ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI
MILANO

FONDAZIONE COMMERCIALISTI ODCEC di MILANO

Macro-Micro: La Congiuntura Economica / Blockchain e Mercati

Bitcoin and Blockchain Technology: A Quick Introduction

Ferdinando M. Ametrano
https://www.ametrano.net/about

CERIF ASSOCIAZIONE CENTRO DI RICERCA SULLE IMPRESE DI FAMIGLIA

28 Novembre 2018, Milano

Bitcoin (and Blockchain): Hard to Understand

At the crossroads of:
Cryptography
Computer networking and distributed systems
Game theory
Monetary theory

Mainly not a technology,
a <u>cultural paradigm shift</u> instead

Table of Contents

1. **Internet Money**
2. The Double Spending Problem
3. Bitcoin as Digital Gold
4. Blockchain Beyond Bitcoin: Notarization
5. Bitcoin as Investment Asset

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?

Reliable E-Cash Will Be Developed on the Internet

The one thing that's missing, but that'll soon be developed, is a reliable e-cash, a method whereby on the internet you can transfer funds from A to B, without A knowing B or B knowing A, the way I can take a 20 Dollar bill and hand it over to you...

Milton Friedman, 1999

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

Permissionless Innovation: Gentle, 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 new money and its decentralized transactional network be designed by a consortium of banks?

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

Take Money out of the Hands of Government

I don't believe we shall ever have a good money again before we take the thing out of the hands of government, that is, we can't take them violently out of the hands of government, all we can do is by some sly roundabout way introduce something that they can't stop.

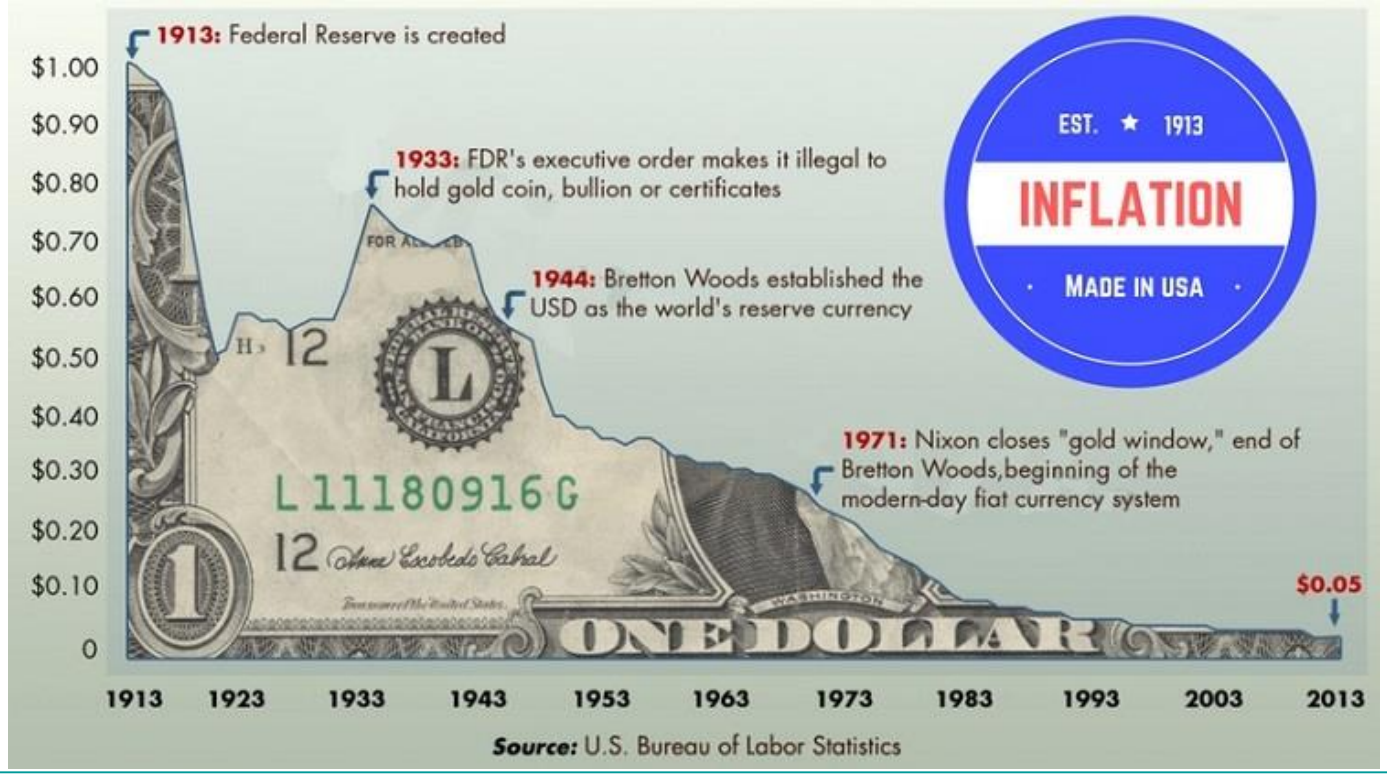
F. A. Hayek

https://youtu.be/EYhEDxFwFRU?t=19m23s

© Ferdinando Ametrano 2018

USD Purchasing Power

has lost 96% since the establishment of Federal Reserve in 1913



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

©2018 Ferdinando Ametrano 2018

Table of Contents

1. Internet Money
2. **The Double Spending Problem**
3. Bitcoin as Digital Gold
4. Blockchain Beyond Bitcoin: Notarization
5. Bitcoin as Investment Asset

The 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***

© Ferdinando Ametrano 2018

Bitcoin Network: A Distributed Back-office

All network nodes validate and clear all transactions

Mining nodes provide also the additional computational power required for settlement

Without a central trusted party, how do they reach consensus on the transaction history?

Consensus in a distributed network with faulty (or malicious) nodes is a very hard problem

Mining

Miners compete to validate a new block of transactions

The winner providing *proof-of-work* for the finalization of a new block is rewarded with the issuance of new bitcoins in a special *coinbase* transaction included in that same block

Miners solve the double spending problem:

- 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
- The winning miner would have wasted his work

Nakamoto Distributed Consensus

Practical Byzantine Fault Tolerant (PBFT) *distributed consensus* is achieved using *(game theory) economic incentive* for the mining nodes to be honest

Double spending is solved without a central trusted party

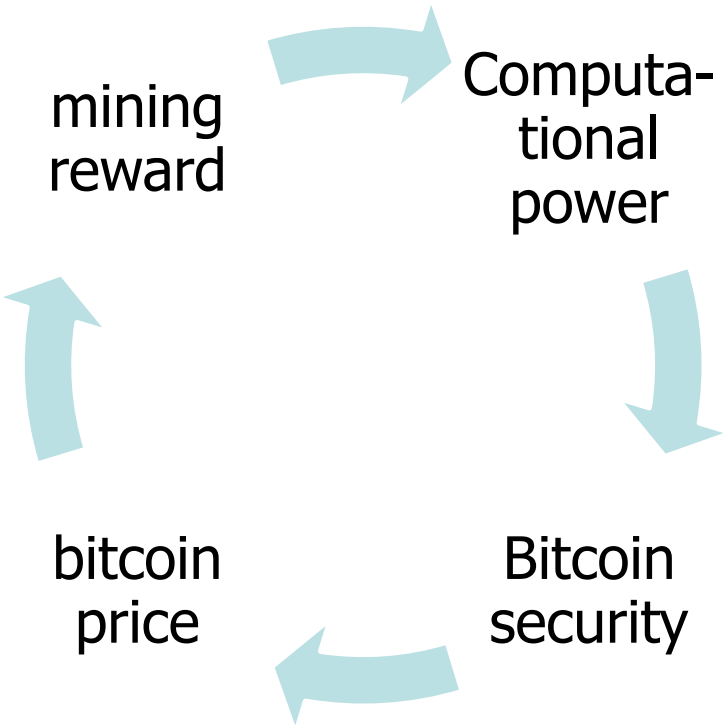
Bitcoin can resist attacks of malicious agents, as long as they do not control network majority

Miners are compensated for their *proof-of-work* using seigniorage revenues, i.e. with issuance of new bitcoins

Seigniorage revenues subsidize the network

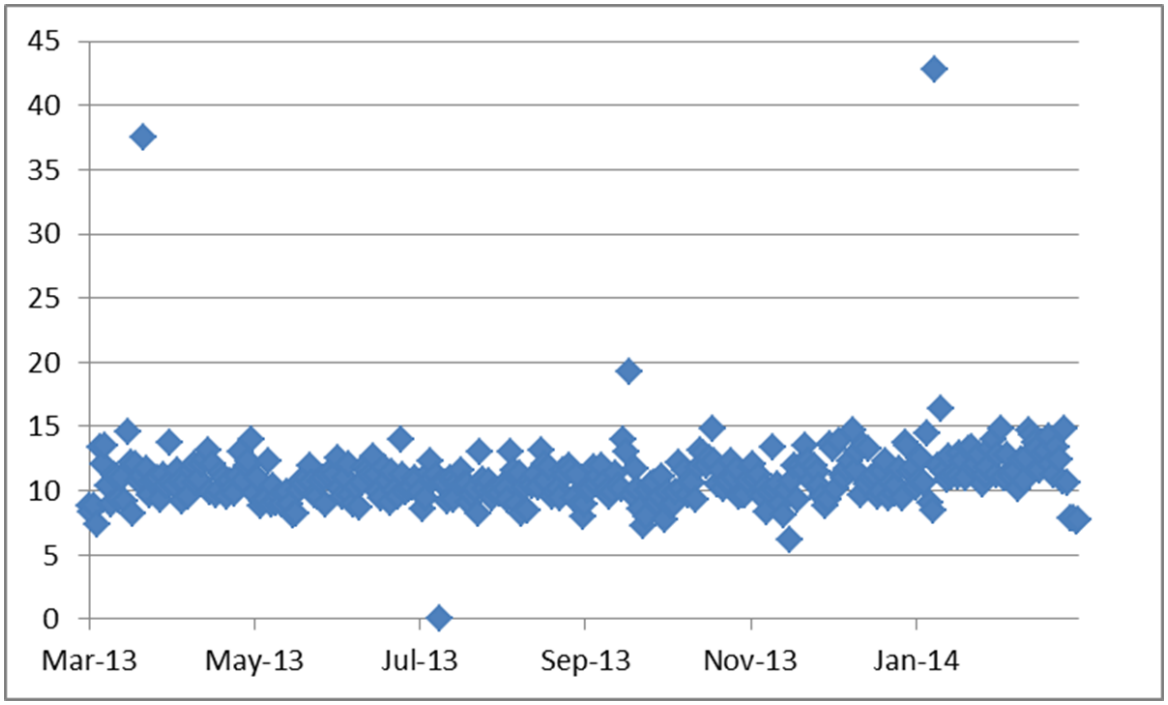
© Ferdinando Ametrano 2018

Virtuous Cycle



Validation Process: Block Generation

The proof-of-work *difficulty* is adapted to the overall available computing power to ensure an average of one block every ten minutes



©Ferdinando Ametrano 2018

Table of Contents

1. Internet Money
2. The Double Spending Problem
3. **Bitcoin as Digital Gold**
4. Blockchain Beyond Bitcoin: Notarization
5. Bitcoin as Investment Asset

Bitcoin Monetary Rule

2009: 50BTC per block, every 10 minutes

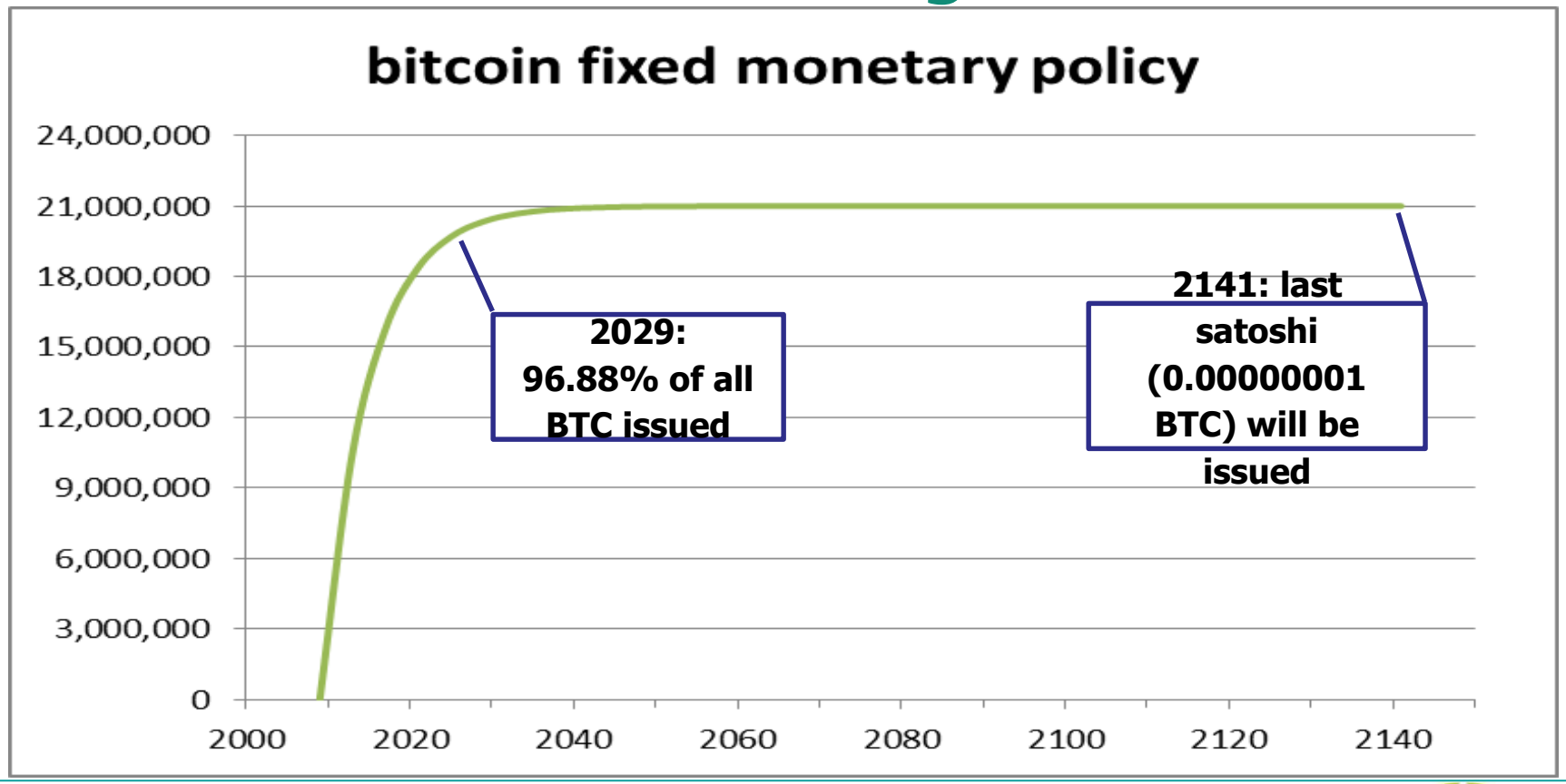
- halving every 4Y

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



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

It mimics gold monetary policy

What Makes Bitcoin Special?

Bitcoin is digital gold

with a secure uncensorable embedded

settlement network

More a crypto-commodity then a crypto-currency

This is the groundbreaking achievement by Satoshi Nakamoto, not blockchain "technology"

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

Bitcoin can be the new global reserve asset

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

gold	bitcoin
Its adoption was not centrally planned	Its adoption has not been centrally planned
For centuries it has been the most successful form of money	It is the most successful form of cryptocurrency
It has bootstrapped all monetary systems we know of	It will bootstrap new monetary systems
It has been surpassed by other kind of money without becoming obsolete	It might be surpassed by more advanced type of cryptocurrencies without becoming obsolete

Gold Is Not Loved

1933 Gold Act "forbidding the hoarding of gold coin, gold bullion, and gold certificates within the continental United States".

1966 Greenspan: “This is the shabby secret of the welfare statists' tirades against gold. Deficit spending is simply a scheme for the confiscation of wealth. Gold stands in the way of this insidious process. It stands as a protector of property rights. If one grasps this, one has no difficulty in understanding the statists' antagonism toward the gold standard.”

1972 Nixon shock: unilateral cancellation of the convertibility of the United States dollar to gold.

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

Hayek Money:
A New Generation of Cryptocurrencies

The cryptocurrency monetary standard of **elastic <u>non-discretionary</u>** supply

Price stability paradigm with respect to a given reference basket

Concurrent cryptocurrencies will compete in monetary policy definition and reference basket choices

Table of Contents

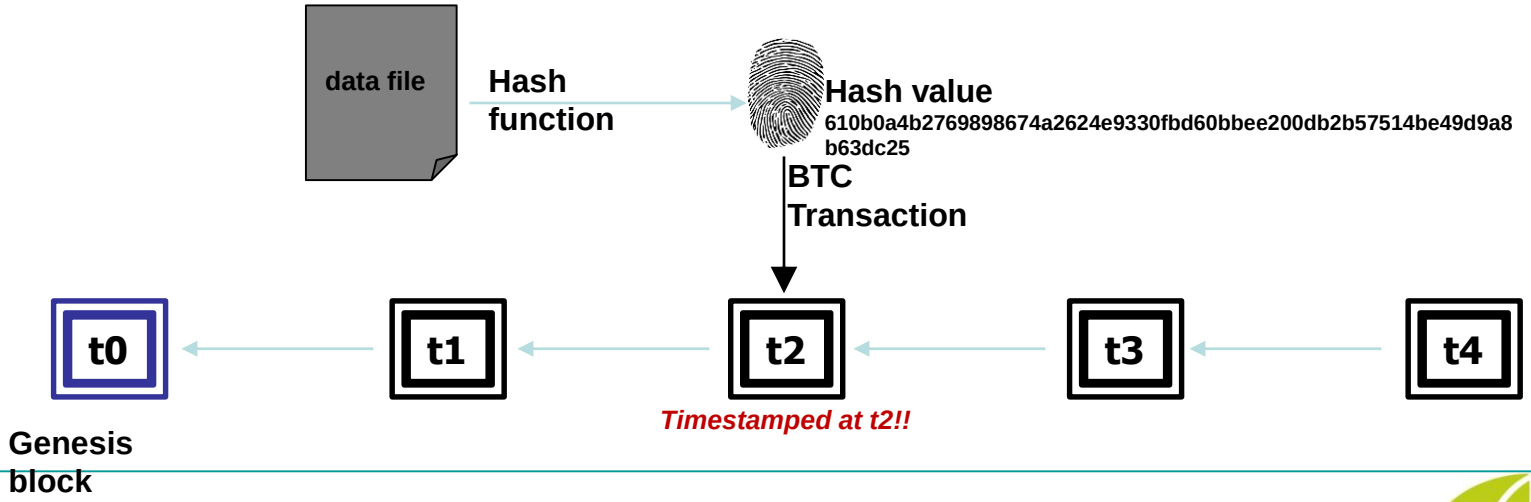
1. Internet Money
2. The Double Spending Problem
3. Bitcoin as Digital Gold
4. **Blockchain Beyond Bitcoin: Notarization**
5. Bitcoin as Investment Asset

Blockchain Beyond Bitcoin: 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

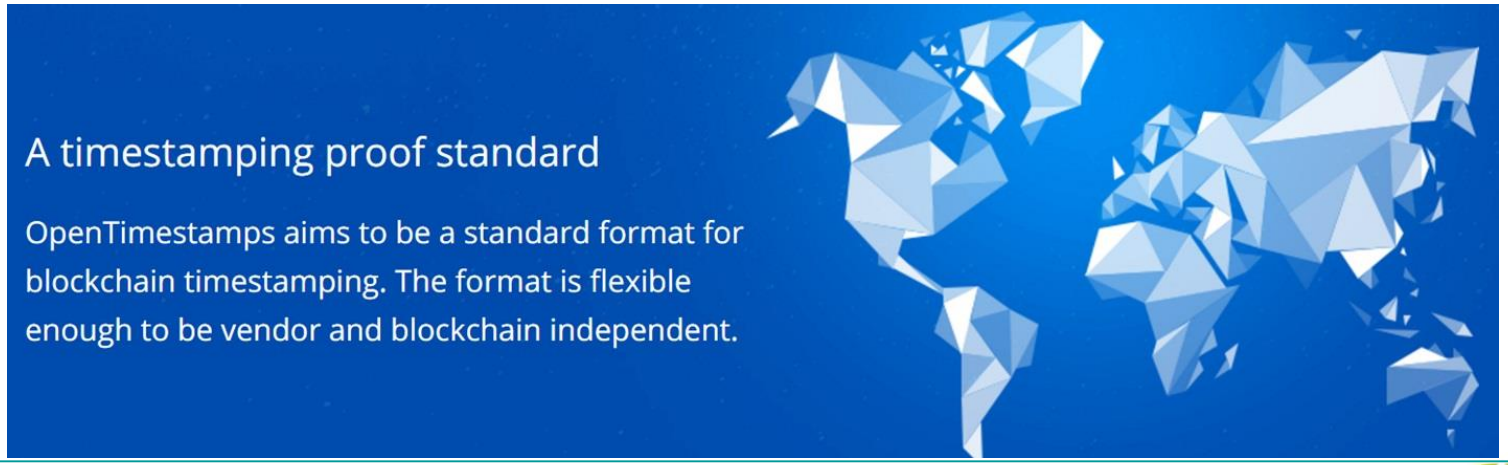
A single transaction can timestamp an unlimited number of documents

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



Digital Gold Jewelry

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

not essential
but effective at leveraging its beauty

Table of Contents

1. Internet Money
2. The Double Spending Problem
3. Bitcoin as Digital Gold
4. Blockchain Beyond Bitcoin: Notarization
5. **Bitcoin as Investment Asset**

BTC/USD Exchange Rate

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

BTC Market Cap: about $100 (USD M0 1959-2017 average has been $680B)

This chart is licensed under a Creative Commons Attribution-ShareAlike 3.0 Unported License.

BTC/USD Exchange Rate

https://bitcoincharts.com/charts/bitstampUSD#tgWzm1g10zm2g25zl

Exponential growth

This chart is licensed under a Creative Commons Attribution-ShareAlike 3.0 Unported License.

Risk Measures

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

Bibliography

Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008) https://bitcoin.org/bitcoin.pdf

Bitcoin, 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

Blockchain Needs A Native Digital Asset, https://www.finextra.com/videoarticle/1241/blockchain-needs-a-native-digital-asset

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 Videos, 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

Bitcoin is hard to understand: not a technology, a cultural paradigm shift instead

Bitcoin solves the double spending problem (distributed consensus), allowing for the decentralization paradigm

Bitcoin is digital gold:

- it could be as relevant as physical gold for the history of our civilization and the future of money & finance;
- it is bootstrapping new monetary systems

There is a blockchain beyond bitcoin: notarization

Bitcoin is a new asset class with no correlation with other asset classes: investing in bitcoin is rational diversification