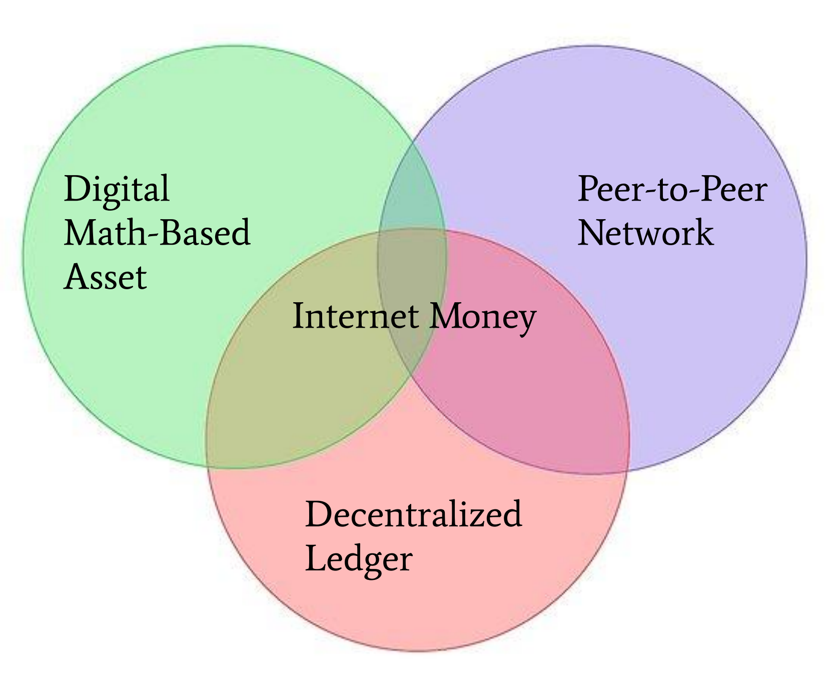
The case for a small allocation to Bitcoin

Why most portfolios should allocate at least 1% to Bitcoin

What is Bitcoin?

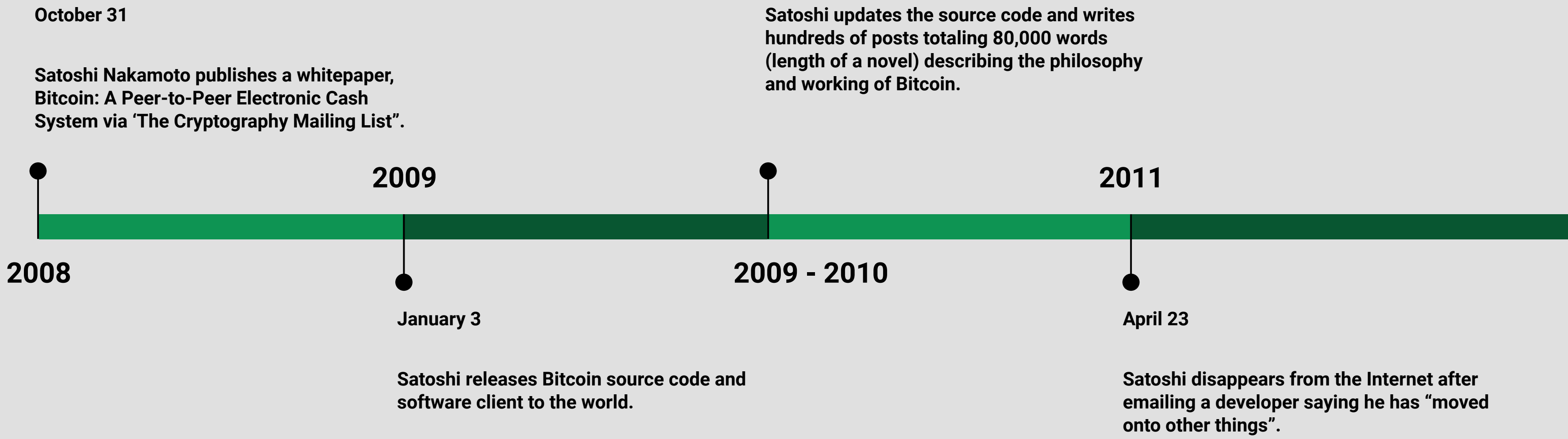
Bitcoin (capital "B") is a peer-to-peer network that maintains a public decentralized ledger of digital math-based assets known as bitcoins (lowercase "b"). The integrity of this ledger is backed and secured by a subnetwork of computers (miners) who audit and archive its transactions for a reward.

Their ownership cannot be changed within the ledger without instructions from their current owner that have been cryptographically authenticated (digital signatures) by a majority of nodes on the Bitcoin network. In essence, "sending a bitcoin" is sending instructions to the network to make a change of custody in the public ledger.



These attributes make the Bitcoin network a financial network or Internet Money.

Who created Bitcoin?



2008

October 31

Satoshi Nakamoto publishes a whitepaper, Bitcoin: A Peer-to-Peer Electronic Cash System via ‘The Cryptography Mailing List”.

2009

January 3

Satoshi releases Bitcoin source code and software client to the world.

2009 - 2010

Satoshi updates the source code and writes hundreds of posts totaling 80,000 words (length of a novel) describing the philosophy and working of Bitcoin.

2011

April 23

Satoshi disappears from the Internet after emailing a developer saying he has “moved onto other things”.

What really is Bitcoin?

It is not about the Tech, it's about Money

"The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micro-payments impossible."

-Satoshi Nakamoto, blogpost in P2P Foundation forum | February 11, 2009, 22:27

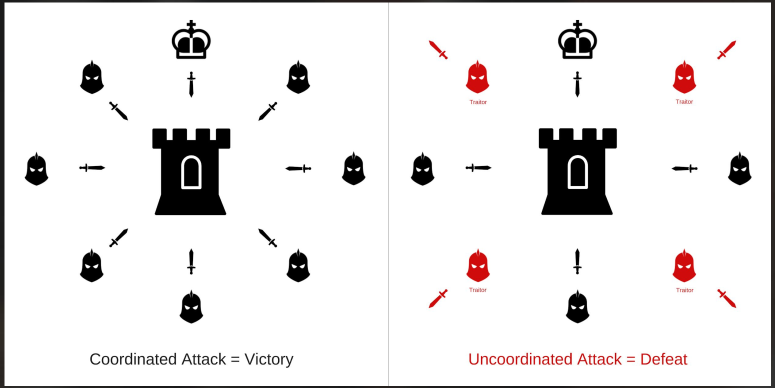
"What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party."

-Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" | October 31, 2008

Byzantine General's Problem

How to reach consensus in a decentralized system?

In 2008 Satoshi Nakamoto, published a 9 page solution to a long-standing problem of computer science known as the Byzantine General's Problem. Nakamoto's solution and the system he built from it — Bitcoin — allowed, for the first time ever, value to be quickly transferred, at great distance, in a completely trustless way. The ramifications of the creation of Bitcoin are so profound for both economics and computer science that Nakamoto should rightly be the first person to qualify for both a Nobel prize in Economics and the Turing award.

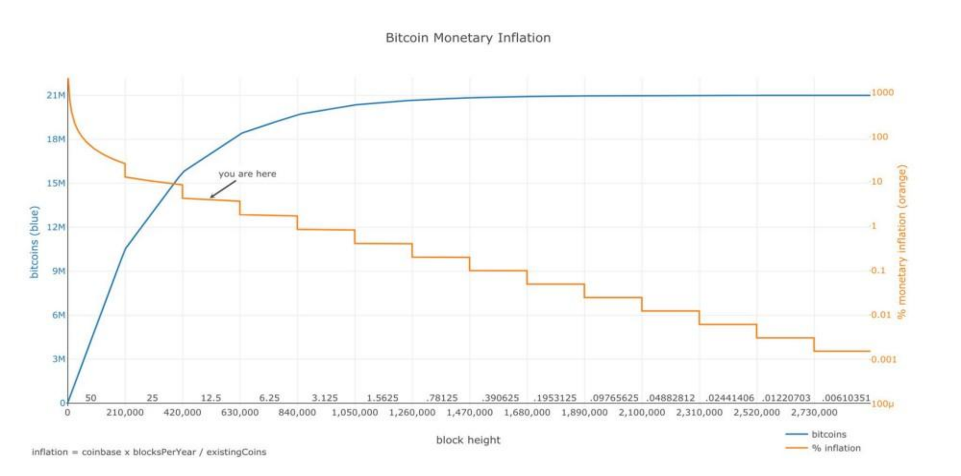


"A group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement."

-Pease, Shosthak and Lamport, The Byzantine Generals Problem

Scarce Digital Good

- Fixed predetermined rate of supply of 21 million bitcoins.
- 17.5 million already mined, only about 3.5 million supply left.
- Every 4 years production by mining halves.
- Currently each block produces 12.5 bitcoins.
- The last bitcoin will be mined in 2140.



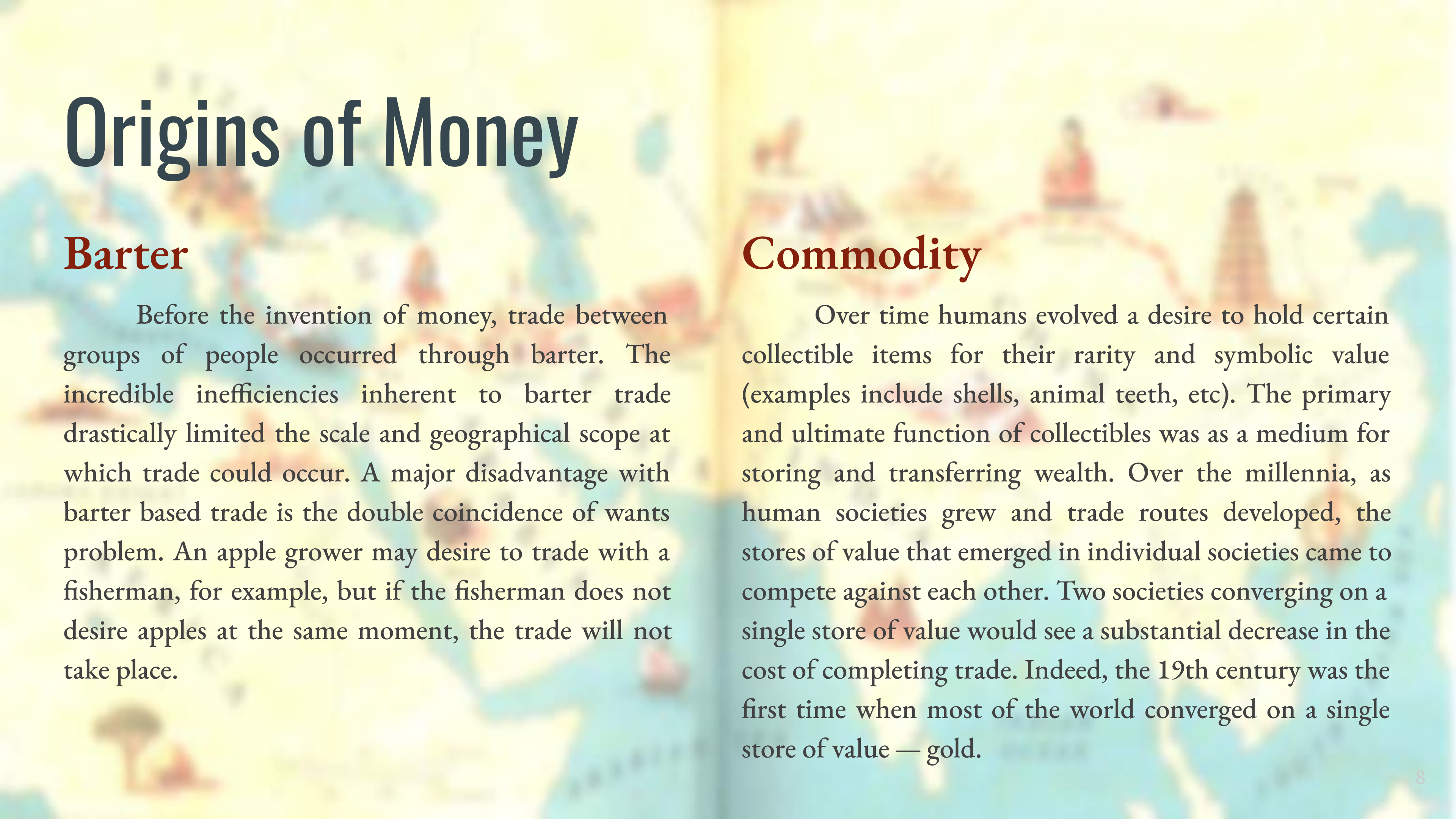
For an investor, the salient fact of the invention of Bitcoin is the creation of a new scarce digital good — bitcoins. Bitcoins are transferable digital tokens that are created on the Bitcoin network in a process known as “mining”. Bitcoin mining is roughly analogous to gold mining except that production follows a designed, predictable schedule.

Why does Bitcoin have any value?

Bitcoins are not backed by any physical commodity, nor are they guaranteed by any government or company, which raises the obvious question for a new bitcoin investor: why do they have any value at all?

Unlike stocks, bonds, real-estate or even commodities such as oil and wheat, bitcoins cannot be valued using standard discounted cash flow analysis or by demand for their use in the production of higher order goods.

Bitcoin falls into an entirely different category of goods, known as monetary goods whose value is set game theoretically, i.e. each market participant values the good based on their appraisal of whether and how much other participants will value it. To understand this we need to briefly explore the origins of money.



Origins of Money

Barter

Before the invention of money, trade between groups of people occurred through barter. The incredible inefficiencies inherent to barter trade drastically limited the scale and geographical scope at which trade could occur. A major disadvantage with barter based trade is the double coincidence of wants problem. An apple grower may desire to trade with a fisherman, for example, but if the fisherman does not desire apples at the same moment, the trade will not take place.

Commodity

Over time humans evolved a desire to hold certain collectible items for their rarity and symbolic value (examples include shells, animal teeth, etc). The primary and ultimate function of collectibles was as a medium for storing and transferring wealth. Over the millennia, as human societies grew and trade routes developed, the stores of value that emerged in individual societies came to compete against each other. Two societies converging on a single store of value would see a substantial decrease in the cost of completing trade. Indeed, the 19th century was the first time when most of the world converged on a single store of value — gold.

Attributes of a good store of value

When stores of value compete against each other, it is the specific attributes that make a good store of value that allows one to out-compete another at the margin and increase demand for it over time. While many goods have been used as stores of value or "proto-money", certain attributes emerged that were particularly demanded and allowed goods with these attributes to out-compete others:

- Durable: The good itself and it's value must not be perishable or easily destroyed.
- Divisible: It must be easy to subdivide to facilitate smaller and precise trades.
- Verifiable: It must be easy to quickly identify and verify its authenticity.
- Portable: It must be easy to transport and store, making it possible to secure against loss or theft and facilitate long-distance trade.
- Fungible: One specimen should be interchangeable with another of the same value. Without fungibility, the double coincidence of wants problem remains.
- Scarce: It must not be abundant or easy to either obtain or produce, as Nick Szabo termed it, "unforgeable costliness". Scarcity is perhaps the most important attribute.
- Established History: The longer the good is perceived to be valuable to society, the greater its appeal as a store of value.
- Censorship-resistant: A new attribute which has become increasingly important in our modern, digital society with pervasive surveillance. That is, how difficult it is for an external party such as a state or corporation to prevent an owner for the good from keeping and using it.

Comparing Bitcoin, Gold and Fiat as Store of Value

	Durable	Portable	Fungible	Verifiable	Divisible	Scarce	Established History	Censorship Resistant
Bitcoin	A	A+	A	A+	A+	A+	D	A
Gold	A+	D	A	B	C	A	A+	C
Fiat	C	B	B	B	B	F	C	D

- Durability: Gold is the king of durability. Most gold ever mined, remains extant today and will a 1000 years hence. Since a torn currency note can be exchanged for a new one, it is the durability of the issuing institute that matters. Many governments have come and gone with their currencies with them. It would be folly to consider them durable as every fiat currency was more valuable 20 years ago than today. Due to Bitcoin's decentralised and distributed ledger, despite nation-states attempting to regulate Bitcoin and years of attacks by hackers, the network has continued to function, displaying remarkable degree of "anti-fragility".

- Portability: Bitcoins are most portable store of value ever used by man. Private keys representing billions of dollars can be stored on a tiny USB and equally big transactions can be made across the world near instantly. Fiat currencies being fundamentally digital are also portable. However, government regulations and capital controls make certain transactions difficult, not possible or may take days. Gold is least portable as it is heavy and dense. Transporting it is slow, risky, costly and requires customs declarations if cross-border.

Bitcoin vs Gold vs Fiat

- Scarcity: The supply of bitcoins is fixed at 21 million. This gives the owner of bitcoins a known percentage of the total possible supply. An owner of 10 bitcoins knows that at most 2.1 million people on earth (less than 0.03% of the world's population) will ever have as many bitcoins as they had. Gold, while remaining quite scarce through history, is not immune to increases in supply (example seafloor mining). Finally, fiat currencies have proven to be prone to constant increases in supply. Nations-states have shown a persistent proclivity to inflate their money supply to solve short-term political problems. The inflationary tendencies of governments across the world leave the owner of a fiat currency with the likelihood that their savings will diminish in value over time.

- Divisibility: Bitcoins can be divided to a hundred millionth unit and transmitted at such infinitesimally small amounts. Fiat currencies are typically divisible down to pocket change, which has little purchasing power, making fiat divisible enough in practice. Gold, while physically divisible, is difficult to use when divided into small enough quantities for lower-value day-to-day trade.

Bitcoin vs Gold vs Fiat

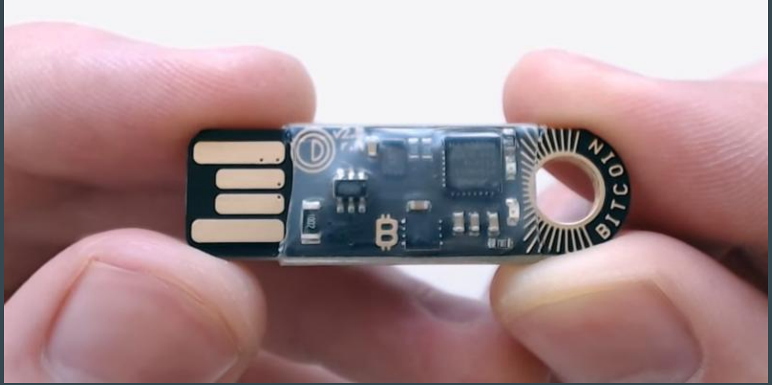
- Verifiability: Fiat & Gold are fairly easy to verify for authenticity. However, both are not immune to being counterfeited. Bitcoins, on the other hand, can be verified with mathematical certainty. Using cryptographic signatures, the owner of a bitcoin can publicly prove she owns the bitcoins she says she does.

- Fungibility: Gold is the standard for fungibility. When melted, every gram of gold is the same as every other gram. Fiat currencies, on the other hand, are only as fungible as the issuing institutions allow them to be, e.g. India's demonetization of 500 & 1000 rupee notes. Bitcoin is fungible at the network level. But because all transactions are public on the blockchain, though still very technical, with special precautions fungibility can be maintained.

- Established History: No monetary good has a history as long and storied as gold, which has been valued for as long as civilization has existed. Fiat currencies, a relatively recent anomaly of history, have had a near-universal tendency toward eventual worthlessness. Using inflation as an insidious means of invisibly taxing a citizenry have established that they cannot be trusted to maintain their value over time. Bitcoin, despite its short existence, has weathered enough trials in the market that there is a high likelihood it will not vanish as a valued asset any time soon. Furthermore, after growing stronger for more than a decade, the Lindy effect suggests that the longer Bitcoin remains in existence the greater society's confidence that it will continue to exist long into the future.

Bitcoin vs Gold vs Fiat

- Censorship Resistance: The key attribute that makes Bitcoin valuable for illicit activities is not because its anonymous, it is "permissionless" at the network level. No human decides which transaction should be allowed. Bitcoin, by its very nature, is designed to be censorship-resistant. This is in stark contrast to the fiat banking system, where states regulate banks and the other gatekeepers of money transmission to report and prevent outlawed uses of monetary goods. Although gold is not issued by states, its physical nature makes it difficult to transmit at distance, making it far more susceptible to state regulation than Bitcoin. India's Gold Control Act is an example of such regulation.



This tiny USB device can securely store bitcoins worth billions of dollars.

Bitcoin excels across the majority of attributes listed above, allowing it to outcompete modern and ancient monetary goods at the margin and providing a strong incentive for its increasing adoption. In particular, the potent combination of censorship resistance and absolute scarcity has been a powerful motivator for wealthy investors to allocate a portion of their wealth to the nascent asset class.

IMPLICATIONS

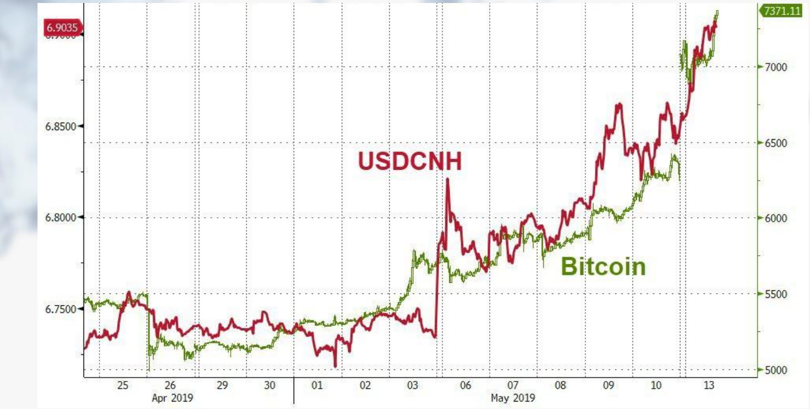
- **Cyprus:** 2013 - Cypriot Financial Crisis: Cyprus freezes all bank accounts, restricting all withdrawals and transfers of money. Cyprus faces greatest risk of stagflation and drop in Eurozone bank deposits (-€10B). Crisis introduces bitcoin to the world as an asset class immune to bail-ins and fiscal mismanagement; price of a bitcoin increases 10x.

- **Argentina:** 2013 - The Argentine government tightens capital controls, while inflation climbs to over 20% in June 2013. The spot price of bitcoin in Argentina is 38%higher than its spot price on global exchanges.

- **Venezuela:** 2015 - Inflation rose by 335% and reported 2059 btc were exchanged on localbitcoins a 983% rise over 2014 volumes(190). 2016 - With inflation @ 500%, 8624 btc traded, a 319% rise over 2015. 2017 - 21,556 btc traded, a 150% rise over 2016.

- **India:** November, 2016 - After the demonetization speech the price of bitcoins in india surged by about 50% with more than 300 btc traded a day. Thousands of bitcoins were bought by people across India to safeguard their money.

- **US-China:** May, 2019 - US-China trade war, btc rose 15% in a single day as people scrambled to save their wealth with the free fall of Yuan.



Soure: Zerohedge

Why only Bitcoin and not any other cryptocurrency?

There are about 1,000 cryptocurrencies with more than 1 transaction/day. So why only Bitcoin?

- Over 60 million holders of Bitcoin.
- Over $1 billion transaction value/day.
- Bitcoin miner fees are 8 times higher than all the cryptocurrencies combined.
- With over 1 million new holders/month, Bitcoin will add more users in the next 5 months than all cryptocurrencies in their combined history.
- The most important metric of all, though, is how much can we trust these platforms or how sovereign they are. We measure it as the square of the computing power they have. If we use electricity consumption as a proxy for computing power then all those 1000 cryptocurrencies combined have less than 1% of the Bitcoin’s processing (mining) power, so none of them is really sovereign and in many cases their code is controlled by a person or a small group of people.

Bitcoin, the Protocol

Bitcoin is an open protocol, not a company. In the history of companies there is a lot of change, disruption and churn (Microsoft-Apple, eBay-Amazon, Altavista-Google, MySpace-Facebook, etc.). However, protocols are very different. Once a protocol gets established it almost never changes. For example, we use IP (Internet Protocol, or just “the Internet” colloquially) for almost all transport of data (until 90s cisco routers used to route dozens of protocols, but now only route IP). We are using only one web protocol and only one email protocol.

Once a protocol gets established it becomes the only protocol for that use case and it is not possible to displace it with a better protocol. Right now, it looks like the standard protocol for a sovereign platform will be the Bitcoin.

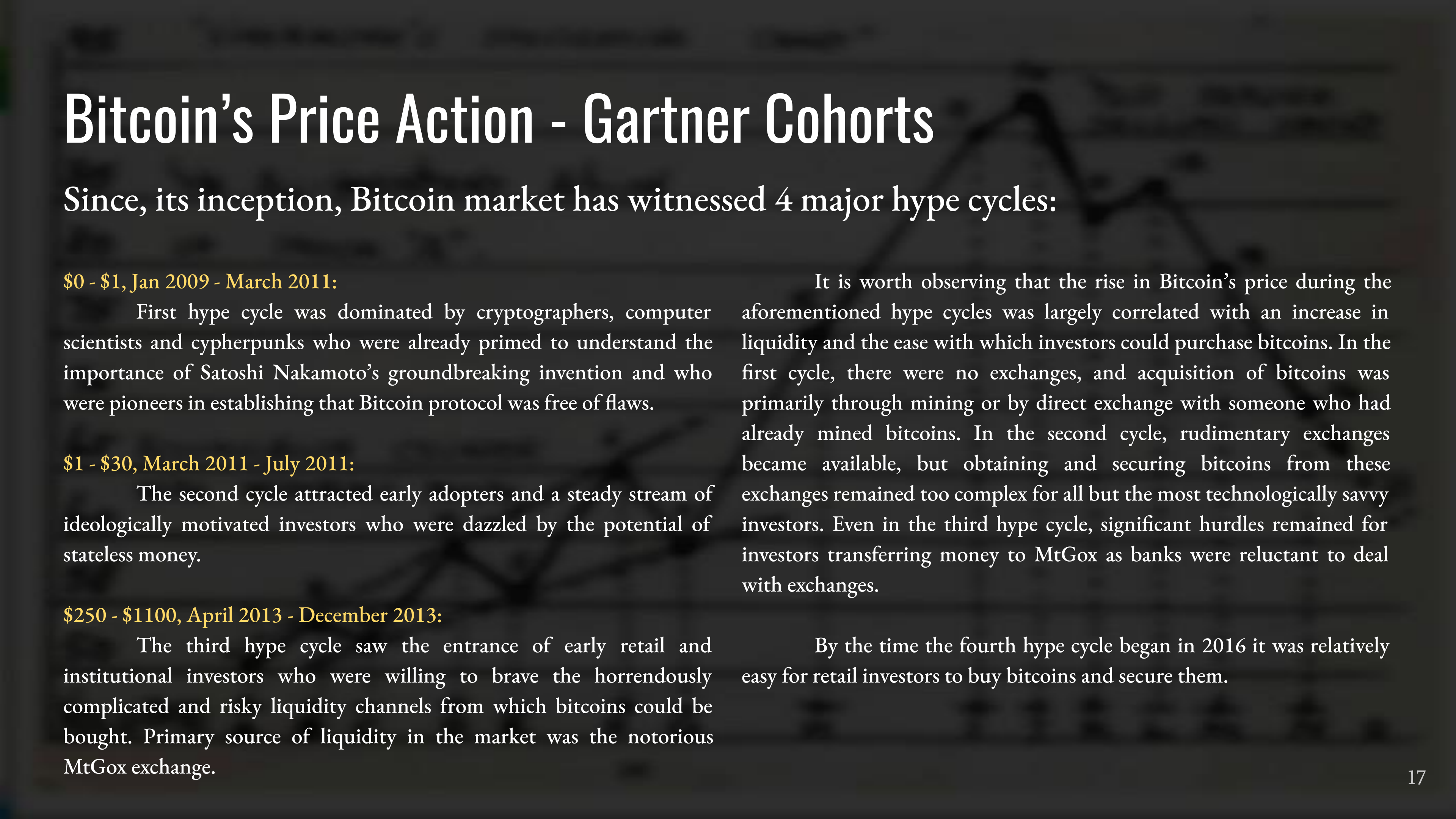
Many interesting technologies and applications are being implemented on top of Bitcoin. The Bitcoin blockchain is limited in that it can only process approximately 3,000 transactions every 10 minutes.

Lightning Network takes advantage of the robustness of the Bitcoin blockchain and works as a “Layer 2” solution on top of Bitcoin, enabling thousands of transactions/second of as little as 1 satoshi ($0.00008), for free and in real time.

RSK which enables the full functionality of Ethereum but on top of the much more robust Bitcoin, using it as settlement layer.

Liquid is an open source wholesale settlement network developed by Blockstream that operates on top of the Bitcoin blockchain.

Bitcoin’s Price Action - Gartner Cohorts



Since, its inception, Bitcoin market has witnessed 4 major hype cycles:

$0 - $1, Jan 2009 - March 2011:

First hype cycle was dominated by cryptographers, computer scientists and cypherpunks who were already primed to understand the importance of Satoshi Nakamoto’s groundbreaking invention and who were pioneers in establishing that Bitcoin protocol was free of flaws.

$1 - $30, March 2011 - July 2011:

The second cycle attracted early adopters and a steady stream of ideologically motivated investors who were dazzled by the potential of stateless money.

$250 - $1100, April 2013 - December 2013:

The third hype cycle saw the entrance of early retail and institutional investors who were willing to brave the horrendously complicated and risky liquidity channels from which bitcoins could be bought. Primary source of liquidity in the market was the notorious MtGox exchange.

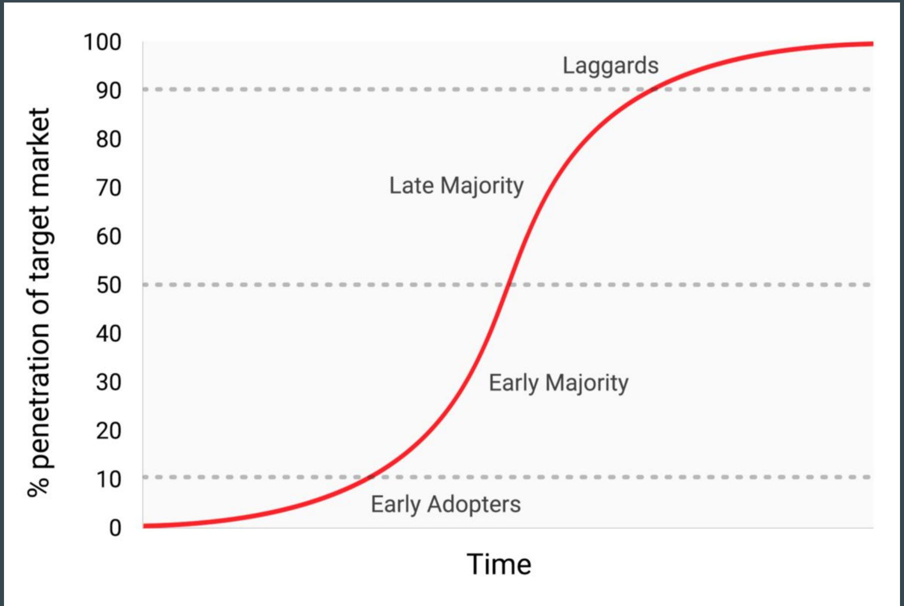
It is worth observing that the rise in Bitcoin’s price during the aforementioned hype cycles was largely correlated with an increase in liquidity and the ease with which investors could purchase bitcoins. In the first cycle, there were no exchanges, and acquisition of bitcoins was primarily through mining or by direct exchange with someone who had already mined bitcoins. In the second cycle, rudimentary exchanges became available, but obtaining and securing bitcoins from these exchanges remained too complex for all but the most technologically savvy investors. Even in the third hype cycle, significant hurdles remained for investors transferring money to MtGox as banks were reluctant to deal with exchanges.

By the time the fourth hype cycle began in 2016 it was relatively easy for retail investors to buy bitcoins and secure them.

The 4th Gartner Hype Cycle of Bitcoin

$1100 - $19,700, December 2013 - December 2017:

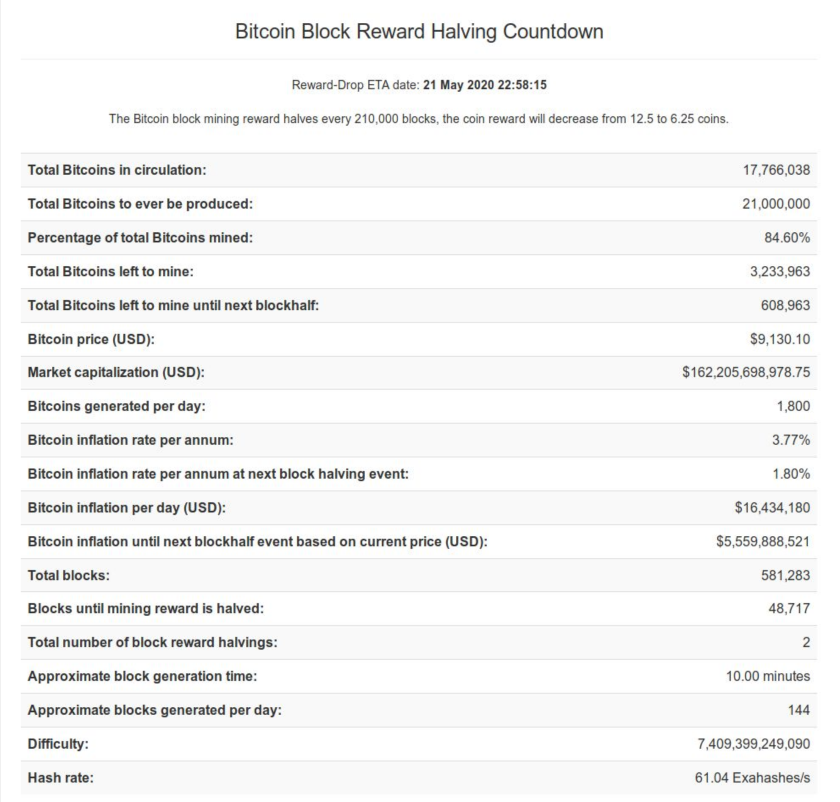
This is the cycle when Bitcoin became mainstream. Participation in the current hype cycle has been dominated by what Michael Casey described as the “early majority” of retail and institutional investors. As sources of liquidity have deepened and matured, major institutional investors now have the opportunity to participate through regulated futures markets. The availability of a regulated futures market paves the way for the creation of a Bitcoin ETF, which will then usher in the “late majority” and “laggards” in subsequent hype cycles.



The Current Gartner Hype Cycle

Currently we are at the beginning of the fifth major hype cycle. Although it is impossible to predict the exact magnitude of the current cycle, it would be reasonable to conjecture that the cycle reaches its zenith in the range of $80,000 to $130,000.

Much higher than this range and Bitcoin would command a significant fraction of gold's entire market capitalization (gold and Bitcoin would have equivalent market capitalizations at a bitcoin price of approximately $393,000 at the time of writing). A significant fraction of gold's market capitalization comes from central bank demand and it's unlikely that central banks or nation states will participate in this particular hype cycle.



Bitcoin Block Reward Halving Countdown

Reward-Drop ETA date: **21 May 2020 22:58:15**

The Bitcoin block mining reward halves every 210,000 blocks, the coin reward will decrease from 12.5 to 6.25 coins.

Total Bitcoins in circulation:	17,766,038
Total Bitcoins to ever be produced:	21,000,000
Percentage of total Bitcoins mined:	84.60%
Total Bitcoins left to mine:	3,233,963
Total Bitcoins left to mine until next blockhalf:	608,963
Bitcoin price (USD):	$9,130.10
Market capitalization (USD):	$162,205,698,978.75
Bitcoins generated per day:	1,800
Bitcoin inflation rate per annum:	3.77%
Bitcoin inflation rate per annum at next block halving event:	1.80%
Bitcoin inflation per day (USD):	$16,434,180
Bitcoin inflation until next blockhalf event based on current price (USD):	$5,559,888,521
Total blocks:	581,283
Blocks until mining reward is halved:	48,717
Total number of block reward halvings:	2
Approximate block generation time:	10.00 minutes
Approximate blocks generated per day:	144
Difficulty:	7,409,399,249,090
Hash rate:	61.04 Exahashes/s

Bitcoin blockchain stats at the time of writing. Source: bitcoinblockhalf.com

Enter Nation States

Bitcoin's final Gartner hype cycle will begin when nation-states start accumulating it as a part of their foreign currency reserves. The market capitalization of Bitcoin is currently too small for it to be considered a viable addition to reserves for most countries. However, as private sector interest increases and the capitalization of Bitcoin approaches 1 trillion dollars it will become liquid enough for most states to enter the market. The entrance of the first state to officially add bitcoins to their reserves will likely trigger a stampede for others to do so. The states that are the earliest in adopting Bitcoin would see the largest benefit to their balance sheets if Bitcoin ultimately became a global reserve currency.

However, it will not come about without resistance from the same nation states. The banking industry and the US Federal Reserve are finally having their first inkling of the existential threat Bitcoin poses to US monetary policy if it were to become a global reserve currency.

> *There is another danger, perhaps even more serious from the point of view of the central banks and regulators: bitcoin might not crash. If the speculative fervor in the cryptocurrency is merely the precursor to it being widely used as an alternative to the dollar, it will threaten the central banks' monopoly on money.*

Wall Street Journal published a commentary on the threat Bitcoin poses to US monetary policy

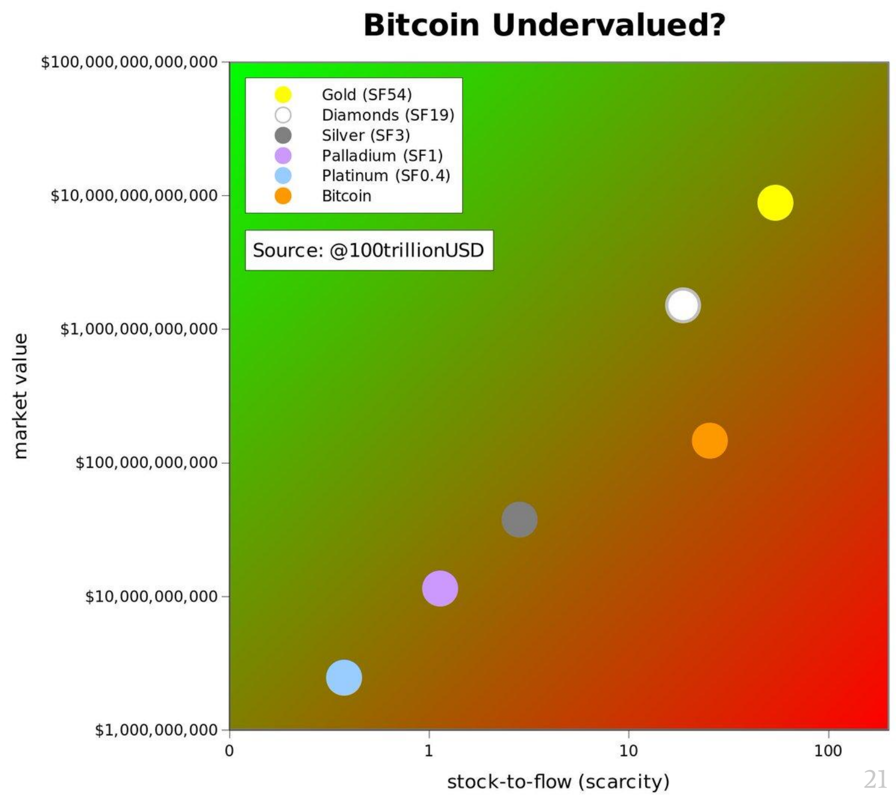
In the coming years there will be a great struggle between entrepreneurs and innovators across the world, who will attempt to keep Bitcoin free of state control, and the banking industry and central banks who will do everything in their power to regulate Bitcoin to prevent their industry and money-issuing powers from being disrupted. Congressman Brad Sherman recently called for a ban on Bitcoin and other cryptocurrencies[1], the effect on bitcoin has only been positive as bitcoin price increased by 50% within minutes.

[1] Video of Mr. Sherman's hearing in the Senate.

The Case for small allocation to Bitcoin

Bitcoin is a fascinating experiment but it is still just that: an experiment. It still has a chance of failing. But after 10 years of infrastructure development and uninterrupted functioning, with more than 60 million holders, adding more than 1 million new holders every month and moving more than $1 billion every day worldwide, it has a good chance of succeeding.

If Bitcoin does succeed, 1 Bitcoin will at least be worth $2 million in 7 to 10 years. That is 250 times what it is worth today (at the time of writing the price of Bitcoin is ~ $8,400).

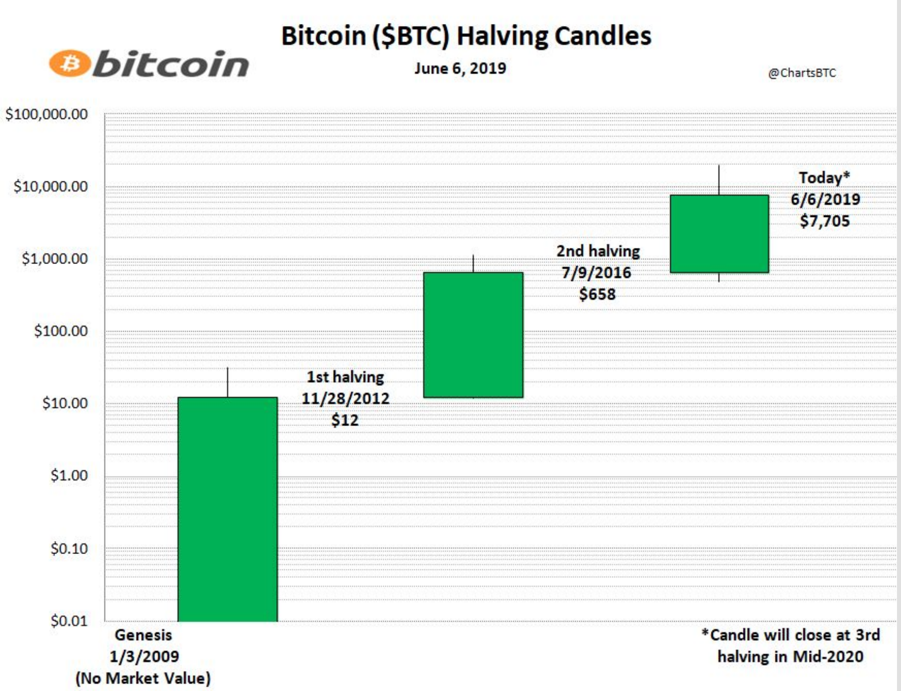


Source: @100trillionUSD

The Case for small allocation to Bitcoin

In today's world where every asset seems priced for perfection, it is hard, if not impossible, to find an asset that is so mispriced and where the possible outcomes are so asymmetrical. The current state of Bitcoin is similar to the state of the Internet in 1992. Back then, Internet was very nascent and experimental. Just like the Internet, Bitcoin offers a unique opportunity for a non-material exposure to produce a material outcome.

It is reasonable to assert that the long term risk-reward ratio of Bitcoin is currently most favorable of any liquid investment in the world.



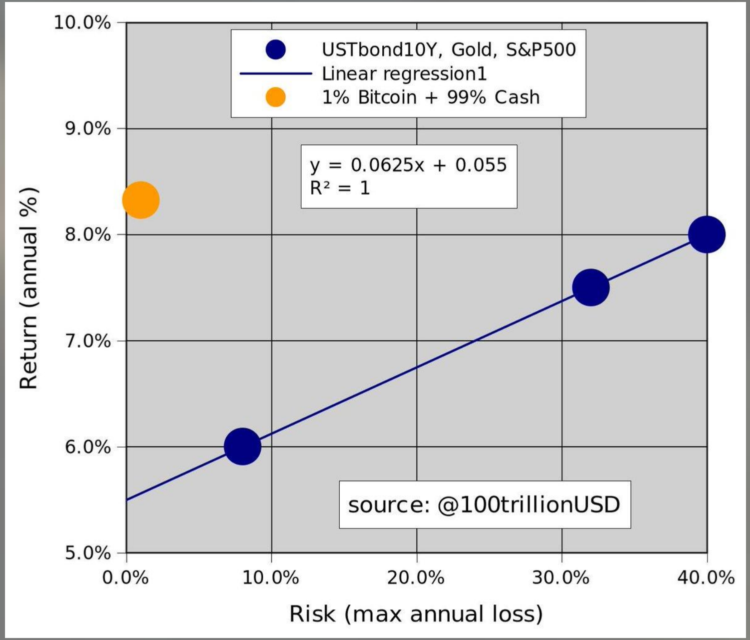
Source: @ChartsBtc

The Case for small allocation to Bitcoin

In a world where Bitcoin succeeds, it will most likely be a supranational currency that exists on top of all national currencies. It may be a global non-political standard of value and settlement. All currencies may be quoted in satoshis (the smallest fraction of a Bitcoin). When your granddaughter asks what is the price of Indian Rupees she may receive an answer in satoshis: it is 25 satoshis today. US Dollars? 52 satoshis. A barrel of oil? 4,200 satoshis. Global GDP? 9,666,666 bitcoins.

The stage is set for mass market adoption in the coming 5 years. In our assessment, during this phase (its "Windows moment") Bitcoin will become widely recognized as a portfolio hedging instrument and reserve asset.

Source: @100trillionUSD



A $10 million portfolio if invests $1,00,000 (1%) will lose at most 1% of its value over 3 to 5 years, which most portfolios can bear if Bitcoin fails. But, if Bitcoin succeeds, in 7 to 10 years those $1,00,00 may be worth more than $25 million, more than twice the value of the entire initial portfolio.

Acknowledgements

This presentation is made as an education tool and would not have been possible without the insights of the following people's work which this is based on. I am grateful for their work which has helped me understand bitcoin better and hope it helps you too. For further reading I'd urge you to make use of the following resources:

- The Bullish Case for Bitcoin, by Vijay Boyapati
- The Case for Small allocation to Bitcoin, by Wences Caseres

Other great resources:

- The Bitcoin Standard, by Saifedean Ammous
- The Bitcoin Whitepaper, by Satoshi Nakamoto
- The Bitcoin Wiki

- @jodobear