

The Bullish Case for Bitcoin

By Vijay Boyapati

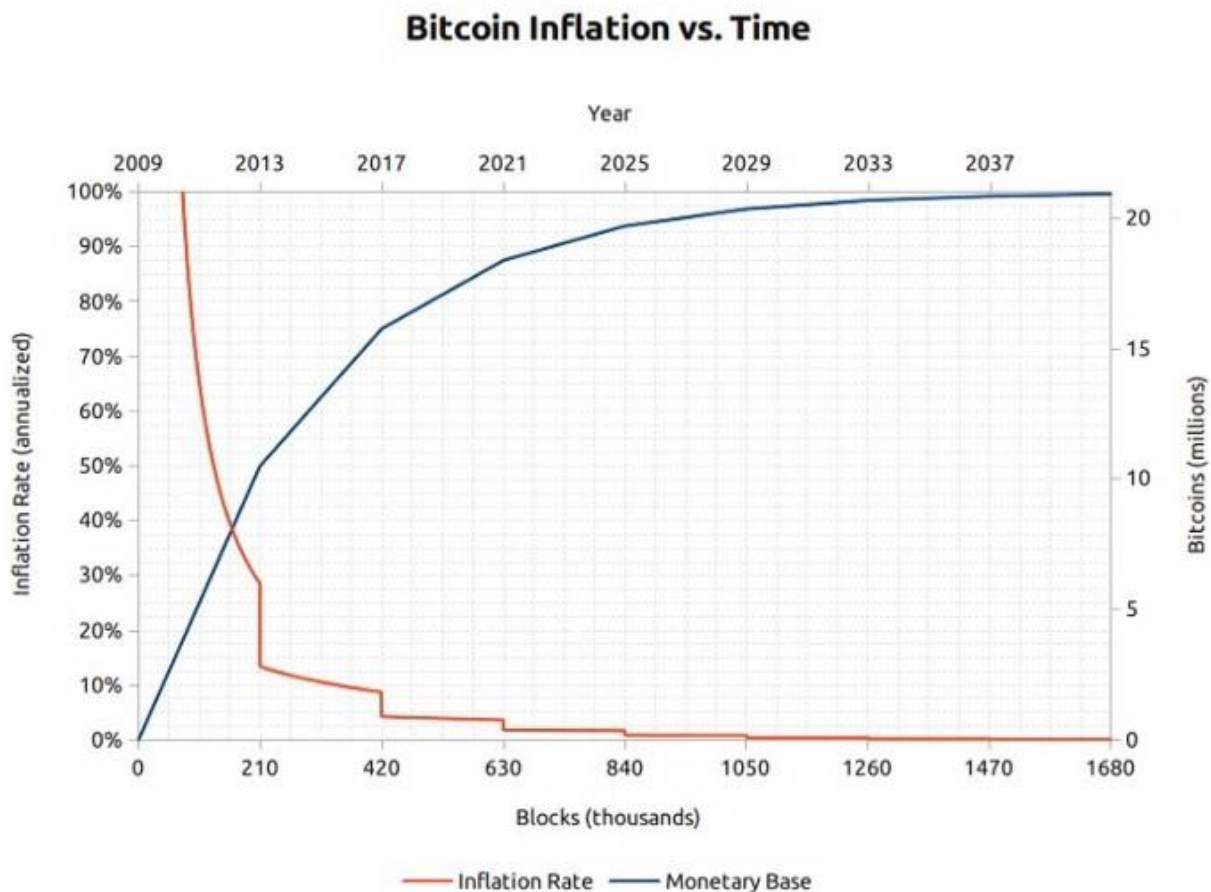
Posted March 2, 2018

With the price of a bitcoin surging to new highs in 2017, the bullish case for investors might seem so obvious it does not need stating. Alternatively, it may seem foolish to invest in a digital asset that isn't backed by any commodity or government and whose price rise has prompted some to compare it to the tulip mania or the dot-com bubble. Neither is true; the bullish case for Bitcoin is compelling but far from obvious. There are significant risks to investing in Bitcoin, but, as I will argue, there is still an immense opportunity.

Genesis

Never in the history of the world had it been possible to transfer value between distant peoples without relying on a trusted intermediary, such as a bank or government. In 2008 Satoshi Nakamoto, whose identity is still unknown, 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.

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. By design, only 21 million bitcoins will ever be mined and most of these already have been — approximately 16.8 million bitcoins have been mined at the time of writing. Every four years the number of bitcoins produced by mining halves and the production of new bitcoins will end completely by the year 2140.



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. Bitcoins fall 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 the game-theoretic nature of monetary goods, we need to explore the origins of money.

The Origins of Money

In the earliest human societies, 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 trade with a fisherman, for example, but if the fisherman does not desire apples at the

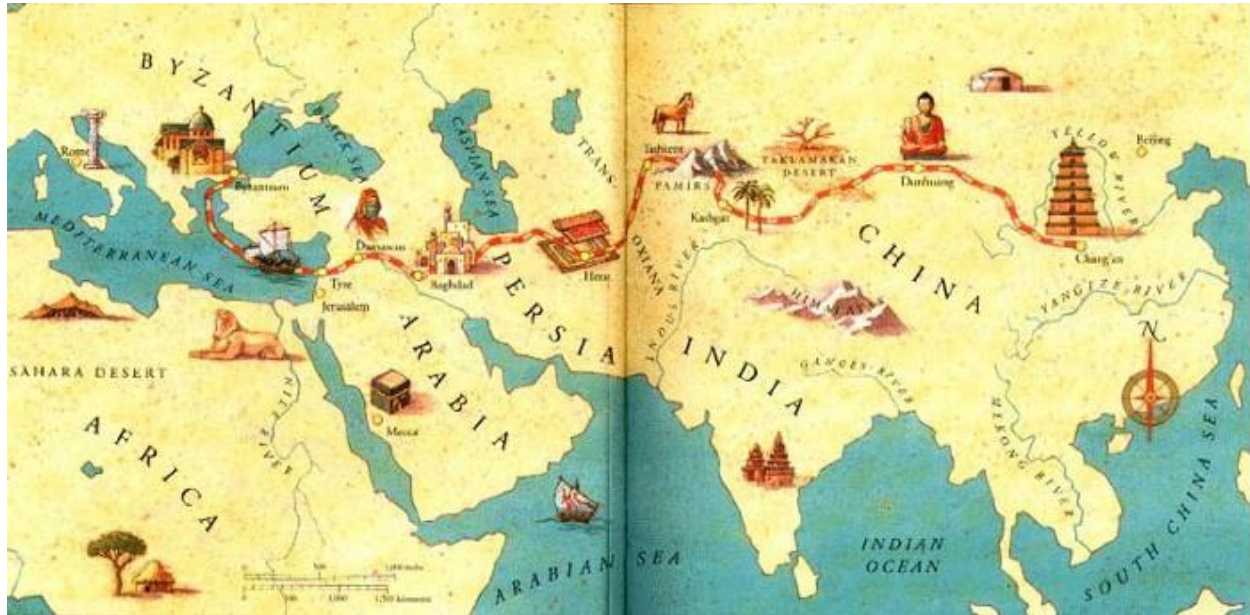
same moment, the trade will not take place. Over time humans evolved a desire to hold certain collectible items for their rarity and symbolic value (examples include shells, animal teeth and flint). Indeed, as Nick Szabo argues in his brilliant [essay on the origins of money](#), the human desire for collectibles provided a distinct evolutionary advantage for early man over his nearest biological competitors, *Homo neanderthalensis*.

The primary and ultimate evolutionary function of collectibles was as a medium for storing and transferring wealth.

Collectibles served as a sort of “proto-money” by making trade possible between otherwise antagonistic tribes and by allowing wealth to be transferred between generations. Trade and transfer of collectibles were quite infrequent in paleolithic societies, and these goods served more as a “store of value” rather than the “medium of exchange” role that we largely recognize modern money to play. Szabo explains:

Compared to modern money, primitive money had a very low velocity — it might be transferred only a handful of times in an average individual's lifetime. Nevertheless, a durable collectible, what today we would call an heirloom, could persist for many generations and added substantial value at each transfer — often making the transfer even possible at all.

Early man faced an important game-theoretic dilemma when deciding which collectibles to gather or create: which objects would be desired by other humans? By correctly anticipating which objects might be demanded for their collectible value, a tremendous benefit was conferred on the possessor in their ability to complete trade and to acquire wealth. Some Native American tribes, such as the Narragansetts, specialized in the manufacture of otherwise useless collectibles simply for their value in trade. It is worth noting that the earlier the anticipation of future demand for a collectible good, the greater the advantage conferred to its possessor; it can be acquired more cheaply than when it is widely demanded and its trade value appreciates as the population which demands it expands. Furthermore, acquiring a good in hopes that it will be demanded as a future store of value hastens its adoption for that very purpose. This seeming circularity is actually a feedback loop that drives societies to quickly converge on a single store of value. In game-theoretic terms, this is known as a “[Nash Equilibrium](#)”. Achieving a Nash Equilibrium for a store of value is a major boon to any society, as it greatly facilitates trade and the division of labor, paving the way for the advent of civilization.



Over the millennia, as human societies grew and trade routes developed, the stores of value that had emerged in individual societies came to compete against each other. Merchants and traders would face a choice of whether to save the proceeds of their trade in the store of value of their own society or the store of value of the society they were trading with, or some balance of both. The benefit of maintaining savings in a foreign store of value was the enhanced ability to complete trade in the associated foreign society. Merchants holding savings in a foreign store of value also had an incentive to encourage its adoption within their own society, as this would increase the purchasing power of their savings. The benefits of an imported store of value accrued not only to the merchants doing the importing, but also to the societies themselves. Two societies converging on a single store of value would see a substantial decrease in the cost of completing trade with each other and an attendant increase in trade-based wealth. Indeed, the 19th century was the first time when most of the world converged on a single store of value — gold — and this period saw the greatest explosion of trade in the history of the world. Of this halcyon period, Lord Keynes wrote:

What an extraordinary episode in the economic progress of man that age was ... for any man of capacity or character at all exceeding the average, into the middle and upper classes, for whom life offered, at a low cost and with the least trouble, conveniences, comforts, and amenities beyond the compass of the richest and most powerful monarchs of other ages. The inhabitant of London could order by telephone, sipping his morning tea in bed, the various products of the whole earth, in such quantity as he might see fit, and reasonably expect their early delivery upon his doorstep

The 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. An ideal store of value will be:

- **Durable:** the good must not be perishable or easily destroyed. Thus wheat is not an ideal store of value
- **Portable:** the good must be easy to transport and store, making it possible to secure it against loss or theft and allowing it to facilitate long-distance trade. A cow is thus less ideal than a gold bracelet.
- **Fungible:** one specimen of the good should be interchangeable with another of equal quantity. Without fungibility, the coincidence of wants problem remains unsolved. Thus gold is better than diamonds, which are irregular in shape and quality.
- **Verifiable:** the good must be easy to quickly identify and verify as authentic. Easy verification increases the confidence of its recipient in trade and increases the likelihood a trade will be consummated.
- **Divisible:** the good must be easy to subdivide. While this attribute was less important in early societies where trade was infrequent, it became more important as trade flourished and the quantities exchanged became smaller and more precise.
- **Scarce:** As Nick Szabo termed it, a monetary good must have “unforgeable costliness”. In other words, the good must not be abundant or easy to either obtain or produce in quantity. Scarcity is perhaps the most important attribute of a store of value as it taps into the innate human desire to collect that which is rare. It is the source of the original value of the store of value.
- **Established history:** the longer the good is perceived to have been valuable by society, the greater its appeal as a store of value. A long-established store of value will be hard to displace by a new upstart except by force of conquest or if the arriviste is endowed with a significant advantage among the other attributes listed above.
- **Censorship-resistant:** a new attribute, which has become increasingly important in our modern, digital society with pervasive surveillance, is censorship-resistance. That is, how difficult is it for an external party such as a corporation or state to prevent the owner of the good from keeping and using it. Goods that are censorship-resistant are ideal to those living under regimes that are trying to enforce capital controls or to outlaw various forms of peaceful trade.

The table below grades Bitcoin, gold and fiat money (such as dollars) against the attributes listed above and is followed by an explanation of each grade:

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

Durability:

Gold is the undisputed King of durability. The vast majority of gold that has ever been mined or minted, including the gold of the Pharaohs, remains

extant today and will likely be available a thousand years hence. Gold coins that were used as money in antiquity still maintain significant value today. Fiat currency and bitcoins are fundamentally digital records that may take physical form (such as paper bills). Thus it is not their physical manifestation whose durability should be considered (since a tattered dollar bill may be exchanged for a new one), but the durability of the institution that issues them. In the case of fiat currencies, many governments have come and gone over the centuries, and their currencies disappeared with them. The Papiermark, Rentenmark and Reichsmark of the Weimar Republic no longer have value because the institution that issued them no longer exists. If history is a guide, it would be folly to consider fiat currencies durable in the long term — the US dollar and British Pound are relative anomalies in this regard. Bitcoins, having no issuing authority, may be considered durable so long as the network that secures them remains in place. Given that Bitcoin is still in its infancy, it is too early to draw strong conclusions about its durability. However, there are encouraging signs that, despite prominent instances of nation-states attempting to regulate Bitcoin and years of attacks by hackers, the network has continued to function, displaying a remarkable degree of “anti-fragility”.

Portability:

Bitcoins are the most portable store of value ever used by man. Private keys representing hundreds of millions of dollars can be stored on a tiny USB drive and easily carried anywhere. Furthermore, equally valuable sums can be transmitted between people on opposite ends of the earth near instantly. Fiat currencies, being fundamentally digital, are also highly portable. However, government regulations and capital controls mean that large transfers of value usually take days or may not be possible at all. Cash can be used to avoid capital controls, but then the risk of storage and cost of transportation become significant. Gold, being physical in form and incredibly dense, is by far the least portable. It is no wonder that the majority of bullion is never transported. When bullion is transferred between a buyer and a seller it is typically only the title to the gold that is transferred, not the physical bullion itself. Transmitting physical gold across large distances is costly, risky and time-consuming.

Fungibility:

Gold provides the standard for fungibility. When melted down, an ounce of gold is essentially indistinguishable from any other ounce, and gold has always traded this way on the market. Fiat currencies, on the other hand, are only as fungible as the issuing institutions allow them to be. While it may be the case that a fiat banknote is usually treated like any other by merchants accepting them, there are instances where large-denomination notes have been treated differently to small ones. For instance, India's government, in an

attempt to stamp out India's untaxed gray market, completely demonetized their 500 and 1000 rupee banknotes. The demonetization caused 500 and 1000 rupee notes to trade at a discount to their face value, making them no longer truly fungible with their lower denomination sibling notes. Bitcoins are fungible at the network level, meaning that every bitcoin, when transmitted, is treated the same on the Bitcoin network. However, because bitcoins are traceable on the blockchain, a particular bitcoin may become tainted by its use in illicit trade and merchants or exchanges may be compelled not to accept such tainted bitcoins. Without improvements to the privacy and anonymity of Bitcoin's network protocol, bitcoins cannot be considered as fungible as gold.

Verifiability:

For most intents and purposes, both fiat currencies and gold are fairly easy to verify for authenticity. However, despite providing features on their banknotes to prevent counterfeiting, nation-states and their citizens still face the potential to be duped by counterfeit bills. Gold is also not immune from being counterfeited. Sophisticated criminals have used gold-plated tungsten as a way of fooling gold investors into paying for false gold. 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.

Divisibility:

Bitcoins can be divided down to a hundred millionth of a bitcoin and transmitted at such infinitesimal amounts (network fees can, however, make transmission of tiny amounts uneconomic). Fiat currencies are typically divisible down to pocket change, which has little purchasing power, making fiat divisible enough in practice. Gold, while physically divisible, becomes difficult to use when divided into small enough quantities that it could be useful for lower-value day-to-day trade.

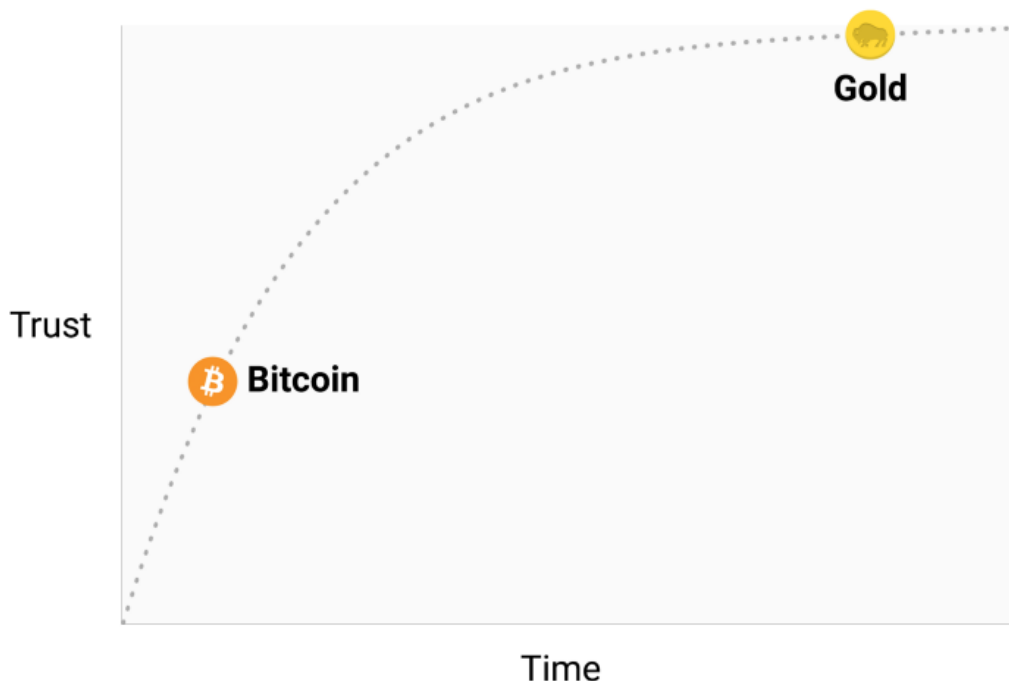
Scarcity:

The attribute that most clearly distinguishes Bitcoin from fiat currencies and gold is its predetermined scarcity. By design, at most 21 million bitcoins can ever be created. This gives the owner of bitcoins a known percentage of the total possible supply. For instance, an owner of 10 bitcoins would know that at most 2.1 million people on earth (less than 0.03% of the world's population) could ever have as many bitcoins as they had. Gold, while remaining quite scarce through history, is not immune to increases in supply. If it were ever the case that a new method of mining or acquiring gold became economic, the supply of gold could rise dramatically (examples include sea-floor or asteroid mining). Finally, fiat currencies, while only a relatively recent

invention of history, 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.

Established history:

No monetary good has a history as long and storied as gold, which has been valued for as long as human civilization has existed. Coins minted in the distant days of antiquity still maintain significant value today. The same cannot be said of fiat currencies, which are a relatively recent anomaly of history. From their inception, fiat currencies have had a near-universal tendency toward eventual worthlessness. The use of inflation as an insidious means of invisibly taxing a citizenry has been a temptation that few states in history have been able to resist. If the 20th century, in which fiat monies came to dominate the global monetary order, established any economic truth, it is that fiat money cannot be trusted to maintain its value over the long or even medium term. 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, 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. In other words, the societal trust of a new monetary good is asymptotic in nature, as is illustrated in the graph below:



If Bitcoin exists for 20 years, there will be near-universal confidence that it will be available forever, much as people believe the Internet is a permanent feature of the modern world.

Censorship resistance:

One of the most significant sources of early demand for bitcoins was their use in the illicit drug trade. Many subsequently surmised, mistakenly, that the primary demand for bitcoins was due to their ostensible anonymity. Bitcoin, however, is far from an anonymous currency; every transaction transmitted on the Bitcoin network is forever recorded on a public blockchain. The historical record of transactions allows for later forensic analysis to identify the source of a flow of funds. It was such an analysis that led to the apprehending of a perpetrator of the infamous MtGox heist. While it is true that a sufficiently careful and diligent person can conceal their identity when using Bitcoin, this is not why Bitcoin was so popular for trading drugs. The key attribute that makes Bitcoin valuable for proscribed activities is that it is “permissionless” at the network level. When bitcoins are transmitted on the Bitcoin network, there is no human intervention deciding whether the transaction should be allowed. As a distributed peer-to-peer network, Bitcoin is, by its very nature, 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. A classic example of regulated money transmission is capital controls. A wealthy millionaire, for instance, may find it very hard to transfer their wealth to a new domicile if they wish to flee an oppressive regime. 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.

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.

The Evolution of Money

There is an obsession in modern monetary economics with the medium of exchange role of money. In the 20th century, states have monopolized the issuance of money and continually undermined its use as a store of value, creating a false belief that money is primarily defined as a medium of exchange. Many have criticized Bitcoin as being an unsuitable money because its price has been too volatile to be suitable as a medium of

exchange. This puts the cart before the horse, however. Money has always evolved in stages, with the store of value role preceding the medium of exchange role. One of the fathers of marginalist economics, William Stanley Jevons, explained that:

Historically speaking ... gold seems to have served, firstly, as a commodity valuable for ornamental purposes; secondly, as stored wealth; thirdly, as a medium of exchange; and, lastly, as a measure of value.

Using modern terminology, money always evolves in the following four stages:

1. **Collectible.** In the very first stage of its evolution, money will be demanded solely based on its peculiar properties, usually becoming a whim of its possessor. Shells, beads and gold were all collectibles before later transitioning to the more familiar roles of money.
2. **Store of value:** Once it is demanded by enough people for its peculiarities, money will be recognized as a means of keeping and storing value over time. As a good becomes more widely recognized as a suitable store of value, its purchasing power will rise as more people demand it for this purpose. The purchasing power of a store of value will eventually plateau when it is widely held and the influx of new people desiring it as a store of value dwindles.
3. **Medium of exchange:** When money is fully established as a store of value, its purchasing power will stabilize. Having stabilized in purchasing power, the opportunity cost of using money to complete trades will diminish to a level where it is suitable for use as a medium of exchange. In the earliest days of Bitcoin, many people did not appreciate the huge opportunity cost of using bitcoins as a medium of exchange, rather than as an incipient store of value. The famous story of a man trading 10,000 bitcoins (worth approximately \$94 million at the time of this article's writing) for two pizzas illustrates this confusion.
4. **Unit of account.** When money is widely used as a medium of exchange, goods will be priced in terms of it. I.e., the exchange ratio against money will be available for most goods. It is a common misconception that bitcoin prices are available for many goods today. For example, while a cup of coffee might be available for purchase using bitcoins, the price listed is not a true bitcoin price; rather it is the dollar price desired by the merchant translated into bitcoin terms at the current USD/BTC market exchange rate. If the price of bitcoin were to drop in dollar terms, the number of bitcoins requested by the merchant would increase commensurately. Only when merchants are willing to accept bitcoins for payment without regard to the bitcoin

exchange rate against fiat currencies can we truly think of Bitcoin as having become a unit of account.

Monetary goods that are not yet a unit of account may be thought of as being “partly monetized”. Today gold fills such a role, being a store of value but having been stripped of its medium of exchange and unit of account roles by government intervention. It is also possible that one good fills the medium of exchange role of money while another good fills the other roles. This is typically true in countries with dysfunctional states, such as Argentina or Zimbabwe. In his book *Digital Gold*, Nathaniel Popper writes:

In America, the dollar seamlessly serves the three functions of money: providing a medium of exchange, a unit for measuring the cost of goods, and an asset where value can be stored. In Argentina, on the other hand, while the peso was used as a medium of exchange — for daily purchases — no one used it as a store of value. Keeping savings in the peso was equivalent to throwing away money. So people exchanged any pesos they wanted to save for dollars, which kept their value better than the peso. Because the peso was so volatile, people usually remembered prices in dollars, which provided a more reliable unit of measure over time.

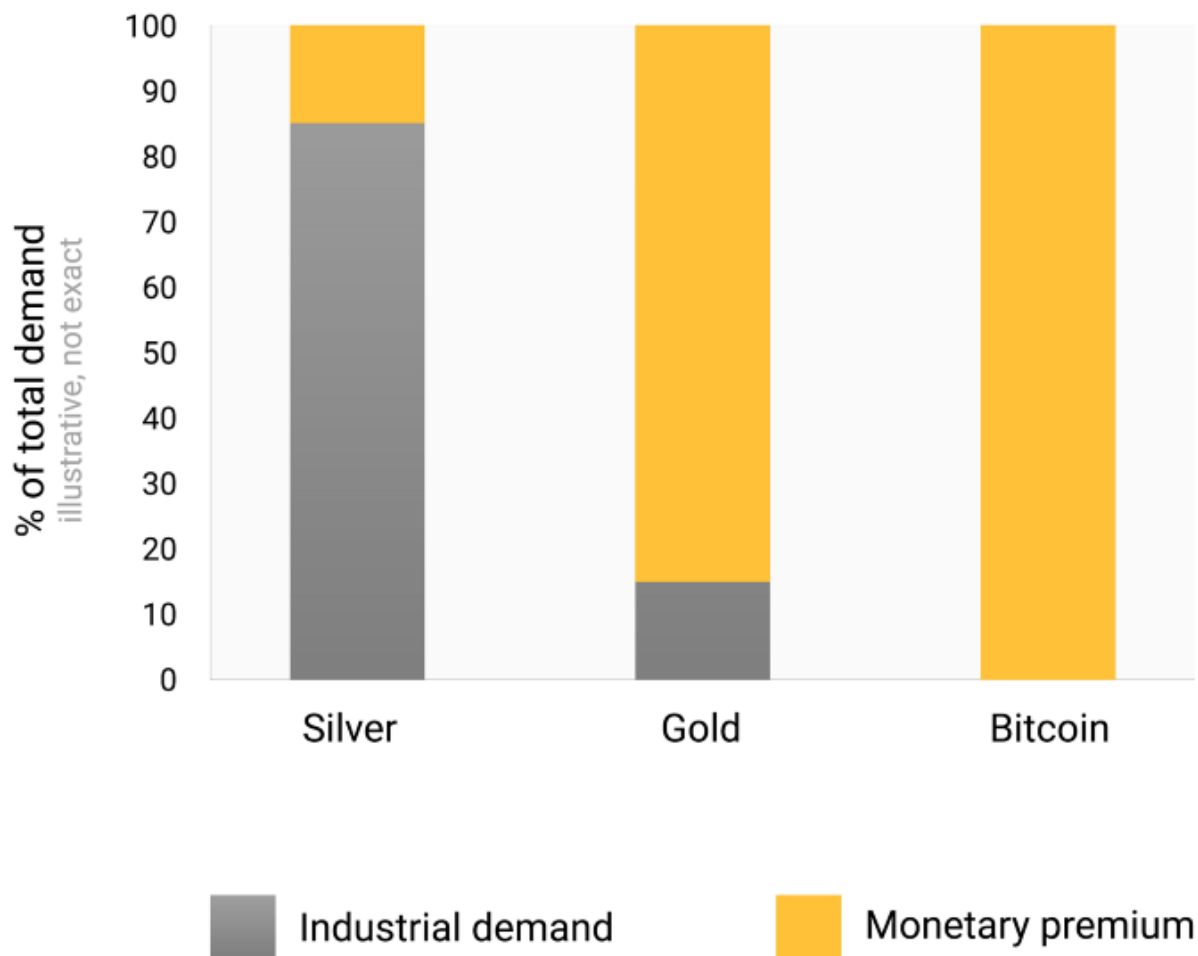
Bitcoin is currently transitioning from the first stage of monetization to the second stage. It will likely be several years before Bitcoin transitions from being an incipient store of value to being a true medium of exchange, and the path it takes to get there is still fraught with risk and uncertainty. It is striking to note that the same transition took many centuries for gold. No one alive has seen the real-time monetization of a good (as is taking place with Bitcoin), so there is precious little experience regarding the path this monetization will take.

Path dependence

In the process of being monetized, a monetary good will soar in purchasing power. Many have commented that the increase in purchasing power of Bitcoin creates the appearance of a “bubble”. While this term is often used disparagingly to suggest that Bitcoin is grossly overvalued, it is unintentionally apt. A characteristic that is common to all monetary goods is that their purchasing power is higher than can be justified by their use-value alone. Indeed, many historical monies had no use-value at all. The difference between the purchasing power of a monetary good and the exchange-value it could command for its inherent usefulness can be thought of as a “monetary premium”. As a monetary good transitions through the stages of monetization (listed in the section above), the monetary premium will increase. The premium does not, however, move in a straight, predictable

line. A good X that was in the process of being monetized may be outcompeted by another good Y that is more suitable as money, and the monetary premium of X may drop or vanish entirely. The monetary premium of silver disappeared almost entirely in the late 19th century when governments across the world largely abandoned it as money in favor of gold.

Monetary premium for different monetary goods



Even in the absence of exogenous factors such as government intervention or competition from other monetary goods, the monetary premium for a new money will not follow a predictable path. Economist Larry White observed that:

the trouble with [the] bubble story, of course, is that [it] is consistent with any price path, and thus gives no explanation for a particular price path

The process of monetization is game-theoretic; every market participant attempts to anticipate the aggregate demand of other participants and thereby the future monetary premium. Because the monetary premium is unanchored to any inherent usefulness, market participants tend to default to past prices when determining whether a monetary good is cheap or expensive and whether to buy or sell it. The connection of current demand to past prices is known as “path dependence” and is perhaps the greatest source of confusion in understanding the price movements of monetary goods.

When the purchasing power of a monetary good increases with increasing adoption, market expectations of what constitutes “cheap” and “expensive” shift accordingly. Similarly, when the price of a monetary good crashes, expectations can switch to a general belief that prior prices were “irrational” or overly inflated. The path dependence of money is illustrated by the words of well-known Wall Street fund manager Josh Brown:

I bought [bitcoins] at like \$2300 and had an immediate double on my hands. Then I started saying “I can’t buy more of it,” as it rose, even though that’s an anchored opinion based on nothing other than the price where I originally got it. Then, as it fell over the last week because of a Chinese crackdown on the exchanges, I started saying to myself, “Oh good, I hope it gets killed so I can buy more.”

The truth is that the notions of “cheap” and “expensive” are essentially meaningless in reference to monetary goods. The price of a monetary good is not a reflection of its cash flow or how useful it is but, rather, is a measure of how widely adopted it has become for the various roles of money.

Further complicating the path-dependent nature of money is the fact that market participants do not merely act as dispassionate observers, trying to buy or sell in anticipation of future movements of the monetary premium, but also act as active evangelizers. Since there is no objectively correct monetary premium, proselytizing the superior attributes of a monetary good is more effective than for regular goods, whose value is ultimately anchored to cash flow or use-demand. The religious fervor of participants in the Bitcoin market can be observed in various online forums where owners actively promote the benefits of Bitcoin and the wealth that can be made by investing in it. In observing the Bitcoin market, Leigh Drogen comments:

You recognize this as a religion — a story we all tell each other and agree upon. Religion is the adoption curve we ought to be thinking about. It’s almost perfect — as soon as someone gets in, they tell everyone and go out evangelizing. Then their friends get in and they start evangelizing.

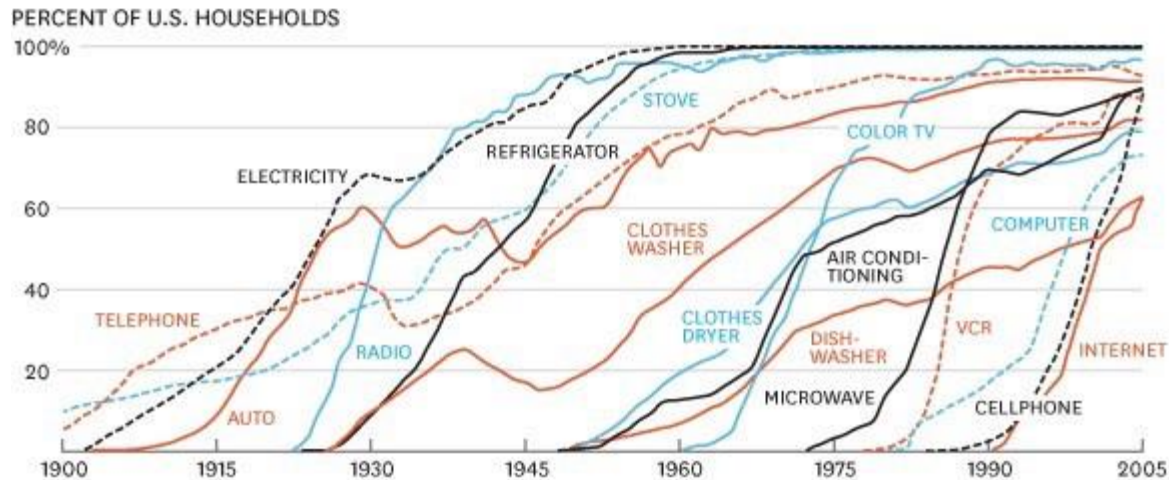
While the comparison to religion may give Bitcoin an aura of irrational faith, it is entirely rational for the individual owner to evangelize for a superior monetary good and for society as a whole to standardize on it. Money acts as the foundation for all trade and savings, so the adoption of a superior form of money has tremendous multiplicative benefits to wealth creation for all members of a society.

The shape of monetization

While there are no *a priori* rules about the path a monetary good will take as it is monetized, a curious pattern has emerged during the relatively brief history of Bitcoin's monetization. Bitcoin's price appears to follow a fractal pattern of increasing magnitude, where each iteration of the fractal matches the classic shape of a Gartner hype cycle.



In his article on [the Speculative Bitcoin Adoption/Price Theory](#), Michael Casey posits that the expanding Gartner hype cycles represent phases of a standard S-curve of adoption that was followed by many transformative technologies as they become commonly used in society.



Each Gartner hype cycle begins with a burst of enthusiasm for the new technology, and the price is bid up by the market participants who are “reachable” in that iteration. The earliest buyers in a Gartner hype cycle typically have a strong conviction about the transformative nature of the technology they are investing in. Eventually the market reaches a crescendo of enthusiasm as the supply of new participants who can be reached in the cycle is exhausted and the buying becomes dominated by speculators more interested in quick profits than the underlying technology.

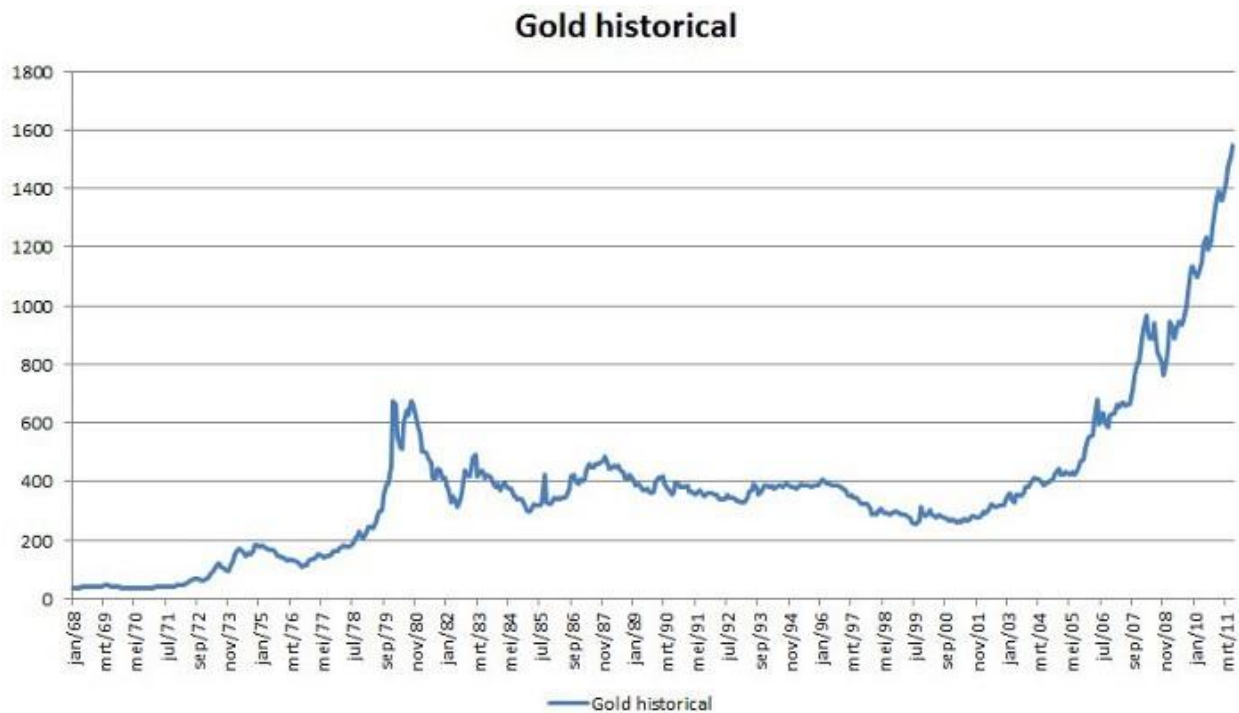
Following the peak of the hype cycle, prices rapidly drop and the speculative fervor is replaced by despair, public derision and a sense that the technology was not transformative at all. Eventually the price bottoms and forms a plateau where the original investors who had strong conviction are joined by a new cohort who were able to withstand the pain of the crash and who appreciated the importance of the technology.

The plateau persists for a prolonged period of time and forms, as Casey calls it, a “stable, boring low”. During the plateau, public interest in the technology will dwindle but it will continue to be developed and the collection of strong believers will slowly grow. A new base is then set for the next iteration of the hype cycle as external observers recognize the technology is not going away and that investing in it may not be as risky as it seemed during the crash phase of the cycle. The next iteration of the hype cycle will bring in a much larger set of adopters and be far greater in magnitude.

Very few people participating in an iteration of a Gartner hype cycle will correctly anticipate how high prices will go in that cycle. Prices usually reach levels that would seem absurd to most investors at the earliest stages of the cycle. When the cycle ends, a popular cause it typically attributed to the crash by the media. While the stated cause (such as an exchange failure) may be a precipitating event, it is not the fundamental reason for the cycle to end.

Gartner hype cycles end because of an exhaustion of market participants reachable in the cycle.

It is telling that gold followed the classic pattern of a Gartner hype cycle from the late 1970s to the early 2000s. One might speculate that the hype cycle is an inherent social dynamic to the process of monetization.



Gartner cohorts

Since the inception of the first exchange traded price in 2010, the Bitcoin market has witnessed four major Gartner hype cycles. With hindsight we can precisely identify the price ranges of previous hype cycles in the Bitcoin market. We can also qualitatively identify the cohort of investors that were associated with each iteration of prior cycles.

\$0– \$1 (2009–March 2011): The first hype cycle in the Bitcoin market 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 the Bitcoin protocol was free of technical flaws.

\$1– \$30 (March 2011–July 2011): The second cycle attracted both early adopters of new technology and a steady stream of ideologically motivated investors who were dazzled by the potential of a stateless money. Libertarians such as Roger Ver were attracted to Bitcoin for the anti-establishment activities that would become possible if the nascent technology became widely adopted. Wences Casares, a brilliant and well-connected serial entrepreneur, was also

part of the second Bitcoin hype cycle and is known to have evangelized Bitcoin to some of the most prominent technologists and investors in Silicon Valley.

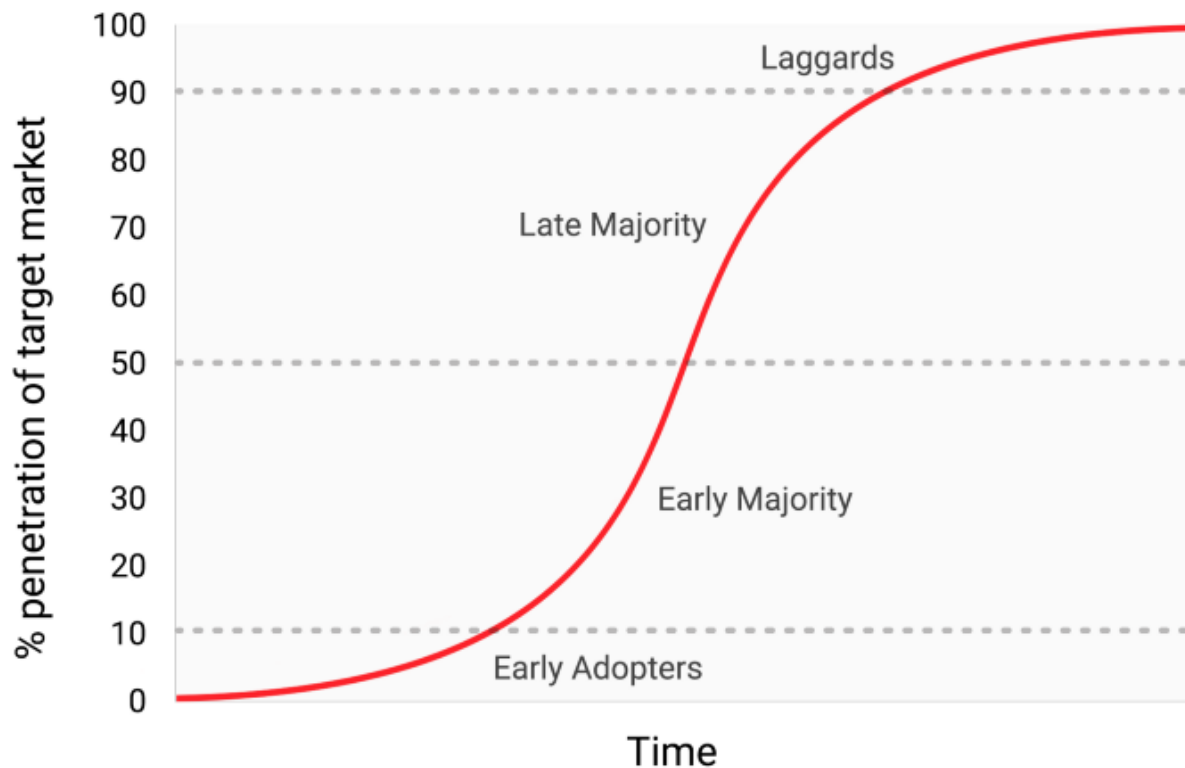
\$250– \$1100 (April 2013–December 2013): The third hype cycle saw the entrance of early retail and institutional investors who were willing to brave the horrendously complicated and risky liquidity channels from which bitcoins could be bought. The primary source of liquidity in the market during this period was the Japan-based MtGox exchange that was run by the notoriously incompetent and malfeasant Mark Karpeles, who later saw prison time for his role in the collapse of the 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 hype cycle, there were no exchanges available, and acquisition of bitcoins was primarily through mining or by direct exchange with someone who had already mined bitcoins. In the second hype 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 to acquire bitcoins. Banks were reluctant to deal with the exchange, and third party vendors who facilitated transfers were often incompetent, criminal, or both. Further, many who did manage to transfer money to MtGox ultimately faced loss of funds when the exchange was hacked and later closed.

It was only after the collapse of the MtGox exchange and a two-year lull in the market price of Bitcoin that mature and deep sources of liquidity were developed; examples include regulated exchanges such as GDAX and OTC brokers such as Cumberland mining. By the time the fourth hype cycle began in 2016 it was relatively easy for retail investors to buy bitcoins and secure them.

\$1100– \$19600? (2014– ?):

At the time of writing, the Bitcoin market is undergoing its fourth major hype cycle. 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.

Although it is impossible to predict the exact magnitude of the current hype cycle, it would be reasonable to conjecture that the cycle reaches its zenith in the range of \$20,000 to \$50,000. 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 \$380,000 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.

The entrance of 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. Unfortunately, it will probably be the states with the strongest executive powers — dictatorships such as North Korea — that will move the fastest in accumulating bitcoins. The unwillingness to see such states improve their financial position and the inherently weak executive branches of the Western democracies will cause them to dither and be laggards in accumulating bitcoins for their reserves.

There is a great irony that the US is currently one of the nations most open in its regulatory position toward Bitcoin, while China and Russia are the most hostile. The US risks the greatest downside to its geopolitical position if Bitcoin were to supplant the dollar as the world's reserve currency. In the 1960s, Charle de Gaulle criticized the "exorbitant privilege" the US enjoyed from the international monetary order it crafted with the Bretton Woods agreement of 1944. The Russian and Chinese governments have not yet awoken to the geo-strategic benefits of Bitcoin as a reserve currency and are currently preoccupied with the effects it may have on their internal markets. Like de Gaulle in the 1960s, who threatened to reestablish the classical gold standard in response to the US's exorbitant privilege, the Chinese and Russians will, in time, come to see the benefits of a large reserve position in a non-sovereign store of value. With the largest concentration of Bitcoin mining power residing in China, the Chinese state already has a distinct advantage in its potential to add bitcoins to its reserves.

The US prides itself as a nation of innovators, with Silicon Valley being a crown jewel of the US economy. Thus far, Silicon Valley has largely dominated the conversation toward regulators on the position they should take vis-à-vis Bitcoin. However, 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. The Wall Street Journal, known to be a mouth-piece for the Federal Reserve, published a commentary on the threat Bitcoin poses to US monetary policy:

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.

In the coming years there will be a great struggle between entrepreneurs and innovators in Silicon Valley, 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.

The transition to a medium of exchange

A monetary good cannot transition to being a generally accepted medium of exchange (the standard economic definition of “money”) before it is widely valued, for the tautological reason that a good that is not valued will not be accepted in exchange. In the process of becoming widely valued, and hence a store of value, a monetary good will soar in purchasing power, creating an opportunity cost to relinquishing it for use in exchange. Only when the opportunity cost of relinquishing a store of value drops to a suitably low level can it transition to becoming a generally accepted medium of exchange.

More precisely, a monetary good will only be suitable as a medium of exchange when the sum of the opportunity cost and the transactional cost of using it in exchange drops below the cost of completing a trade without it.

In a barter-based society, the transition of a store of value to a medium of exchange can occur even when the monetary good is increasing in purchasing power because the transactional costs of barter trade are extremely high. In a developed economy, where transactional costs are low, it is possible for a nascent and rapidly appreciating store of value, such as Bitcoin, to be used as a medium of exchange, albeit in a very limited scope. An example is the illicit drug market where buyers are willing to sacrifice the opportunity of holding bitcoins to minimize the substantial risk of purchasing the drugs using fiat currency.

There are, however, major institutional barriers to a nascent store of value becoming a *generally* accepted medium of exchange in a developed society. States use taxation as a powerful means to protect their sovereign money from being displaced by competing monetary goods. Not only does a sovereign money enjoy the advantage of a constant source of demand, by way of taxes being remittable only in it, but competing monetary goods are taxed whenever they are exchanged at an appreciated value. This latter kind of taxation creates significant friction to using a store of value as a medium of exchange.

The handicapping of market-based monetary goods is not an insurmountable barrier to their adoption as a generally accepted medium of exchange, however. If faith is lost in a sovereign money, its value can collapse in a process known as hyperinflation. When a sovereign money hyperinflates, its value first collapses against the most liquid goods in the society, such as gold or a foreign money like the US dollar, if they are available. When no liquid goods are available or their supply is limited, a hyperinflating money

collapses against real goods, such as real estate and commodities. The archetypal image of a hyperinflation is a grocery store emptied of all its produce as consumers flee the rapidly diminishing value of their nation's money.



Eventually, when faith is completely lost during a hyperinflation, a sovereign money will no longer be accepted by anyone, and the society will either devolve to barter or the monetary unit will be completely replaced as a medium of exchange. An example of this process was the replacement of the Zimbabwe dollar with the US dollar. The replacement of a sovereign money with a foreign one is made more difficult by the scarcity of the foreign money and the absence of foreign banking institutions to provide liquidity.

The ability to easily transmit bitcoins across borders and absence of a need for a banking system make Bitcoin an ideal monetary good to acquire for those afflicted by hyperinflation. In the coming years, as fiat monies continue to follow their historical trend toward eventual worthlessness, Bitcoin will become an increasingly popular choice for global savings to flee to. When a nation's money is abandoned and replaced by Bitcoin, Bitcoin will have transitioned from being a store of value in that society to a generally accepted medium of exchange. Daniel Krawisz coined the term "hyperbitcoinization" to describe this process.

Common misconceptions

Much of this article has focused on the monetary nature of Bitcoin. With this foundation we can now address some of the most commonly held misconceptions about Bitcoin.



Bitcoin is a bubble

Bitcoin, like all market-based monetary goods, displays a monetary premium. The monetary premium is what gives rise to the common criticism that Bitcoin is a “bubble”. However, *all* monetary goods display a monetary premium. Indeed, it is this premium (the excess over the use-demand price) that is the defining characteristic of all monies. In other words, money is always and everywhere a bubble. Paradoxically, a monetary good is both a bubble and may be undervalued if it’s in the early stages of its adoption for use as money.

Bitcoin is too volatile

Bitcoin’s price volatility is a function of its nascency. In the first few years of its existence, Bitcoin behaved like a penny-stock, and any large buyer — such as the Winklevoss twins — could cause a large spike in its price. As adoption and liquidity have increased over the years, Bitcoin’s volatility has decreased commensurately. When Bitcoin achieves the market capitalization of gold, it

will display a similar level of volatility. As Bitcoin surpasses the market capitalization of gold, its volatility will decrease to a level that will make it suitable as a widely used medium of exchange. As previously noted, the monetization of Bitcoin occurs in a series of Gartner hype cycles. Volatility is lowest during the plateau phase of the hype cycle, while it is highest during the peak and crash phases of the cycle. Each hype cycle has lower volatility than the previous ones because the liquidity of the market has increased.

Transaction fees are too high

A recent criticism of the Bitcoin network is that the increase in fees to transmit bitcoins makes it unsuitable as a payment system. However, the growth in fees is healthy and expected. Transaction fees are the cost required to pay bitcoin miners to secure the network by validating transactions. Miners can either be paid by transaction fees or by block rewards, which are an inflationary subsidy borne by current bitcoin owners.

Given Bitcoin's fixed supply schedule — a monetary policy which makes it ideally suited as a store of value — block rewards will eventually decline to zero and the network must ultimately be secured with transaction fees. A network with “low” fees is a network with little security and prone to external censorship. Those touting the low fees of Bitcoin alternatives are unknowingly describing the weakness of these so-called “alt-coins”.

The specious root of the criticism of Bitcoin's “high” transaction fees is the belief that Bitcoin should be a payment system first and a store of value later. As we have seen with the origins of money, this belief puts the cart before the horse. Only when Bitcoin has become a deeply established store of value will it become suitable as a medium of exchange. Further, once the opportunity cost of trading bitcoins is at a level at which it is suitable as a medium of exchange, most trades will not occur on the Bitcoin network itself but on “second layer” networks with much lower fees. Second layer networks, such as the Lightning network, provide the modern equivalent of the promissory notes that were used to transfer titles for gold in the 19th century. Promissory notes were used by banks because transferring the underlying bullion was far more costly than transferring the note that represented title to the gold. Unlike promissory notes, however, the Lightning network will allow the transfer of bitcoins at low cost while requiring little or no trust of third parties such as banks. The development of the Lightning network is a profoundly important technical innovation in Bitcoin's history and its value will become apparent as it is developed and adopted in the coming years.

Competition

As an open-source software protocol, it has always been possible to copy Bitcoin's software and imitate its network. Over the years, many imitators have been created, ranging from ersatz facsimiles, such as Litecoin, to complex variants like Ethereum that promise to allow arbitrarily complex contractual arrangements using a distributed computational system. A common investment criticism of Bitcoin is that it cannot maintain its value when competitors can be easily created that are able to incorporate the latest innovations and software features.



The fallacy in this argument is that the scores of Bitcoin competitors that have been created over the years lack the “network effect” of the first and dominant technology in the space. A network effect — the increased value of using Bitcoin simply because it is already the dominant network — is a feature in and of itself. For any technology that possesses a network effect, it is by far the most important feature.

The network effect for Bitcoin encompasses the liquidity of its market, the number of people who own it, and the community of developers maintaining and improving upon its software and its brand awareness. Large investors, including nation-states, will seek the most liquid market so that they can enter and exit the market quickly without affecting its price. Developers will flock to the dominant development community which has the highest-calibre talent, thereby reinforcing the strength of that community. And brand awareness is self-reinforcing, as would-be competitors to Bitcoin are always mentioned in the context of Bitcoin itself.

A fork in the road

A trend that became popular in 2017 was not only to imitate Bitcoin's software, but to copy the entire history of its past transactions (known as the blockchain). By copying Bitcoin's blockchain up to a certain point and then splitting off into a new network, in a process known as "forking", competitors to Bitcoin were able to solve the problem of distributing their token to a large user base.



The most significant fork of this kind occurred on August 1st, 2017 when a new network known as Bitcoin Cash (BCash) was created. An owner of N bitcoins before August 1st, 2017, would then own both N bitcoins and N BCash tokens. The small but vocal community of BCash proponents have tirelessly attempted to expropriate Bitcoin's brand recognition, both through the naming of their new network and a campaign to convince neophytes in the Bitcoin market that Bcash is the "real" Bitcoin. These attempts have largely failed, and this failure is reflected in the market capitalizations of the two networks. However, for new investors, there remains an apparent risk that a competitor might clone Bitcoin and its blockchain and succeed in overtaking it in market capitalization, thus becoming the de facto Bitcoin.

An important rule can be gleaned from the major forks that have happened to both the Bitcoin and Ethereum networks. The majority of the market capitalization will settle on the network that retains the highest-calibre and most active developer community. For although Bitcoin can be viewed as a nascent money, it is also a computer network built on software that needs to be maintained and improved upon. Buying tokens on a network which has little or inexperienced developer support would be akin to buying a clone of Microsoft Windows that was not supported by Microsoft's best developers. It

is clear from the history of the forks that occurred in 2017 that the best and most experienced computer scientists and cryptographers are committed to developing for the original Bitcoin and not any of the growing legion of imitators that have been created from it.

Real risks

Although the common criticisms of Bitcoin found in the media and economics profession are misplaced and based on a flawed understanding of money, there are real and significant risks to investing in Bitcoin. It would be prudent for a prospective Bitcoin investor to understand and weigh these risks before considering an investment in Bitcoin.

Protocol risk

The Bitcoin protocol and the cryptographic primitives that it is built upon could be found to have a design flaw, or could be made insecure with the development of quantum computing. If a flaw is found in the protocol, or some new means of computation makes possible the breaking of the cryptography underpinning Bitcoin, the faith in Bitcoin may be severely compromised. The protocol risk was highest in the early years of Bitcoin's development, when it was still unclear, even to seasoned cryptographers, that Satoshi Nakamoto had actually found a solution to the Byzantine Generals' Problem. Concerns about serious flaws in the Bitcoin protocol have dissipated over the years, but given its technological nature, protocol risk will always remain for Bitcoin, if only as an outlier risk.

Exchange shutdowns

Being decentralized in design, Bitcoin has shown a remarkable degree of resilience in the face of numerous attempts by various governments to regulate it or shut it down. However, the exchanges where bitcoins are traded for fiat currencies are highly centralized and susceptible to regulation and closure. Without these exchanges and the willingness of the banking system to do business with them, the process of monetization of Bitcoin would be severely stunted, if not halted completely. While there are alternative sources of liquidity for Bitcoin, such as over-the-counter brokers and decentralized markets for buying and selling Bitcoins (like localbitcoins.com), the critical process of price discovery happens on the most liquid exchanges, which are all centralized.

Mitigating the risk of exchange shutdowns is jurisdictional arbitrage. Binance, a prominent exchange that started in China, moved to Japan after the Chinese government halted its operations in China. National governments are also wary of smothering a nascent industry that may prove as

consequential as the Internet, thereby ceding a tremendous competitive advantage to other nations.

Only with a coordinated global shutdown of Bitcoin exchanges would the process of monetization be halted completely. The race is on for Bitcoin to become so widely adopted that a complete shutdown becomes as politically infeasible as a complete shutdown of the Internet. The possibility of such a shutdown is still real, however, and must be factored into the risks of investing in Bitcoin. As was discussed in the prior section on the entrance of nation-states, national governments are finally awakening to the threat that a non-sovereign, censorship-resistant, digital currency poses to their monetary policies. It is an open question whether they will act on this threat before Bitcoin becomes so entrenched that political action against it proves ineffectual.

Fungibility

The open and transparent nature of the Bitcoin blockchain makes it possible for states to mark certain bitcoins as being “tainted” by their use in proscribed activities. Although Bitcoin’s censorship resistance at the protocol level allows these bitcoins to be transmitted, if regulations were to appear that banned the use of such tainted bitcoins by exchanges or merchants, they could become largely worthless. Bitcoin would then lose one of the critical properties of a monetary good: fungibility.

To ameliorate Bitcoin’s fungibility, improvements will need to be made at the protocol level to improve the privacy of transactions. While there are new developments in this regard, pioneered in digital currencies such as Monero and Zcash, there are major technological tradeoffs to be made between the efficiency and complexity of Bitcoin and its privacy. It remains an open question whether privacy-enhancing features can be added to Bitcoin in a way that doesn’t compromise its usefulness as money in other ways.

Conclusion

Bitcoin is an incipient money that is transitioning from the collectible stage of monetization to becoming a store of value. As a non-sovereign monetary good, it is possible that at some stage in the future Bitcoin will become a global money much like gold during the classical gold standard of the 19th century. The adoption of Bitcoin as global money is precisely the bullish case for Bitcoin, and was articulated by Satoshi Nakamoto as early as 2010 in an [email exchange](#) with Mike Hearn:

If you imagine it being used for some fraction of world commerce, then there’s only going to be 21 million coins for the whole world, so it would be worth much more per unit.

This case was made even more trenchantly by the brilliant cryptographer Hal Finney, the recipient of the first bitcoins sent by Nakamoto, shortly after the announcement of the first working Bitcoin software:

[I]magine that Bitcoin is successful and becomes the dominant payment system in use throughout the world. Then the total value of the currency should be equal to the total value of all the wealth in the world. Current estimates of total worldwide household wealth that I have found range from \$100 trillion to \$300 trillion. With 20 million coins, that gives each coin a value of about \$10 million.

Even if Bitcoin were not to become a fully fledged global money and were simply to compete with gold as a non-sovereign store of value, it is currently massively undervalued. Mapping the market capitalization of the extant above-ground gold supply (approximately 8 trillion dollars) to a maximum Bitcoin supply of 21 million coins gives a value of approximately \$380,000 per bitcoin. As we have seen in prior sections, for the attributes that make a monetary good suitable as a store of value, Bitcoin is superior to gold along every axis except for established history. As time passes and the Lindy effect takes hold, established history will no longer be a competitive advantage for gold. Thus, it is not unreasonable to expect that Bitcoin will approach, and perhaps surpass, gold's market capitalization in the next decade. A caveat to this thesis is that a large fraction of gold's capitalization comes from central banks holding it as a store of value. For Bitcoin to achieve or surpass gold's capitalization, some participation by nation-states will be necessary. Whether the Western democracies will participate in the ownership of Bitcoin is unclear. It is more likely, and unfortunate, that tin-pot dictatorships and kleptocracies will be the first nations to enter the Bitcoin market.

If no nation-states participate in the Bitcoin market, there still remains a bullish case for Bitcoin. As a non-sovereign store of value used only by retail and institutional investors, Bitcoin is still early in its adoption curve — the so-called “early majority” are now entering the market while the late majority and laggards are still years away from entering. With broader participation from retail and especially institutional investors, a price level between \$100,000 and \$200,000 is feasible.

Owning bitcoins is one of the few asymmetric bets that people across the entire world can participate in. Much like a call option, an investor's downside is limited to 1x, while their potential upside is still 100x or more. Bitcoin is the first truly global bubble whose size and scope is limited only by the desire of the world's citizenry to protect their savings from the vagaries of government economic mismanagement. Indeed, Bitcoin rose like a phoenix from the

ashes of the 2008 global financial catastrophe — a catastrophe that was precipitated by the policies of central banks like the Federal Reserve.

Beyond the financial case for Bitcoin, its rise as a non-sovereign store of value will have profound geopolitical consequences. A global, non-inflationary reserve currency will force nation-states to alter their primary funding mechanism from inflation to direct taxation, which is far less politically palatable. States will shrink in size commensurate to the political pain of transitioning to taxation as their exclusive means of funding. Furthermore, global trade will be settled in a manner that satisfies Charles de Gaulle's aspiration that no nation should have privilege over any other:

We consider it necessary that international trade be established, as it was the case, before the great misfortunes of the World, on an indisputable monetary base, and one that does not bear the mark of any particular country.

50 years from now, that monetary base will be Bitcoin.

Translations

This article has been translated into:

- [English podcast](#) by [Heardit](#).
- [English podcast](#) by [Cryptoconomy](#).
- [Podcast interview about the article](#) with [Peter McCormack](#).
- [Deutsche](#) by [Daniel Schnurr](#), [Simon Lutz](#) and [Arlene Roa Aillaud](#).
- [Österreichisches Deutsch](#) by [Bernie Eder](#).
- Korean by [Hyungmok joh](#) ([part 1](#), [part 2](#), [part 3](#), [part 4](#)).
- Traditional Chinese by [Flora Sun](#) ([part 1](#), [part 2](#), [part 3](#), [part 4](#)).
- Simplified Chinese by [Flora Sun](#) ([part 1](#), [part 2](#), [part 3](#), [part 4](#)).
- Español by [Iñigo](#) and [Carlos Beltrán](#) ([part 1](#), [part 2](#), [part 3](#), [part 4](#)).
- Nederlandse by [Wim](#), edited by [Koen Swinkels](#) ([part 1](#), [part 2](#), [part 3](#), [part 4](#)).
- Française by [Greg Guittard](#) ([part 1](#), [part 2](#), [part 3](#), [part 4](#)).
- Italiano by [Ryan DeLongpre](#).
- Português by [Allex Fer](#) ([part 1](#), [part 2](#), [part 3](#), [part 4](#)).
- Tamil by [Balaji Vaidyanath](#) and [Mahadevan Vaidyanath](#) ([part 1](#)).
- русский/Russian by [CoinSpot](#) ([part 1](#), [part 2](#), [part 3](#), [part 4](#)).
- Bulgarian by [Bo Mirchev](#) ([part 1](#), [part 2](#), [part 3](#), [part 4](#)).

About me

I'm a former Google engineer who's interested in Austrian economics. I'm also a husband and loving father of Addie and Will. [Follow me on Twitter](#).

Acknowledgements

I want to thank Alex Morcos, John Pfeffer, Pierre Rochard, Mat Balez, Ray Boyapati, Daniel Coleman, Koen Swinkels, Patri Friedman, Ardian Tola, Michael Flaxman and Michael Hartl for their valuable feedback on earlier drafts of this series of articles. Sanjay Mavinkurve generously provided his brilliant design skills to create some of the charts.

Disclaimer

The views presented in this article and any errors herein are my own.

This article is for information purposes only. It is not intended to be investment advice. Seek a duly licensed professional for investment advice.

Tags: [Analysis](#) [Asymmetric Bets](#) [Bitcoin](#) [Canon](#) [Canon](#) [CY18 Q1](#) [Economics](#) [Essential Reading](#) [Finance](#) [Financial](#) [Vijay Boyapati](#)