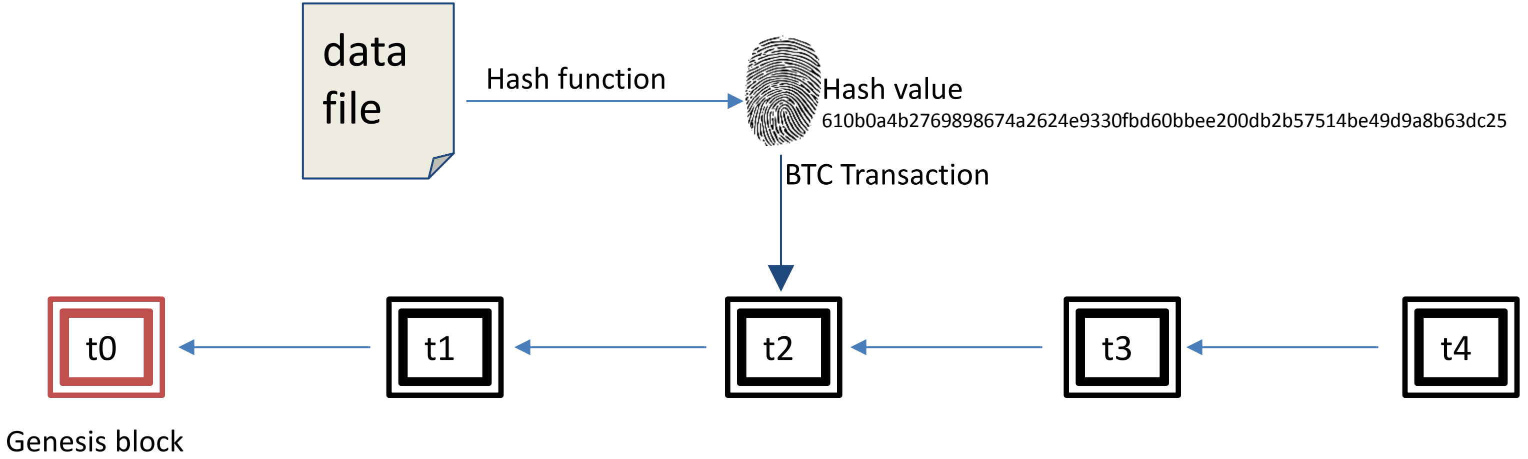
It can be used to harden existing business processes

Databases on cryptographic steroids

Evolutionary, non-disruptive, technology

Blockchain Beyond Bitcoin: Blockchain Timestamping

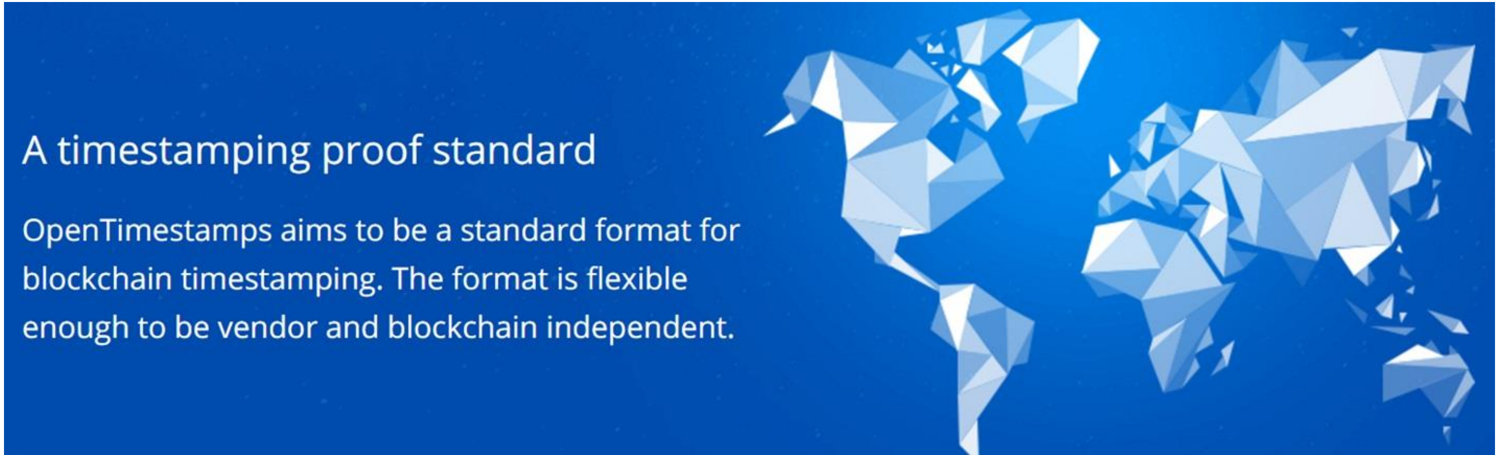
- A generic data file can be hashed to producing a short unique identifier, equivalent to its digital fingerprint
- Such a fingerprint can be associated to a bitcoin transaction (irrelevant amount) and hence registered on the blockchain
- Blockchain immutability provides time-stamping, proving data the file existence at that moment in time in that specific status



Time-stamping is Notarization

- An unlimited number of documents can be timestamped with a single transaction
- Calendar services can provide (Merkle Tree) aggregation and attestation
- The process has been standardized to allow for third party auditability
- Suitable for regulatory prescriptions

OPEN timestamps



A timestamping proof standard

OpenTimestamps aims to be a standard format for blockchain timestamping. The format is flexible enough to be vendor and blockchain independent.

Anchoring: A New Security Paradigm

- Bitcoin blockchain network security is preserved by a computation power unparalleled in human history
- Other transactional networks can tap into this security via *anchoring* (i.e. periodic time-stamping of the network status)
- Any *“stateful system with global memory”* can outsource its security to the bitcoin network, piggybacking its resilience
- Bitcoin seigniorage revenues might provide security for all transactional networks
- Miners as global outsourced decentralized security

Digital Gold Jewelry

What jewelry is for gold,
notarization could be for bitcoin:

not essential
but effective at leveraging its beauty

Bibliography

- Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008) https://bitcoin.org/bitcoin.pdf
- *Hayek Money: the Cryptocurrency Price Stability Solution (2014),* http://ssrn.com/abstract=2425270
- *Blockchain and Distributed Ledger Technology: Hype or Reality?* (2017) https://ssrn.com/abstract=2832249
- Saifedean Ammous, *The Bitcoin Standard: The Decentralized Alternative to Central Banking* (2018)
- *Bitcoin as Digital Gold* (2018), United Nations Department of Economic and Social Affairs; video: https://goo.gl/NkEC9w; slides: https://goo.gl/szzBXh
- *Bitcoin*, YouTube videos, https://goo.gl/qDvKXi

Bibliography (ITA)

- Intervista (“Le Iene”, Mediaset), http://bit.ly/2H2qwqf
- *Bitcoin*, YouTube videos, https://goo.gl/byVNqP
- *Bitcoin & Blockchain Technology course*, University Course Video, https://goo.gl/kNCK3E
- *Il Far West dell’oro digitale* (IlSole24Ore 2017), http://bit.ly/2qjpvzr
- Intervista *Bitcoin: oro digitale, finanza e tulipani* (2018), https://goo.gl/eyjDJ2

Takeaways

Thank You

1. Bitcoin is hard to understand: it is not a technology, a cultural paradigm shift instead
2. Bitcoin solves the double spending problem (distributed consensus), allowing for the decentralization paradigm
3. Bitcoin is digital gold:
   - could be as relevant as physical gold for the history of our civilization and the future of money & finance
   - a new asset class with no correlation with other asset classes: investing in bitcoin is rational diversification
4. Bitcoin is bootstrapping new monetary systems
5. There is no blockchain without bitcoin, but there is a blockchain beyond bitcoin: notarization and anchoring