PART I: Thoughts on Bitcoin

We propose that the best way to conceptualize Bitcoin is to ignore the notions of "currency" and "money" and think about a ledger system of debits and credits. You "buy in" to the ledger system with something that is universally accepted as having value – either with cash or by selling a product or service in Bitcoins, and then are free to trade within the Bitcoin sandbox.

This is the key and why it doesn't matter whether the Bitcoins themselves have intrinsic value – your price of admission has intrinsic value and as long as there is one other person in the world who believes in Bitcoin, you can also "cash out" at any time.

On this view, Bitcoin is "post-currency." Bitcoin allows us to imagine a theoretical steady state where every human's finances live on the same ledger and the notion that we would use some physical means of exchange (gold, cigarettes, dollars) to conduct transactions is a vestigial technology like floppy disks.

Most importantly, whether Bitcoin "wins" or not, we believe that the concept of a post-currency ledger system has taken root. The current price appreciation, capital inflow, popular media coverage, and accelerating transaction volume all point towards Bitcoin having its "Netscape moment." The ledger concept is too powerful to ever put the genie back in the bottle, because of the massive amount of value creation potential it enables:

- Huge reduction of transaction friction, particularly across borders: When money is as easy and secure as email, we anticipate reduced border effects (psychology of geographical distance leads to fewer transactions), lower transaction fees and currency exchange fees, faster transaction processing times, reduced fraud, and indeed greater trust in the currency of record as a means of exchange (mostly true for developing markets)

- De-verticalization of banks: From vertically integrated, *geographically*-specialized institutions to global, *functionally*-specialized platforms. It is a historical anomaly that the "warehouse" for money should also be the "store" for money. In a world of digital money, the intermediary with the best data and the most liquidity should be the best facilitator of credit, independently of who owns the largest stores of deposits. There is no possibility that existing banking institutions will be able to adapt to this disruption, and we anticipate the rise of ledger-based verticals for the warehousing of money and supplying of credit.

- Net new businesses: We envision ledger systems enabling new business models such as "insurance" for digital money, new investment products that make savings accounts and CDs obsolete (P2P lending?), and new "features" such as multiple owners of the same ledger balance, which could improve corporate governance and family financial planning

Our ledger analogy allows us to better understand the "value" of Bitcoins.

To simplify, suppose there are two means of conducting transactions, one is that you use dollar bills and someone charges you 2% each time to use them, the other is that you have 100 seats on the ledger where you can do business with other members on the ledger for free.

Pretty soon more than 100 people at once will want to save 2%, so the ledger seats will get more valuable as people bid for the right to conduct business for free. We will reach an equilibrium quickly, since no one will want to pay more than 2% x the number of transactions they expect to be able to do

with the 99 other people on the ledger. The equilibrium is governed by the number of spots available, the per transaction savings, and the number of transactions that it is possible to conduct with other people on the ledger.

But let's relax the 100 people constraint and say you can buy a fractional seat at the table, which entitles you to all the same trading benefits as if you owned a full seat. Now we will have many more people all willing to pay up to 2% x expected transactions for their fractional seat. And we have also increased the number of potential transactions that can happen on the ledger because more people are participating.

Once we settle at equilibrium, if we add up how much everyone has paid for their fractional seat, we will see that the price of a single original seat has appreciated dramatically.

At unlimited divisibility of seats, the supply of seats does not govern the dollar price of a seat – it is purely a function of the size of the ledger – i.e., the number of potential transactions the network enables - and the economic savings per transaction inside the ledger vs. outside.

<u>This has a few dramatic implications:</u>

Bitcoin has broken the requirement that money be based on belief

…whether that belief is a collective agreement in the value of gold jewelry, or in the government's ability to pay its debts into perpetuity. Against the criteria of divisibility, flexibility, transportability, and (arguably) security, Bitcoin is superior to every other system of money ever invented, and its value comes from internalizing those superiorities. In fact, the incremental economic value enabled by Bitcoin is an externality that will be disproportionately captured by the "early adopters" (or, "early believers") of the system and explains why Bitcoin is not a Ponzi scheme. It makes sense that the early participants in Bitcoin will "do better" than later participants, since their early contributions towards its viability have a greater impact on the strength of the network and its ability to create future economic value through its systemic superiority. The first person to join Facebook contributes more towards its durability and economic value than the one hundredth millionth.

The debate about the "intrinsic value" of an actual Bitcoin is a red herring.

The Bitcoins themselves are just a conceptual bridge to get people trading within the Bitcoin ledger system, which appreciates in value in direct proportion to the number of transactions that are happening within it, which itself is a direct consequence of the number of people on the ledger. Put differently, if you can buy Bitcoins and conduct transactions in a more seamless or lower cost way, then whether they have intrinsic value is meaningless to you.

As "post-currency" money, Bitcoin should not be susceptible to a deflationary spiral.

First, seats on the ledger can only appreciate relative to the total incremental value of ledger-facilitated transactions vs. the higher cost dollar alternative, or it will no longer be worth it to pay higher prices to get access to the lower friction transaction medium.

Second, hoarding slows down transaction velocity which as we've shown is a direct driver of price appreciation. There should be a feedback loop here – expected appreciation leads to hoarding, hoarding

leads to lower velocity, lower velocity leads to reduced expectations about appreciation, lower expectations reduces hoarding. Very much like a thermostat at equilibrium – not too hot, not too cold.

Third, even if there is *some* hoarding effect, as Bitcoin wealth increases through currency appreciation, the risk of loss increases as well. Bitcoins become too attractive not to trade for other goods, either to diversify, protect wealth creation, or simply find a better store of value such as stocks, bonds, or real estate. A company's high stock price doesn't necessarily lead to a collapse in liquidity for that equity. There is a population distribution of risk tolerance which will lead to profit taking and inject Bitcoins back into the market.

There should be intense competition for the future of ledger-based money

If it becomes a pain to use Bitcoins due to limited availability, not 100% certain availability, exchange difficulty, or currency volatility, everyone will see the success of Bitcoin and want to start a competitor.

It is fairly trivial to set up a system to use the internet to trade (going back to our point on "belief no longer required"). Putting aside Bitcoin's features of anonymity, you can compete with Bitcoin using something like Western Union, but more electronic. The competing system has to be able to solve the same problems that Bitcoin, Paypal, and Western Union have—but if they solve those problems, as long as they have some other low transaction cost way to move money (like banks cutting their fees, who don't actually have high costs, they just charge high fees), then you can compete with Bitcoin.

Importantly, there are actually strong incentives for governments to move to a post-currency ledger system. It has been posited by leading economists that electronic money gives central banks the ability to lower interest rates to below zero[1] (this is impossible today since you cannot have negative interest rates on physical currency, which would therefore outcompete negative interest earning bank deposits) and would provide a powerful tool in enacting fiscal stimulus. Additionally, governments can finally extract sales tax on ledger transactions that otherwise would have been conducted in cash.

This last point is worth dwelling on. As a competitor to Bitcoin, a central bank electronic ledger system, backed by the "full faith and credit" of a government, would achieve immediate transactional scale. In our view, this is probably the greatest threat to Bitcoin in the long-term. If Bitcoin is Netscape, the US government is Microsoft (A more important question might be – who/what is Google? (i.e. the vertical application, built on top of the platform, that is a winner-take-all business, with a 10+-year 30%+ annual growth trajectory and 30%+ margins…).

The strength of a government's monetary system ultimately is a function of the strength of the rule of law in that country (and in the most deprecated sense, the strength of the rule of law is a function of military power). So we can say that low quality governments will have low quality monetary systems. These will be the countries where Bitcoin is most likely to thrive. In the US/EU/Japan, the official currency is a fairly safe store of value (at least on a day-to-day basis) and the value of an alternative ledger system is of minimal value. In Argentina, Iraq, Venezuela, et al, this is not true. In those countries Bitcoins will act like black market dollars (much more useful than the official currency). But unlike black market dollars they can be used internationally i.e., you can cross a border and email Bitcoins to yourself, whereas dollars would get confiscated at the border.

[1] [redacted]

We foresee a real possibility that all currencies go digital and competition eliminates all currencies from non-effective governments. The power of friction-free transactions over the internet will unleash the typical forces of consolidation and globalization and we will end up with six digital currencies: US Dollar, Euro, Yen, Pound, Reminbi, and Bitcoin.

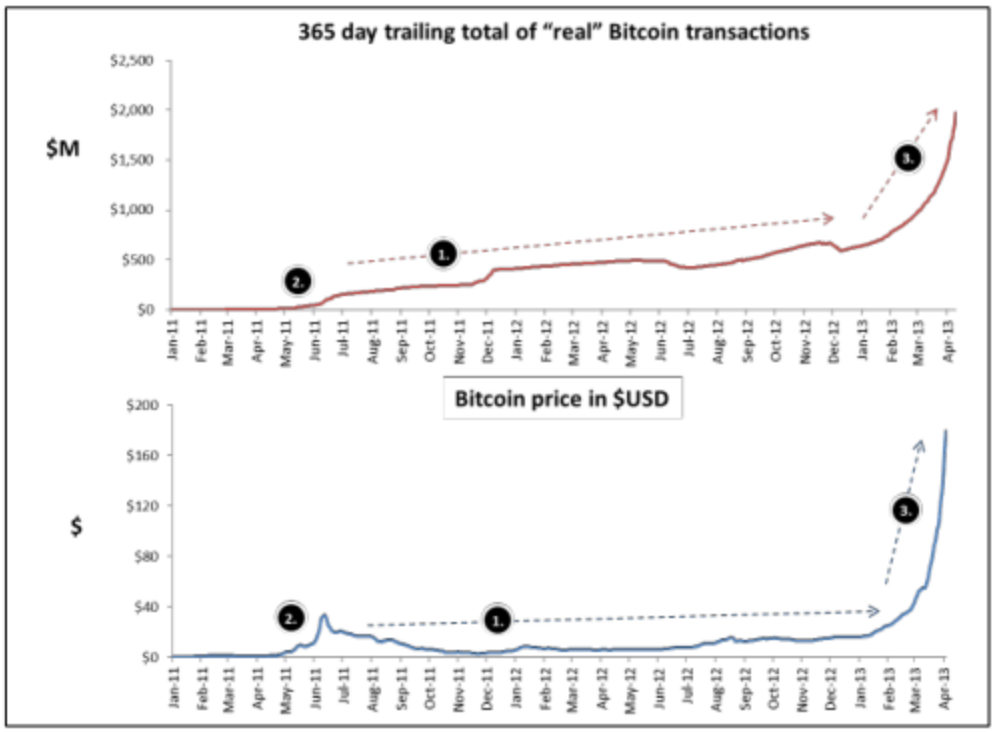
The question then becomes, is Bitcoin viable if the government digital ledger systems are just as good? We think yes, for two reasons:

1. There will always be transactions for which "official money" is less good than Bitcoin
2. If you live outside the US, it is dangerous to have all your money controlled by a state where you have no rights

PART II: Is Bitcoin a bubble?

To answer the question of whether the current appreciation of Bitcoins relative to dollars is a bubble, we go back to our fundamental premise that the value of Bitcoin (i.e., a seat on the ledger) is directly driven by the volume of transactions it facilitates.

Fortunately, the entire transaction history of Bitcoin is available as public record in the blockchain. In addition, since we know BTC prices and volume on the major exchanges, we can back out the transactions that are "currency exchanges" to figure out the "real" BTC-BTC trades for goods and services that make up the Bitcoin economy. To normalize, we take a 365-day trailing total[2]:

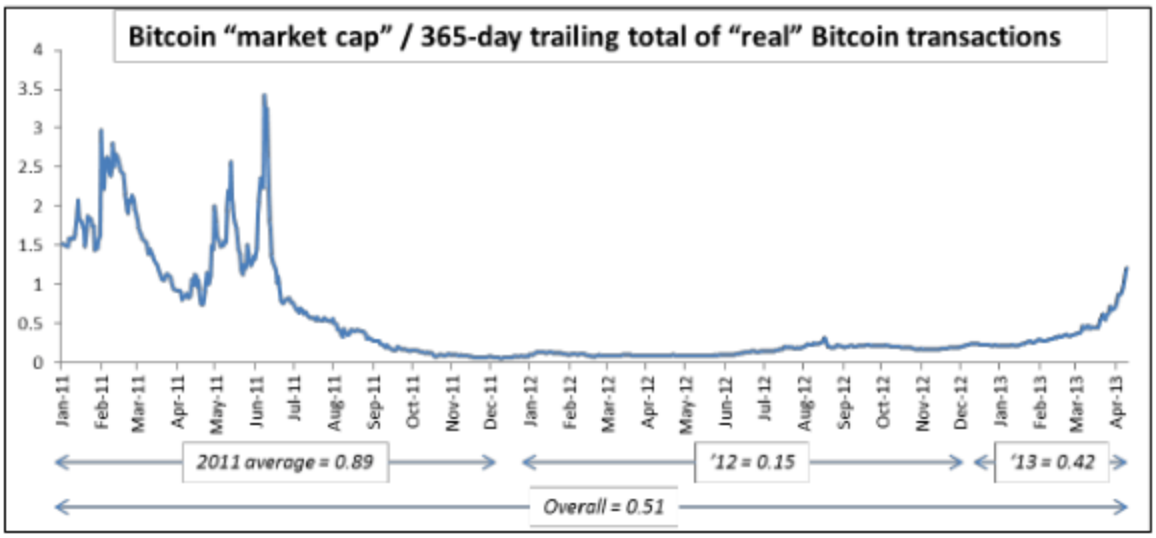


[2] http://blockchain.info/charts

From this, we can make a few observations:

1. There is a clear, steady increase in the "real" transactions happening on Bitcoin over the last two years. This has corresponded with a reasonably steady appreciation of BTC relative to USD
2. In the May '11-July '11 instance of a price spike/collapse, we saw a significant ramp of transactions (on a relative basis – after sitting at essentially $0 for its entire history back to 2009, went to $250M in a month)
3. The current spike in price is not entirely irrational, given real transaction volumes have doubled over the past six months. However, because of what we observe in #2 and the fact that the appreciation slope is steeper than the transaction ramp, it is very likely we will experience a near-term correction

Since we also know the total "market cap" of all BTCs in circulation at any point in time, we can calculate effectively the "multiple" of Bitcoin:



What this shows is that while Bitcoin is indeed getting somewhat more "expensive" relative to where it has traded in the past, it is not wildly so (note also the 2011 spike was much more dramatic). And since we know that real transactions are growing, the currency today is not significantly overvalued as it should be able to grow into the current market cap (spun differently, we see that if the historical "stable" multiple level of 0.15x can be maintained, there is a $30 floor on $/BTC on the current transaction volume). More importantly, there is *massive upside* as long as transactions keep growing, since the supply of Bitcoins is predictable and fixed over time, even if we see "multiple contraction" back to historical levels.

Bitcoin upside potential *($ per BTC)*

		365-day rolling transaction volume			
		Current (*$2.0B*)	$5B	$10B	$100B
Multiple *(@$200/BTC, 1.1; @$70/BTC, 0.4)*	0.15	$27	$68	$136	$1,364
	0.25	$45	$114	$227	$2,273
	0.40	$73	$182	$364	$3,636

Finally, we don't believe that transaction value growth is a hand wave. We hypothesize that there are a number of "killer scenarios" where Bitcoin is substantially advantaged as a currency for *legitimate* commercial activity:

- **Micropayments**: the "$0.15/3%, whichever is greater" fee extracted by credit card companies leads to effectively a 15%+ tax on transactions < $1. In the new digital economy of virtual goods, content, in-app purchases, etc…, 15% is substantial.

- **Online gambling**, where deposits & withdrawals are used as the control mechanism for regulation. Online today represents only 5% of a $400B gambling industry, which has been gated to a large degree by local governments. Online gambling has always participated in the arms race between payments innovation and regulation; as Bitcoin is a breakthrough disruption, it will be rapidly embraced

- **Small $ value international transfers**, using the same logic as micropayments: International fees are exorbitant relative to the value of the payments and are sustained only by the existing payments regimes

- **Brute force malware removal**: As soon as there is an n > 0 transaction cost on anything, it is possible to remove a lot of brute force malware on the web (e.g, if it costs .00001 BTC to load Ticketmaster.com, now bots can't pound the site with bots looking for tickets). We speculate that it might even be possible to solve email spam with Bitcoin (I opt in to 'BTC mail filtering' and it costs .00001 BTC to send me a message. Certainly some cold start problems but not insurmountable)

These killer scenarios will drive the Bitcoin network effect

PART III: Challenges for Bitcoin

Beyond the inherent risk of bootstrapping a new monetary system, we see two primary challenges for Bitcoin:

1. Government intervention (or, potentially, competition)

Control of the money supply is one of the principal roles of government (along with – fiscal policy, monopoly of force, taxation, law-making, etc…) Governments use monetary policy as a tool to effect real economic outcomes, which have a direct impact on the government's ability to maintain power (i.e., Depression = Revolution). Indeed, it is not out of the purview of government to enact draconian measures to control the money supply. Executive Order 6102 signed in 1933 by FDR criminalized the possession of gold.[3] So there is some possibility that at a certain scale, Bitcoin represents a significant threat to the central banks of the world, who have the authority to legally delegitimize it.

And as noted earlier, there are many good reasons for governments not to intervene in Bitcoin, but compete directly with it.

A few thoughts on this:

[3] http://en.wikipedia.org/wiki/Executive_Order_6102

- At $2B "market cap," Bitcoin isn't even big enough to register as a large cap company in the United States. Even at 2 orders of magnitude of growth, Bitcoin would only represent 1% of worldwide GDP. So we are probably looking at *3 orders of magnitude* of growth before Bitcoin becomes an issue for central banks, and possibly not even then given its dispersion around the world

- Despite the network effects at work, it is not necessarily a given that electronic money should be winner-take-all. Network effects imply dominance at scale but whether that means monopoly, duopoly, or oligopoly is very different to predict. Just because a market has the properties of "it is better if everyone in the world does X," doesn't necessarily mean that it will be so (e.g., systems of weights and measures, competing global wireless standards). And there are often exogenous, unknowable factors (e.g., web search: search has tended to monopoly in the rest of the world but in the US has remained 30% non-Google due to Microsoft's persistent non-market subsidy). So even if governments decide to compete with Bitcoin, we might see a world where the US-backed ledger is the de facto standard for the developed world, but there are a cluster of third world economies where Bitcoin still dominates.

- Finally, because of Bitcoin's pseudonymous, distributed structure, government action may not necessarily lead to its demise. We won't go as far as many Bitcoin bulls who will argue that it is "untouchable" from government intervention, but it is certainly more protected than any other currency, ever. The criminalization of something does not necessarily lead to its eradication and this should especially be true for Bitcoin.

2. Technical risk

As a technical system, Bitcoin has demonstrated remarkable resiliency. Attacks on Bitcoin have come not on its core technical architecture but on the third party intermediaries such as the Mt. Gox exchange.[4] While social engineering and "weakest link" hacking will always present some risk for any technical system, two aspects of Bitcoin are particularly worrisome:

- First, most of the protections are theoretical and not testable. While the current SHA-256 block hashing algorithm that ensures Bitcoin's security is NSA-grade, it is possible that the cryptography is hackable; the rebuttal to this is something along the lines of: "by the time that happens, Bitcoin will have leapfrogged to the next level of cryptographic security and it will be trivial to migrate the system" or "if you can hack Bitcoin's cryptography, we have bigger problems" (though, not clear what is a bigger problem than hacking the world's money supply). Bitcoin also is dependent on the sum total of the world's distributed computing power dedicated to Bitcoin being larger than what any single actor could muster (with another handwave of "if you can muscle that much compute power, it's not in your interest to hack Bitcoin, you're better off participating as a miner or using it somewhere else")

- Second, Bitcoin is not fully autonomous. It requires some management by humans, and all the weaknesses that entails. Take the "blockchain" fork that occurred on March 11th 2013.[5]

[4] [redacted]
[5]

"Developers are currently holding an emergency discussion in #bitcoin-dev to determine a way forward"

For an open source, distributed, and in many ways deeply subversive/disruptive computing project that is dependent on mainstream adoption to succeed, even a statement as innocuous as this is deeply troubling. At $1B market cap, it may not be an issue. At $100B, the competing agendas, politics, capabilities, and fallibilities of the Bitcoin development community become magnified and inescapable. Perhaps no worse than central bankers, but the devil you know….

- Third, the unknown unknowns of an experiment like this are massive. We have tried to articulate what we see but remain humble about what we don't yet know.