



Bitcoin and Blockchain Technology

Economics and Environmental Sustainability
of the Digital Scarcity Experiment

Comments, corrections, and questions: <https://drive.google.com/open?id=1FpudunEQrBY8WLTSLzwThOoFxmKGTCho>



Bitcoin Is Hard to Understand

At the crossroads of:

- Cryptography
- Computer networking and distributed systems
- Game theory
- Monetary theory

With relevant cultural and political implications

*Mainly not a technology,
a cultural paradigm shift instead*



Table of Contents

1. Internet Money

2. About Money

3. Private Money and the Centralization Dilemma

4. The Double Spending Problem

5. Bitcoin as Digital Gold

6. Bitcoin as Investment Asset



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 Internet eCash Will Be Developed

"The one thing that's missing, but that'll soon be developed, is a reliable eCash, 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>



- 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/>

USD83M Transacted in Bitcoin, \$0.04 fee

 **BLOCKCHAIN**
info

Home Charts Stats Markets API Wallet

Search 

Transaction View information about a bitcoin transaction

8f1d3a8ef6b2d4a25d2f499279e01518b4770819ccbc39a765c4c326170c61b3

1JEC8vYP9cEDSu6N6DXkkYd3RaeWAdscqN
113L62kchKukrSmA9ur7Xq9KorCV3u4dTG
16vXP31udcx67Xk9KZJNAq2JM6i4hFSGyh
1ABobw22YXGu4vKtysgX9AKRqz3fUFWv4E
1JYTUJZMTsJkqDfLzBG1bGcaBngLgSPAoQ
1NaZM6vqvW14Q3P7XWUTB9Q6NWNESLbwEb
1GVlpITSEwC1vUe3UGFRBHjGTrWVfuiArs
1HNaQ8HWPQCW93aQzCHBr3EdqEgqfQV3ir
1PuSoNughjE4zTdRQS2sDhLEfbVgkB3ks7
1GuJf9YrV853Da9GouBvUq2zAjEdn8ej9d



1JoktQJhCzuCQkt3GnQ8Xddcq4mUgNyXEa

217,517.63438199 BTC

217,517.63438199 BTC

Value at time of transaction
82,982,977.52 USD

Summary	
Size	8680 (bytes)
Received Time	2014-12-02 14:22:15
Included In Blocks	332586 (2014-12-02 14:22:15 +0 minutes)

Inputs and Outputs	
Total Input	217,517.63448199 BTC
Total Output	217,517.63438199 BTC
Fees	0.0001 BTC

<https://blockchain.info/tx/8f1d3a8ef6b2d4a25d2f499279e01518b4770819ccbc39a765c4c326170c61b3>



- Decentralized: no central authority, no intermediaries
- Permissionless: no regulator
- Censorship resistant: no frozen funds
- Open-access: no discrimination, no amount limits, 24/7/365
- 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



Table of Contents

1. Internet Money
- 2. About Money**
3. Private Money and the Centralization Dilemma
4. The Double Spending Problem
5. Bitcoin as Digital Gold
6. Bitcoin as Investment Asset



Money As A Social Relation Instrument

- Human beings are born into a gift economy
- Enlarged relationship circle requires exchange economy
- Barter economy: coincidence of wants
- Trade economy: money as medium of exchange
- Global information economy: supranational digital money

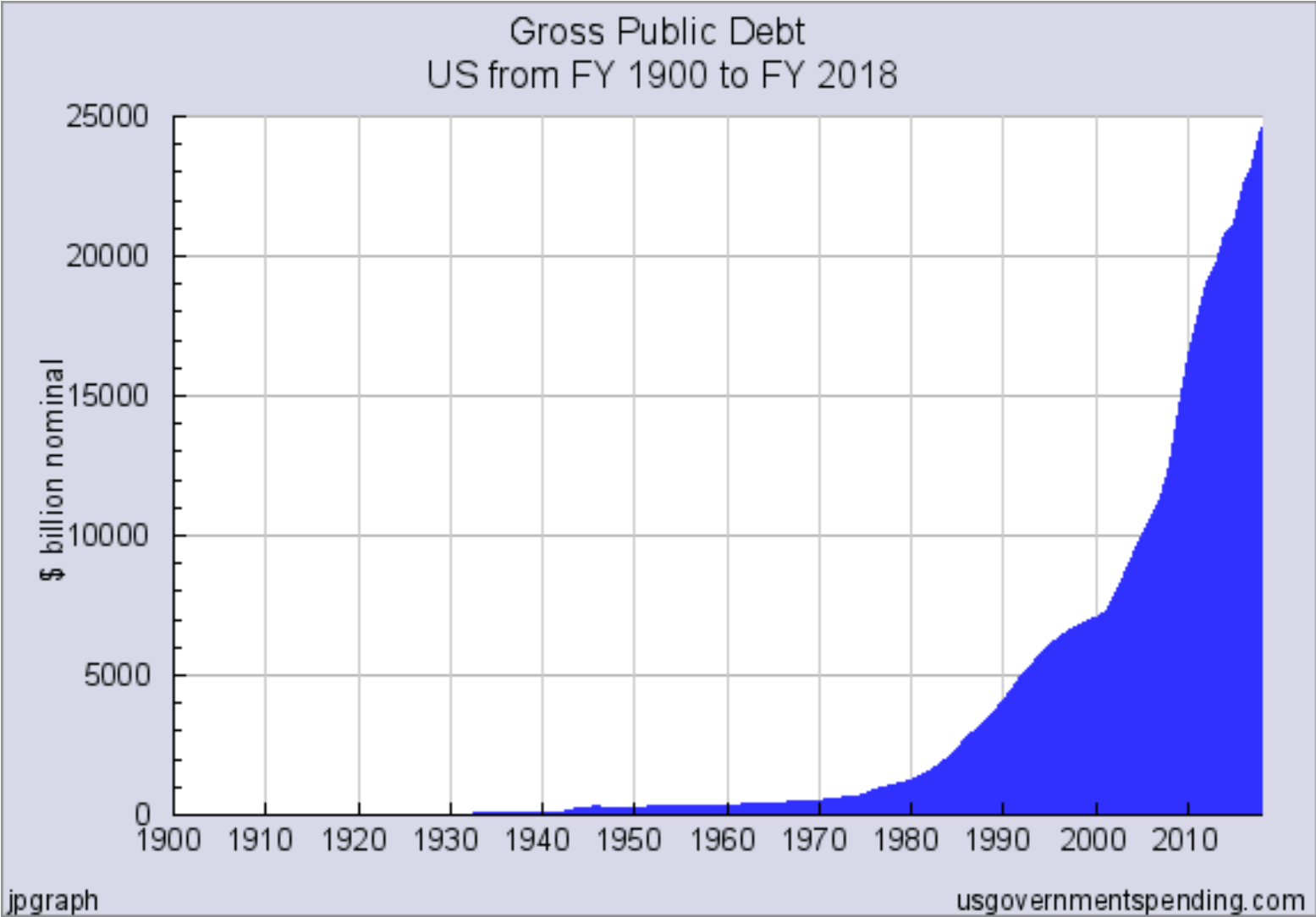


Trade Economy: From Gold Standard to *Fiat* Money

- 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



Gross US Public Debt





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>

Hyperinflation





USD has lost 96% of its Purchasing Power since Federal Reserve establishment in 1913

US Dollar Purchasing Power





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>

Denationalisation of Money, The Institute of Economic Affairs, <http://www.mises.org/books/denationalisation.pdf>



Table of Contents

1. Internet Money
2. About Money
- 3. Private Money and the Centralization Dilemma**
4. The Double Spending Problem
5. Bitcoin as Digital Gold
6. Bitcoin as Investment Asset



Permissionless Innovation: Gentle, Fast, and Effective

Permissionless innovation: 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?



Private Monies

- A widely accepted medium of exchange or payment
 - issued by a non-governmental body
 - without legal privileges
- Private monies do not have to be generally acceptable; they must be accepted in a given economic community
- Public demand for private currencies:
 - hold them in the expectation that they will not diminish in purchasing power as state money has
 - wish to be part of a movement against increasing state control of economic and personal behavior
 - conduct illegal activity
 - just want better money



A Cypherpunk's Manifesto

"Privacy in an open society also requires cryptography [...] We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence. [...] We must defend our own privacy if we expect to have any. [...] We are defending our privacy with cryptography, [...] with digital signatures, and with electronic money"

Eric Hughes, A Cypherpunk's Manifesto

<https://www.activism.net/cypherpunk/manifesto.html>

Cryptography is the slingshot that David, the little man, can use to kill Goliath, the dystopian Big Brother



Bitcoin Precursors

- Ecash, David Chaum, 1982 (blind signature)
- Hashcash, Adam Back, 1997 (Proof-of-Work)
- B-money, Wei Dai, 1998 (distributed database)
- Bit gold, Nick Szabo, 1998 (distributed database, sequential money creation)
- Anonymous Electronic Cash, Tomas Sander and Amnon Ta-Shma, 1999 (anonymity)
- Reusable Proof-of-Work, Hal Finney, 2004



Liberty Dollar: 1998-2009

- Private mint that issued gold and silver coins; also issued notes redeemable in precious metals
- Periodically revalued against USD: the value of the latter fell over time against precious metals
- Specifically designed to function in parallel with and in competition to USD
- Never marketed or represented as official US currency
- Highly successful: second most popular currency in the US
- Its use declared a federal crime by the US government
- Its founders convicted for counterfeiting, fraud and conspiracy against the United States



E-gold: 1996-2007

- Digital payment system with gold as unit of account
- User accounts backed by gold reserves
- By 2005, e-gold was second only to PayPal in the online payments industry: 1.2M accounts and \$1.5B transactions
- Indicted in April 2007 by US law enforcement services
- Charges: unlicensed money-transmitting entity and a means of moving the proceeds of illegal activities
- Never proven and even the judge expressed major doubts
- 'Offshore' payment system rather than a money transmitter or bank as defined under then-existing regulations, not least because gold was not legally 'money'



The Centralization Dilemma

- To remove the weakness of a central point of failure, distributed technologies seemed promising (e.g. BitTorrent)
- Anyway, in digital cash schemes a single digital token, being just a file that can be duplicated, can be spent twice: a centralized trusted party is required to avoid *double spending*



Table of Contents

1. Internet Money
2. About Money
3. Private Money and the Centralization Dilemma
- 4. The Double Spending Problem**
5. Bitcoin as Digital Gold
6. Bitcoin as Investment Asset



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
- How can we forbid Alice from spending the same bitcoins a second time to Carol's **address**? Which transaction should be valid: the one to Bob's **address** or Carol's **address**?
- A centralized trusted party has always been required to prevent ***double spending***



The Bitcoin Announcement

From: Satoshi Nakamoto <satoshi <at> vistomail.com>

Subject: Bitcoin P2P e-cash paper

Newsgroups: gmane.comp.encryption.general (The Cryptography Mailing List)

Date: 2008-10-31 18:10:00 GMT

I've been working on a new electronic cash system that's fully peer-to-peer, with **no trusted third party**. The paper is available at: <http://www.bitcoin.org/bitcoin.pdf>

The main properties:

Double-spending is prevented with a peer-to-peer network.

No mint or other trusted parties.

Participants can be anonymous.

New coins are made from Hashcash style **proof-of-work**.

The **proof-of-work** for new coin generation also powers the network to **prevent double-spending**.

Bitcoin: A Peer-to-Peer Electronic Cash System

Abstract. A purely peer-to-peer version of electronic cash [...]

<http://article.gmane.org/gmane.comp.encryption.general/12588/>



Bitcoin Network: A Distributed Back-office

- All network nodes validate and clear all transactions
- Mining nodes provide the additional computational power required for transaction settlement
- Without a central trusted party, how do they reach *distributed consensus* on the transaction history?
- Consensus in a distributed asynchronous network with faulty (or malicious) nodes is a very hard problem: Computer Science even provides impossibility results



Bitcoin's Public Ledger: A Chain of Blocks

- Transactions are bundled in blocks (about one block every 10 minutes) and sequentially chained
- The cryptographic link between blocks requires computing power to be created
- A block is valid only if it includes valid transactions



Mining

- Miners compete to finalize (settle) 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:
 - A double spending transaction 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



Ledger Immutability

- Because of the *proof-of-work*, the chances of a block being altered decrease exponentially with the number of blocks chained after it
- The chain of blocks is a history of transactions resilient to network attackers because it cannot be altered without huge resources
- Computing power is measured in hash/s, hash being the basic operation needed for validation



Nakamoto Distributed Consensus

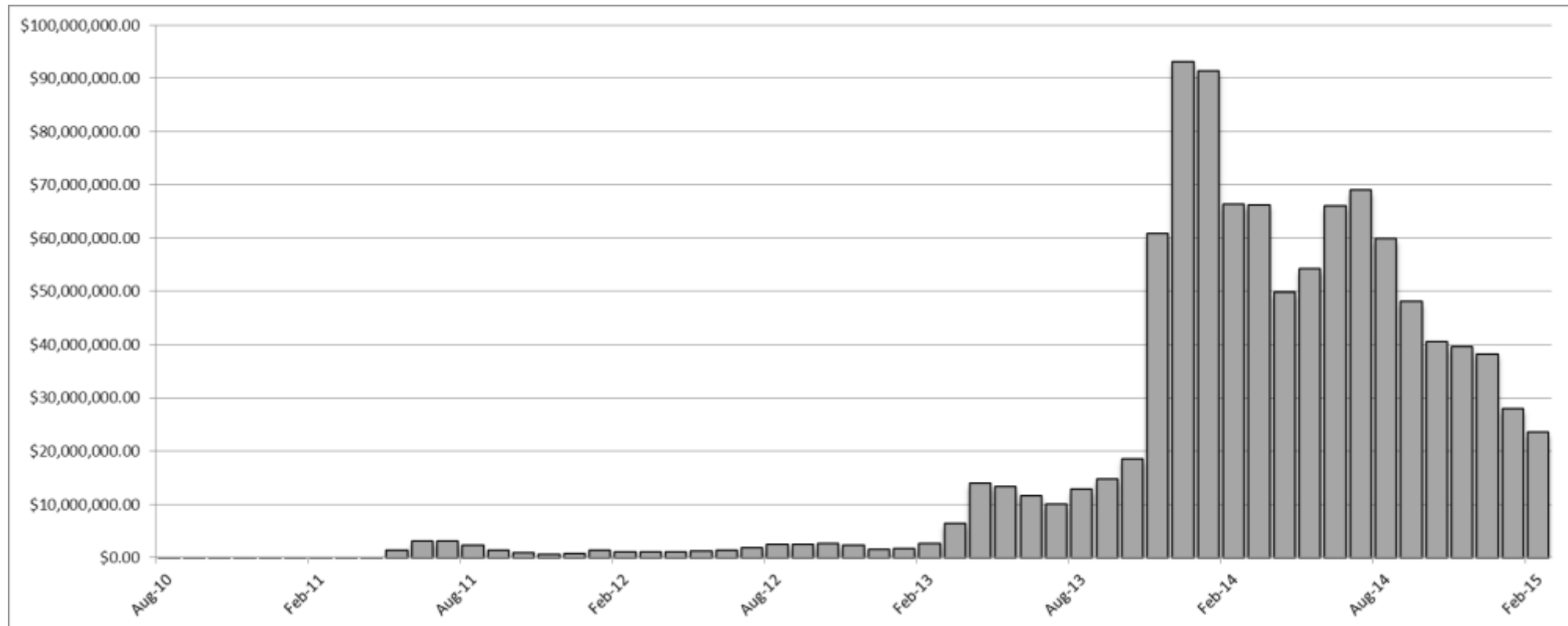
Practical Byzantine Fault Tolerant (PBFT) *distributed consensus* is achieved using (game theory) economic incentive for the mining nodes to be honest

- 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. issuance of new bitcoins
- Seigniorage revenues subsidize the network



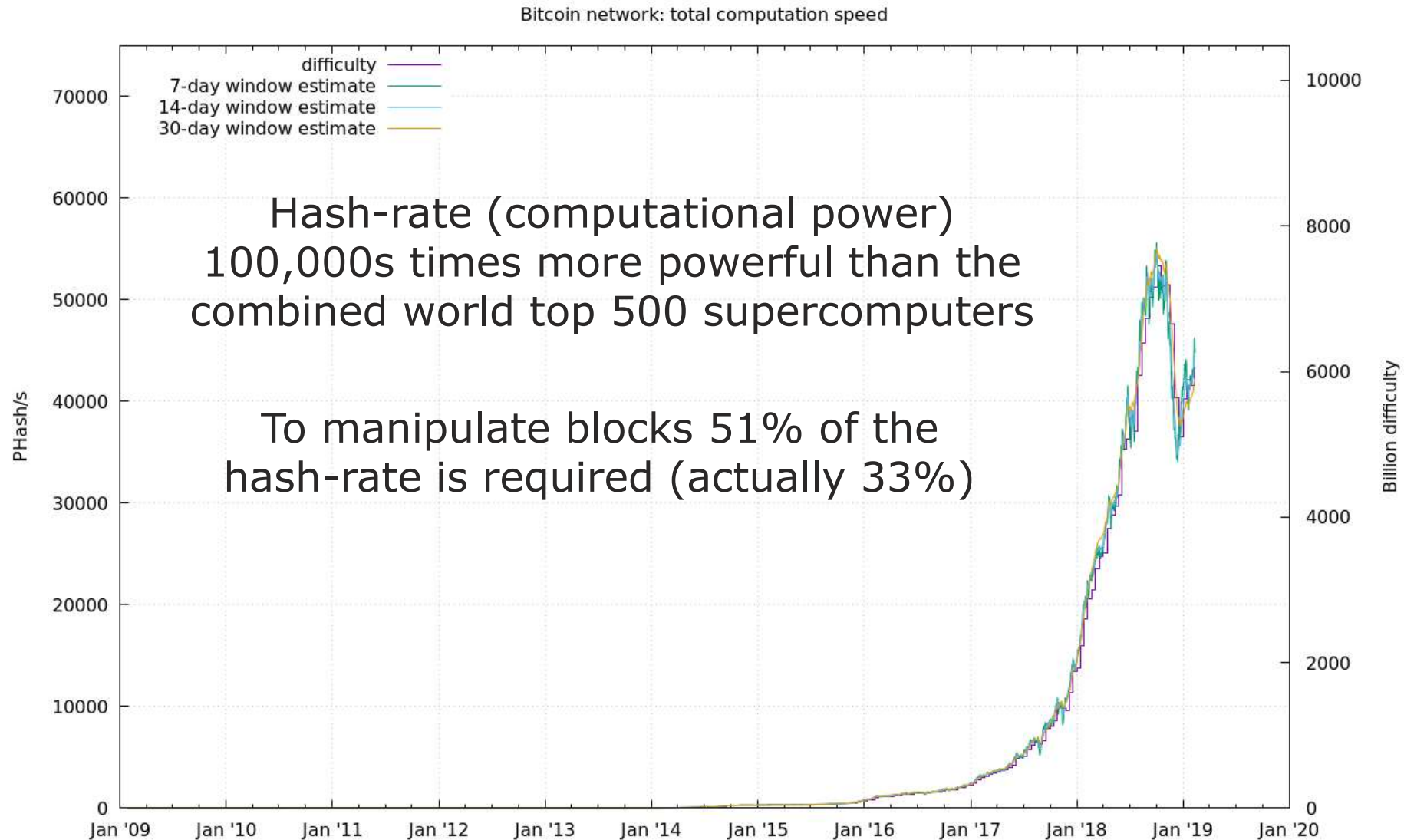
Seigniorage Revenues Cover Consensus Cost

- Seigniorage revenues subsidize the network, making transactions cheap
- 144 block/day, 365 day/year, 12.5 BTC/block
- About \$7 billions per year (as of November 2017, BTC=\$10,000)





Total Network Hashing Rate



<http://bitcoin.sipa.be/speed-lin-ever.png>



Mining Hardware

Driven by the search of lower power consumption and higher hashing rate:

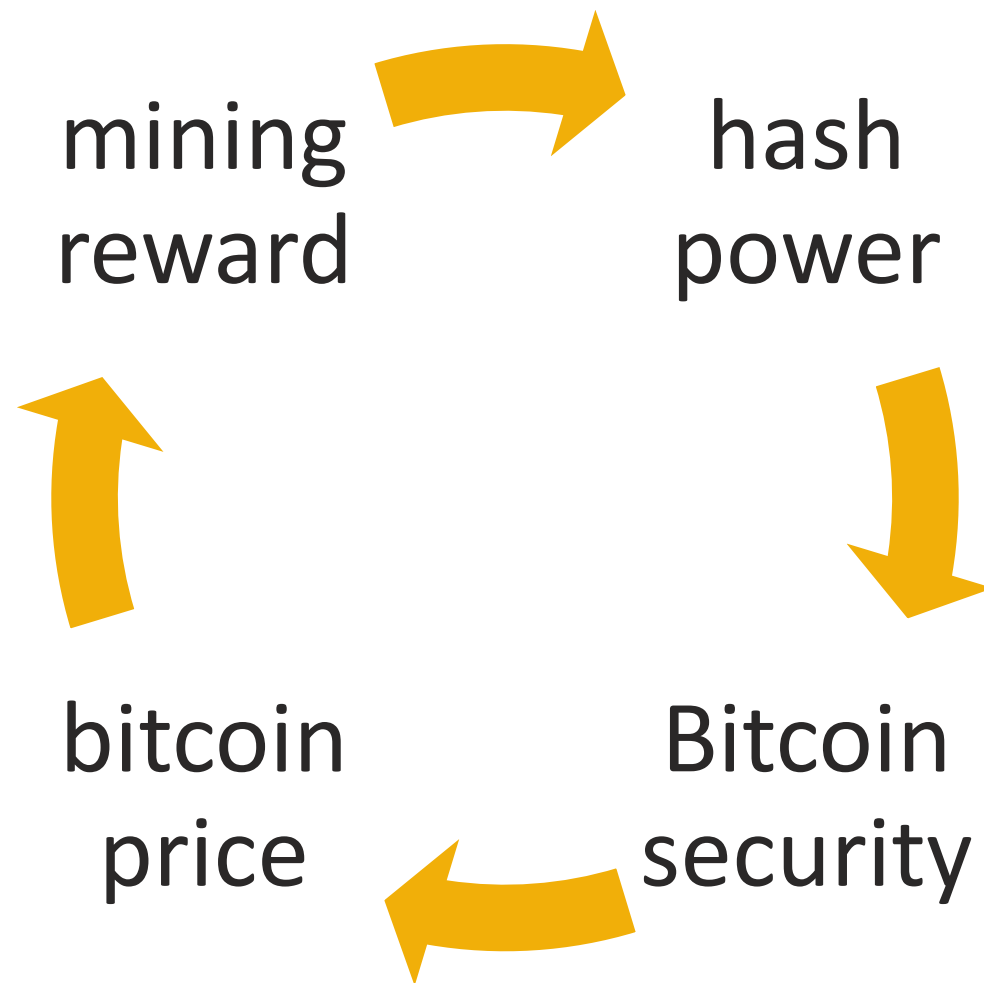
- CPUs (Computer Processing Unit) were used in 2009
- GPUs (Graphical Processing Unit) proved to perform better in 2010

Moving later to special purpose energy-efficient hardware:

- FPGAs (Field Programmable Gate Array) were programmed for hashing and surpassed GPU in 2011
- ASICs (Application Specific Integrated Circuit), designed and manufactured for the specific purpose of hash computations, were introduced in 2013 for Bitcoin and are now the standard



Virtuous Cycle





Proof-of-Work

- Resources consumed as *proof-of-work* make bitcoin valuable
- Miners are willing to destroy resources to acquire bitcoins: they are the first to recognize bitcoin value!
- Miners are rational economic agents, they locate their business where energy is cheap (renewable energy)
- Energy consumption does not grow linearly, because of efficiency improvement (see CPU→GPU→FPGA→ASIC)



Environmental Sustainability

- Bitcoin energy consumption: 8 TWh
 - comparable to Ireland or Denmark
 - 1/8th of US data-centers
 - 0.21% of US overall consumption
- Banknote system: 11 TWh
- Gold extraction: 132 TWh
- 2016 China hydroelectric untapped capacity (dissipated): 95 TWh

- What if PoW might absorb all renewable energy excess capacity available in the future?



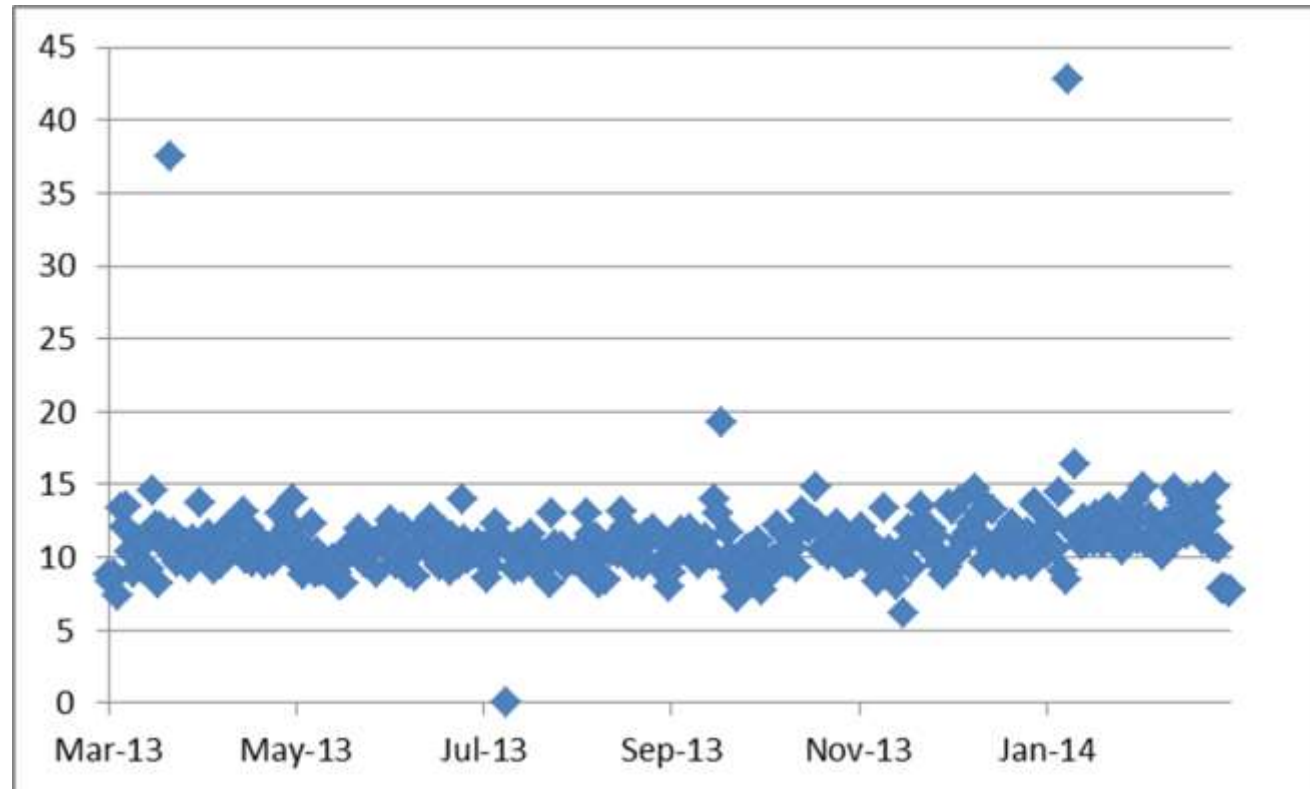
Table of Contents

1. Internet Money
2. About Money
3. Private Money and the Centralization Dilemma
4. The Double Spending Problem
5. Bitcoin as Digital Gold
- 6. Bitcoin as Investment Asset**



Validation Process: Block Generation

The *proof-of-work* difficulty is adapted about every 2 weeks (2015 blocks) to the overall available computing power ensuring about one block every 10 minutes



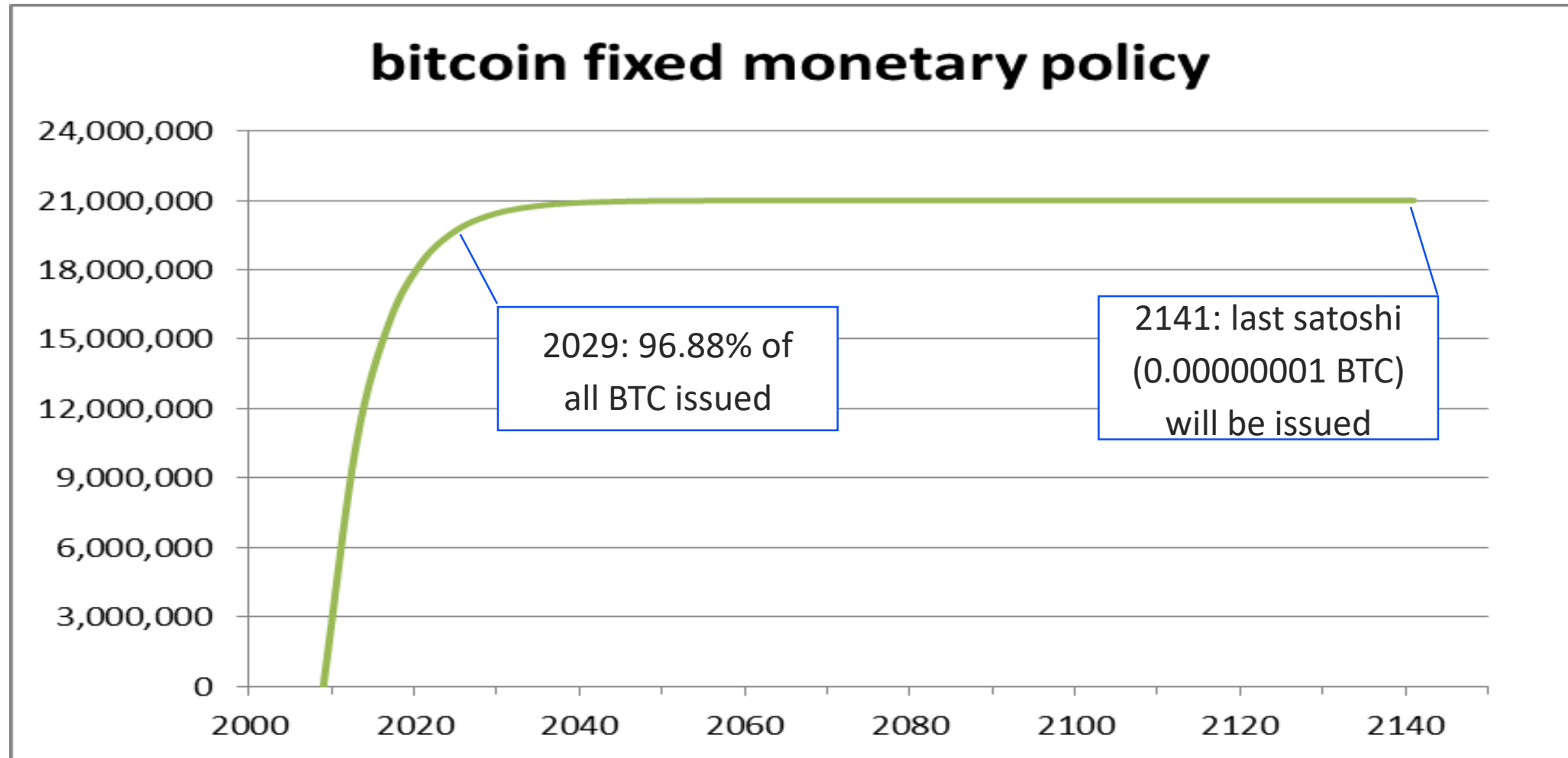


Bitcoin Monetary Rule

- 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 is 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 of decreasing incremental extraction



What Makes Bitcoin Special?

Bitcoin is digital gold

with a secure uncensorable embedded

settlement network

- More a crypto-commodity than 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

It is disconcerting that people are still, continuously, underestimating bitcoin



Explain Money to an Alien

Traditional (*fiat*) money

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

bitcoin

- No intrinsic value (digital gold)
- Currency security based on math/cryptography
- Algorithmic governance
- Deterministic supply
- Available as free non-binding choice



Different Opinions

Alan Greenspan

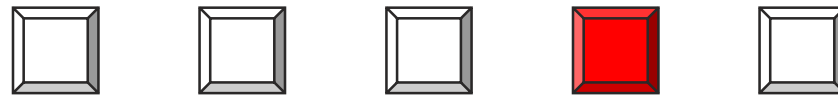
"It's a bubble. It has to have intrinsic value: you have to really stretch your imagination to infer what the intrinsic value of Bitcoin is. I haven't been able to do it. Maybe somebody else can. I do not understand where the backing of Bitcoin is coming from"

Lloyd Blankfein

"The list of things that are conventional today that I use every day that I thought would never make it is a very long list. If bitcoin works, I say to myself... 'Hmmm, maybe that was a natural progression from hard money to fiat money to consensus money.' So who's to say..."

The Schelling Point of Consensus Money

- In game theory Schelling point is: “focal point[s] for each person’s expectation of what the other expects him to expect to be expected to do”
- E.g. two people unable to communicate are urged to select a square among a series of similar squares and rewarded only if they select the same one



- They will look for a choice that might seem more natural, special, or relevant: the red one

Bitcoin is the Schelling point of consensus money!



Bitcoin Transactions Are Not Taking Off

- There is evidence that bitcoin is not really used for transactions
- Max number of transactions per second
 - VISA: 60,000 tx/sec
 - Bitcoin: 7 tx/sec
- Bitcoin can only scale with second layer solutions, e.g. Lightning Network, Sidechain (Liquid)

Two Pizzas for 10,000 Bitcoins... really!!

laszlo

Full Member



Activity: 199



Pizza for bitcoins?

May 18, 2010, 12:35:20 AM

#1

I'll pay 10,000 bitcoins for a couple of pizzas.. like maybe 2 large ones so I have some left over for the next day. I like having left over pizza to nibble on later. You can make the pizza yourself and bring it to my house or order it for me from a delivery place, but what I'm aiming for is getting food delivered in exchange for bitcoins where I don't have to order or prepare it myself, kind of like ordering a 'breakfast platter' at a hotel or something, they just bring you something to eat and you're happy!

I like things like onions, peppers, sausage, mushrooms, tomatoes, pepperoni, etc.. just standard stuff no weird fish topping or anything like that. I also like regular cheese pizzas which may be cheaper to prepare or otherwise acquire.

If you're interested please let me know and we can work out a deal.

Thanks,
Laszlo

laszlo

Full Member



Activity: 199



Re: Pizza for bitcoins?

May 22, 2010, 07:17:26 PM




I just want to report that I successfully traded 10,000 bitcoins for pizza.


Pictures: <http://heliacal.net/~solar/bitcoin/pizza/>

Thanks jercos!

BC: 157fRrqAKrDyGHR1Bx3yDxeMv8Rh45aUet

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.



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 is bootstrapping 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
- Bitcoin can be used as reserve asset
- Concurrent cryptocurrencies competing in monetary policy definition and reference basket choices
- Private monies competing with legal tender monies: towards separation of Money and State



Table of Contents

1. Internet Money
2. About Money
3. Private Money and the Centralization Dilemma
4. The Double Spending Problem
5. Bitcoin as Digital Gold
- 6. Bitcoin as Investment Asset**

BTC/USD Exchange Rate

BTC Market Cap: about \$60B (USD M0 1959-2017 average has been 680)



Price dynamic is the discovery process of value: volatility is physiologic when it comes to assess the fair value of something so controversial as the digital equivalent of gold



This chart is licensed under a [Creative Commons Attribution-ShareAlike 3.0 Unported License](https://creativecommons.org/licenses/by-sa/3.0/).

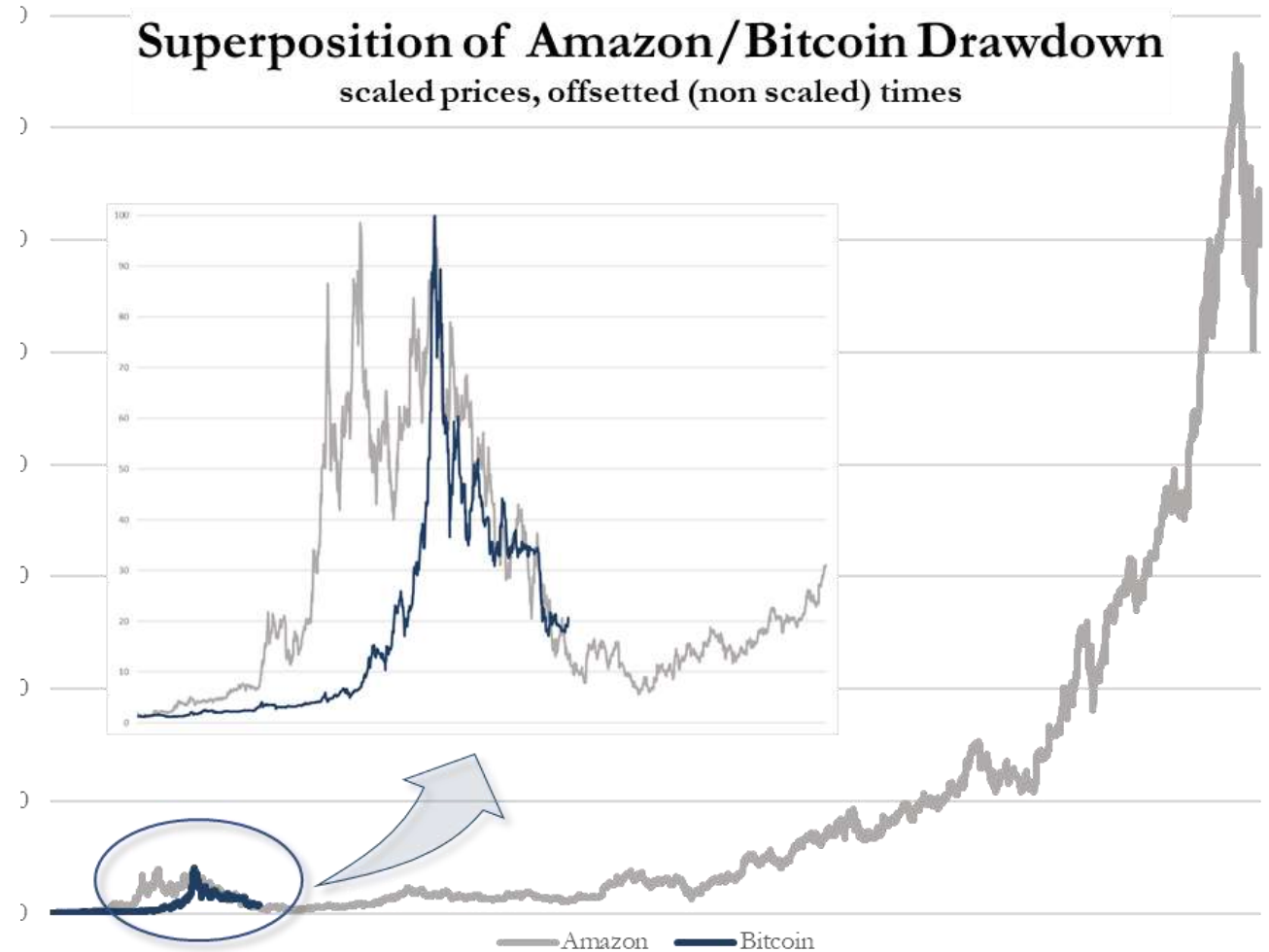
<http://bitcoincharts.com/charts/bitstampUSD#tgWzm1g10zm2g25>



Comparison with Amazon

The value of digital gold is as hard to grasp today as the value of e-commerce in the 90s.

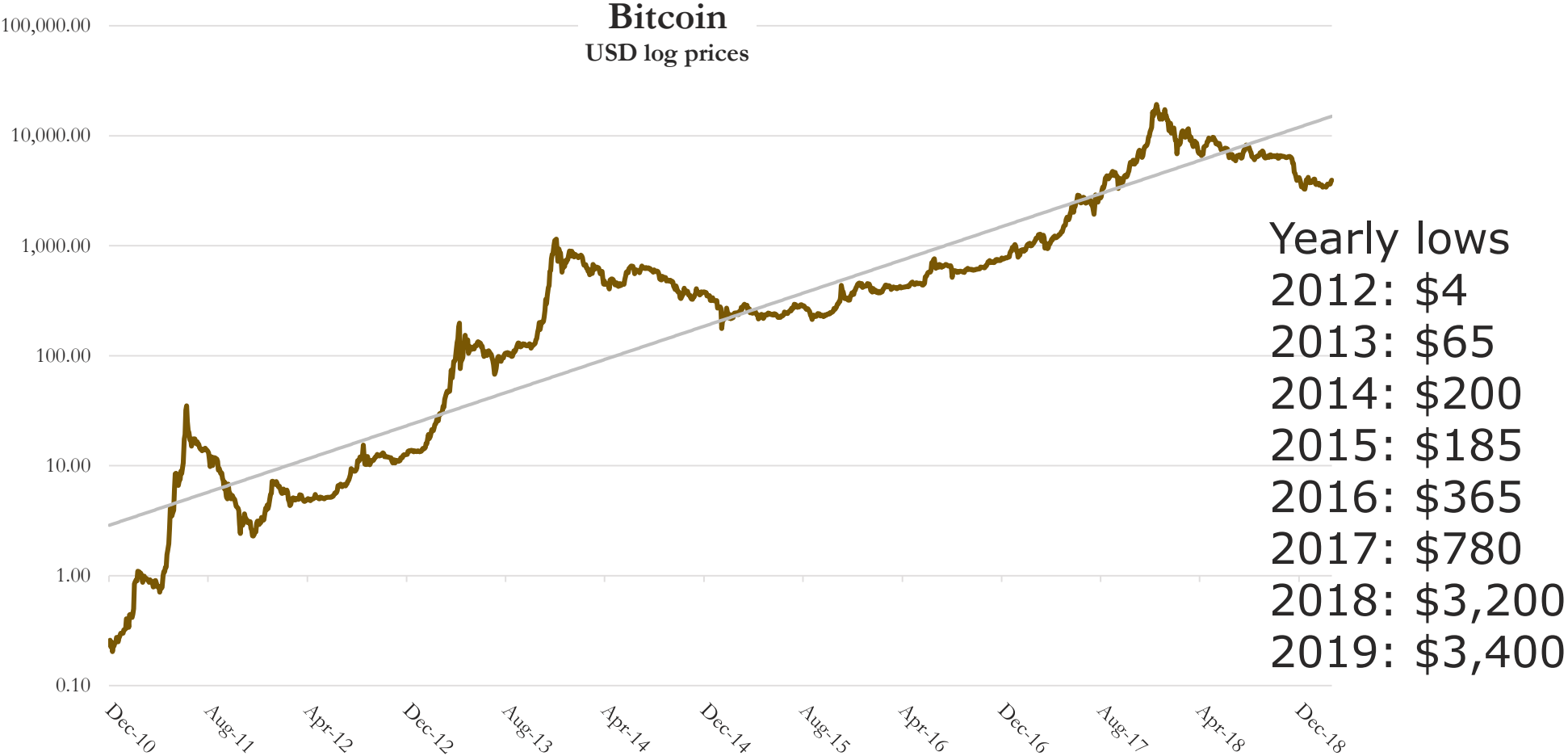
Bitcoin worst drawdown has been 93.07%; Amazon worst drawdown has been 94.40% when the dot-com bubble burst





Exponential Growth

Exponential trendline with a R^2 of 86.9%



High Return: the Compensation for High Risk

Bitcoin risks are an order of magnitude greater than other asset classes

<i>Jul 2010 - Nov 2018</i>		BITCOIN	GOLD	WTI	GRAIN	IND. METALS	EUR	GBP	CHF	JPY
Return	Daily Mean Return	0.50%	0.00%	-0.01%	-0.04%	-0.02%	-0.01%	-0.01%	0.00%	-0.02%
	Daily Min Return	-60.09%	-9.39%	-10.79%	-6.06%	-6.71%	-2.30%	-7.37%	-9.06%	-3.51%
	Daily Max Return	51.70%	5.07%	11.62%	6.39%	5.54%	2.95%	2.58%	13.45%	3.38%
	Mean Return (annualized)	250.95%	-0.95%	-3.40%	-8.90%	-5.06%	-2.46%	-2.54%	-0.29%	-3.90%
Risk	Volatility (daily)	6.48%	0.98%	2.02%	1.34%	1.15%	0.53%	0.52%	0.67%	0.57%
	Volatility (annualized)	102.89%	15.62%	32.00%	21.24%	18.19%	8.45%	8.30%	10.61%	8.99%
	Skewness	-0.264	-0.693	0.072	0.053	-0.062	0.046	-1.431	2.864	-0.142
	Excess Kurtosis	15.154	7.136	3.332	2.375	2.398	1.793	21.171	95.506	3.510
	VaR 99%	18.83%	2.87%	5.61%	3.69%	2.94%	1.45%	1.23%	1.47%	1.63%
	Expected Shortfall at 99%	28.60%	3.97%	6.83%	4.77%	3.89%	1.69%	1.93%	2.19%	2.13%
	Worst Draw-down	93.07%	44.58%	76.99%	65.23%	57.82%	30.19%	29.69%	29.21%	39.66%
Risk/Ret	Sharpe Ratio	2.416	-0.211	-0.180	-0.529	-0.407	-0.568	-0.588	-0.248	-0.695
	Correlation with Bitcoin	100%	0.02%	1.42%	3.41%	3.41%	2.94%	0.72%	3.47%	-1.42%



High Return: the Compensation for High Risk

Bitcoin has volatility and worst draw-down similar to VIX; anyway, VIX is anticorrelated with equities, Bitcoin is decorrelated

<i>Jul 2010 - Nov 2018</i>		BITCOIN	MSCI BRIC	EURO STOXX50	NASDAQ	S&P500	VIX	Euro Bonds	US Bonds	EUR Bonds
Return	Daily Mean Return	0.50%	-0.01%	0.00%	0.05%	0.04%	0.00%	0.00%	0.01%	0.00%
	Daily Min Return	-60.09%	-6.93%	-10.67%	-7.15%	-6.90%	-31.41%	-2.76%	-1.01%	-2.62%
	Daily Max Return	51.70%	4.75%	8.43%	5.16%	4.63%	76.82%	2.55%	0.83%	2.43%
	Mean Return (annualized)	250.95%	-2.81%	-0.86%	13.72%	10.53%	-0.17%	1.08%	2.19%	0.92%
Risk	Volatility (daily)	6.48%	1.09%	1.39%	1.02%	0.88%	7.64%	0.51%	0.20%	0.54%
	Volatility (annualized)	102.89%	17.38%	22.09%	16.15%	14.05%	121.22%	8.10%	3.16%	8.64%
	Skewness	-0.264	-0.283	-0.330	-0.544	-0.602	1.204	-0.117	-0.262	-0.065
	Excess Kurtosis	15.154	2.582	4.917	4.041	5.528	8.133	1.555	1.345	1.414
	VaR 99%	18.83%	2.94%	4.14%	2.98%	2.56%	17.98%	1.36%	0.54%	1.46%
	Expected Shortfall at 99%	28.60%	3.90%	5.33%	3.99%	3.64%	22.24%	1.62%	0.65%	1.70%
	Worst Draw-down	93.07%	51.05%	42.76%	18.71%	19.39%	80.96%	16.84%	4.87%	17.66%
Risk/Ret	Sharpe Ratio	2.416	-0.297	-0.145	0.705	0.583	-0.021	-0.156	-0.047	-0.165
	Correlation with Bitcoin	100%	1.39%	5.01%	4.00%	5.07%	-5.31%	2.06%	-1.27%	2.59%



A New Uncorrelated Asset Class

Bitcoin provides a huge diversification to an investment portfolio

	BITCOIN	GOLD	WTI	GRAIN	IND. METALS	EUR	GBP	CHF	JPY	MSCI BRIC	EUROSTOXX50	NASDAQ	S&P500	VIX	Euro Bonds	US Bonds	EUR Bonds	
BITCOIN	100%																	
GOLD	0.02%	100%																
WTI	1.42%	14.50%	100%															
GRAIN	3.41%	13.82%	18.05%	100%														
IND. METALS	3.41%	31.63%	35.30%	20.14%	100%													
EUR	2.94%	36.61%	17.10%	14.05%	29.73%	100%												
GBP	0.72%	24.47%	21.27%	11.64%	25.30%	57.03%	100%											
CHF	3.47%	36.69%	6.25%	7.76%	20.11%	59.52%	35.99%	100%										
JPY	-1.42%	39.52%	-6.81%	2.30%	-3.77%	31.27%	14.43%	35.71%	100%									
MSCI BRIC	1.39%	12.67%	29.67%	15.19%	42.94%	19.17%	23.54%	7.92%	-16.57%	100%								
EUROSTOXX50	5.01%	8.96%	31.94%	15.12%	46.06%	47.44%	41.78%	21.34%	-17.26%	57.04%	100%							
NASDAQ	4.00%	-1.54%	28.59%	13.54%	31.62%	13.42%	17.60%	-1.95%	-21.58%	47.17%	55.39%	100%						
S&P500	5.07%	-1.04%	34.34%	14.72%	34.15%	16.74%	20.46%	0.07%	-22.29%	48.06%	61.16%	94.92%	100%					
VIX	-5.31%	0.95%	-25.97%	-13.75%	-24.04%	-7.55%	-14.38%	3.40%	21.83%	-38.76%	-46.10%	-77.56%	-80.32%	100%				
Euro Bonds	2.06%	42.61%	13.45%	12.20%	25.33%	91.87%	61.72%	59.71%	39.74%	18.75%	41.31%	9.78%	12.26%	-6.07%	100%			
US Bonds	-1.27%	21.11%	-21.26%	-6.10%	-17.44%	-0.59%	-5.00%	12.91%	37.90%	-15.00%	-28.01%	-30.82%	-33.69%	26.60%	19.36%	100%		
EUR Bonds	2.59%	40.46%	13.29%	11.96%	26.57%	94.39%	53.34%	58.05%	36.77%	18.94%	43.95%	11.12%	13.84%	-6.78%	98.37%	14.31%	100%	

Positive correlation
Uncorrelated
Negative correlation

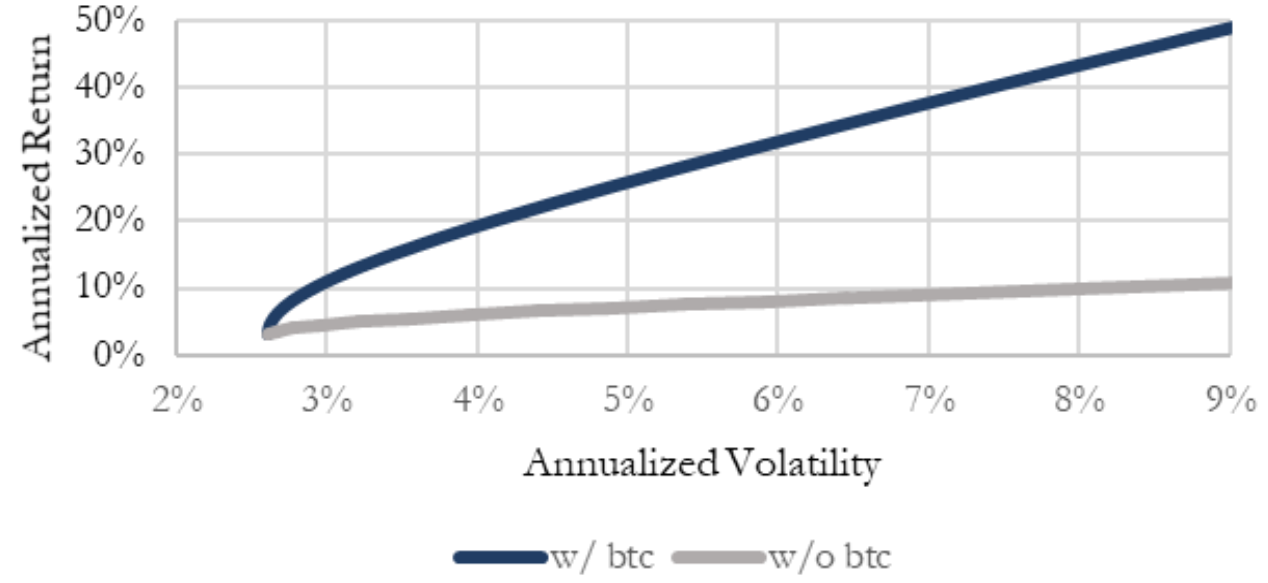


Bitcoin: CAPM Diversification

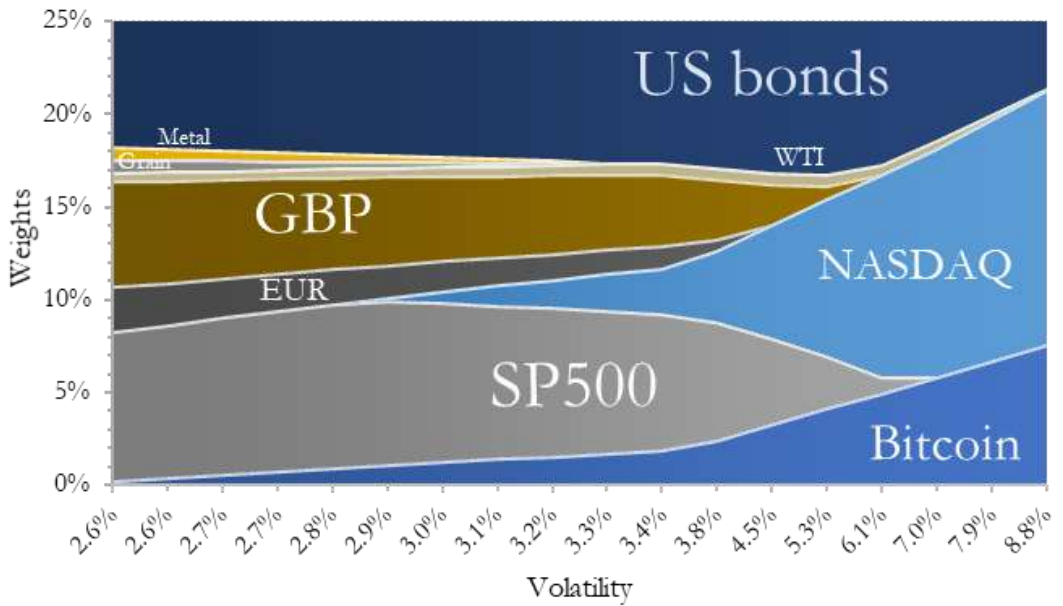
Bitcoin increases expected return for a given level of risk, e.g.

- at 4% volatility, return increases more than 140bps
- at 10% return, volatility decreases from 8.60% to 2.90%

CAPM Efficient Frontier



Optimal Allocation Including Bitcoin



For conservative risk levels, optimal CAPM diversification suggests to invest in Bitcoin up to 5% of the portfolio



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
 - The number of estimated BTC investors is about 50 millions; with a forecast to 350 millions, BTC price might increase x49



Bibliography

- N. Szabo, Shelling Out: The Origins of Money (2002) <https://nakamoinstitute.org/shelling-out/>
- S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2008) <https://bitcoin.org/bitcoin.pdf>
- F. Ametrano, Hayek Money: the Cryptocurrency Price Stability Solution (2014), <http://ssrn.com/abstract=2425270>
- F. Ametrano, Bitcoin, Blockchain and Distributed Ledger Technology: Hype or Reality? (2017) <https://ssrn.com/abstract=2832249>
- S. Ammous, The Bitcoin Standard: The Decentralized Alternative to Central Banking (2018)
- F. Ametrano, Bitcoin as Digital Gold (2018), United Nations Department of Economic and Social Affairs; video: <https://goo.gl/NkEC9w>; slides: <https://goo.gl/szzBXh>
- F. Ametrano, Blockchain Needs A Native Digital Asset, <https://www.finextra.com/videoarticle/1241/blockchain-needs-a-native-digital-asset>
- F. Ametrano, YouTube playlist: <https://goo.gl/qDvKXi>



Takeaways

- Bitcoin (and blockchain): not a technology, a cultural paradigm shift instead
- Bitcoin solves the double spending problem (distributed consensus), allowing for the decentralization paradigm
- Bitcoin is environmentally sustainable
- Bitcoin aims to be the digital equivalent of gold
- Bitcoin might prove to be as relevant as gold for the history of civilization and the future of money and finance; it is already bootstrapping new monetary systems
- Bitcoin has no correlation with other asset classes: bitcoin investing is rational diversification
- Time will tell if the bitcoin experiment of scarcity in digital realm is economically and game-theoretically sustainable



Digital Gold Institute

"Scarcity in the Digital Realm"



Ferdinando M. Ametrano

Executive Director

ferdinando@dgi.io



Paolo Mazzocchi

Chief Operating Officer

paolo@dgi.io

info@dgi.io



www.dgi.io



www.dgi.io/feed.xml



www.github.com/dginst



www.twitter.com/DigitalGoldInst



www.facebook.com/DigitalGoldInstitute



www.linkedin.com/company/digital-gold-institute

