Separating activity from growth on Bitcoin's network

One of the contentious areas of writing about Bitcoin data and emerging markets, is discussing what conclusions and interpretations (if any) can be drawn from say, transactional volume.

Let us put that aside for a moment and consider ways to estimate real commercial volume. Are there any other ways to do so besides a full traffic analysis?

Sell side pressure

On any given day there are at least three entities that continuously sell bitcoins onto the market: merchants (and merchant processors), miners and mining manufacturers (who are sometimes paid in bitcoin).

As I noted in my previous article, last month BitPay announced that it was processing about $1 million in daily payments. It is unclear what amount of bitcoins that constitutes, depending on the time frame and therefore price levels (early December or the month of May) it could represent 1,000-2,000 tokens per day.

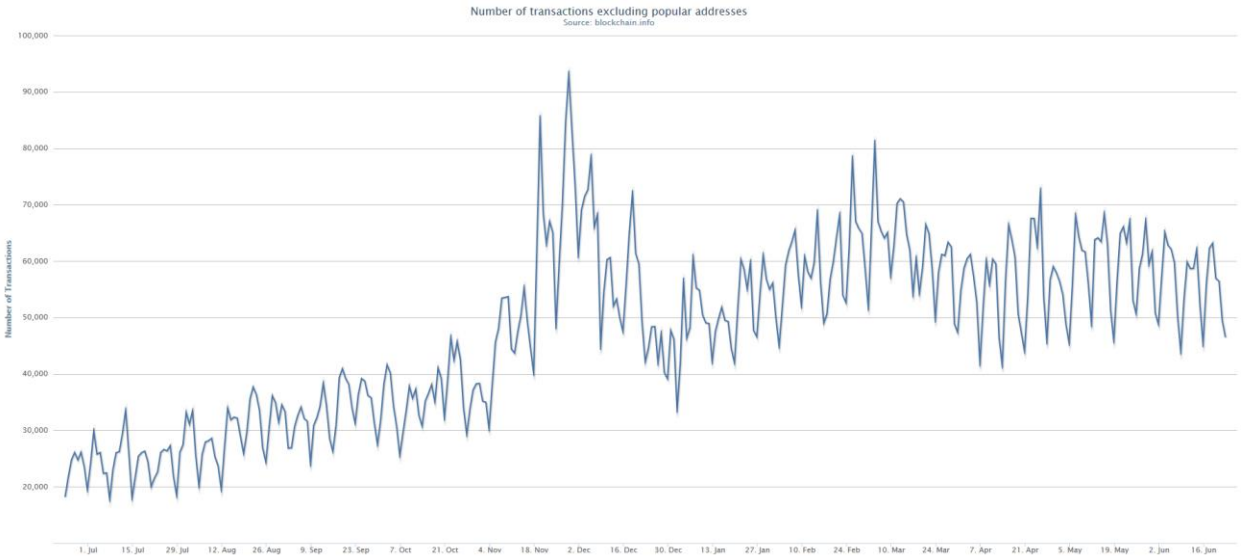
Let us assume that the other merchant processors such as Coinbase and BIPS are also processing a similar amount. And that altogether between 5,000-10,000 bitcoins per day are collectively being spent on commercial activities through these processors.

This puts pressure on the sell side of the price equation. That is to say, to minimize exposure to volatility, nearly all merchants elect to immediately convert bitcoins into fiat and those bitcoins are sold onto the market (both Ben Edelman and David Evans have written on this before).

Similarly, because miners have to pay real costs – capital and operating costs – they too sell their mining rewards on the market: around 3,600 each day (because again, MV=MC).

It is unclear how much mining manufacturers have to sell each day to fund their own developmental and logistical operations, but for the sake of simplicity and roundedness, let us say 1,400 bitcoins (it could also be as little as zero).

Thus altogether, there is a regular 10,000 – 15,000 bitcoins representing commerce that are sold daily on the market today. It also bears mentioning that, although technically the miners receive money, virtually all of it is spent towards utility (electricity) and hardware, not on the bitcoin ecosystem itself. While it is unclear how much other positive-sum value exchange is taking place (such as remittances, houses or cars) we can see that the transactional volume of potential commerce has remained flat during the past six months:



Is there a chart that shows this amount of transactions?

In my last article, I mentioned Total Volume Output – the total value of all transaction outputs per day – yet this includes coins which were returned to the sender as "change" and thus the real number trying to be measured is substantially less. And taken to its maximum readings, roughly 1,000,000 bitcoin outputs (UTXOs) are used each day.

If only 10,000 – 15,000 bitcoins are being used in real commercial activities (instead of merely zero-sum activities like gambling, mixing of coins or cybercrime), then the *perceived* Total Volume Output is potentially two orders in magnitude *larger* than the real economy.

What is the real economy? While the debate over what percentage of bitcoins are being spent in positive-sum activities, between October 15 and December 18 of last year, 41,928 bitcoins were sent to addresses controlled by Cryptolocker (a type of malware) – this is not real economic growth, in fact it is negative-sum. And because it signaled to the market that it was a successful way of generating (stealing) wealth, there are numerous copycats using similar methods (including CryptoDefense and Cryptolocker 2.0).

The cost of information security

For the moment, let us ignore the buy side of the equation, that in order to keep the same price level, at least 10,000 – 15,000 bitcoin are being acquired by other parties each day (primarily high-net worth individuals and institutions through OTC brokers).

What this actual activity translates into is the following:

Miners are the labor force that secures and processes transactions. And because this labor force has real depreciating capital costs and operating expenses, in theory, the cost for their services amounts to roughly $2 million per day (3,600 bitcoins X $600 per bitcoin).

In practice however, most miners are operating at losses. In fact, the network is vastly oversecured by miners operating at losses probably by a factor of 2-5x (described in Estimated costs). For instance, according to a recent report from the National Science Foundation (NSF), a now-banned researcher

used, "about $150,000 worth of NSF-supported computer use at the two universities to generate bitcoins worth about $8,000 to $10,000." Or in other words, the researcher externalized the real costs of mining (energy and capital deprecation) onto another party (the NSF and therefore taxpayers). This is inefficient, yet there are many cases of such activity taking place each day.

Thus while the Bitcoin 'trust fund' (a more accurate description for the network which divvies out a finite amount of block rewards) pays out security of $2 million each day, the labor force is providing significantly more security than they are being paid, probably closer to $6 - $10 million if not more (Hass McCook has additional estimates).

Simultaneously, they are providing these services for commercial activity that ranges from as little as 5,000 bitcoins to perhaps as high as 15,000 bitcoins. Or $30 million to $90 million respectively in today's prices.

For comparison, MasterCard spent $299 million on their capital expenditures in 2013. As part of these expenses, it builds data centers similar to the "fortresses" (with moats) that Visa has also built. In 2013, MasterCard and Visa processed a combined $7.4 trillion in purchases. Together with American Express and Discover, these four companies generated $61.3 billion in revenue during the same period.

While this is not an entirely apples-to-apples comparison, what this means is that the Bitcoin network is enormously oversecured compared with other transactional platforms. The reason this is, is because it is decentralized which creates overhead (since all the nodes have to process and verify the transactions). Yet, as shown with GHash.io over the past month, the network is qualitatively insecure due to economies of scale. That is to say, so as long as the proof-of-work mechanism can be economically scaled, this leads towards centralization. No amount of white papers or tweets will change that.

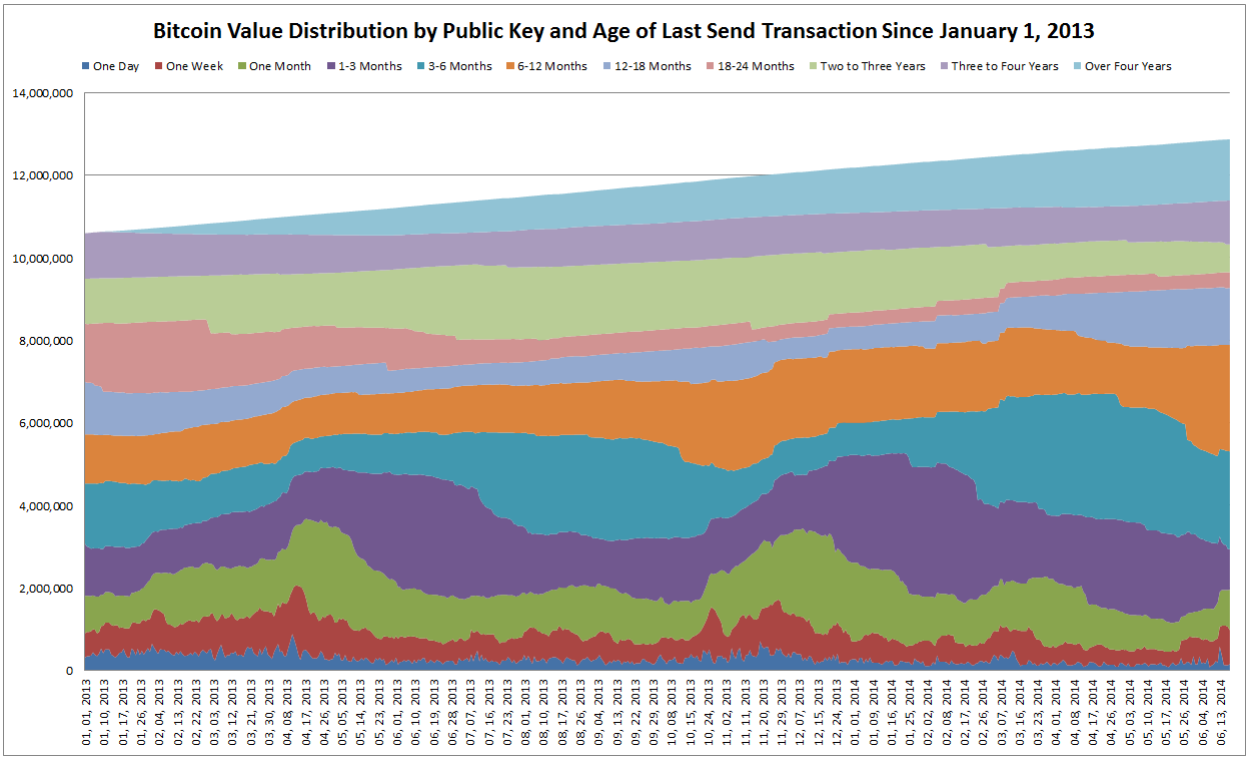
If the labor force of bitcoin is spending $10 million on protecting the network yet real commerce is only $30 million, this would be equivalent to a mall issuing 1 out of 3 customers a personal security detail to go shopping. Or in other words it is, arguably, quantitatively oversecure (it is not qualitatively trustless as shown by GHash.io and previously, Deepbit). Perhaps this mix will change over time. However one thing to consider is that some bullish advocates contend that the Bitcoin network will one day supplant and compete head on with Paypal and even Visa. In order to do so, the Bitcoin labor force are still (assumedly) being paid a fixed income to provide the same services. Thus perhaps in the future, the opposite will occur – the network could become undersecure due to *disproportional* rewards.

I spoke with Greg Simon, co-founder of Cryptowerks who worked as head of International Equity Sales for JP Morgan in Japan. According to him,

> Cryptoledger miners are Japanese banks. They are producing an oversupply of crypto trust relative to an under supply of borrowers of that trust. Their only solution, producing an ever increasing supply of crypto trust, is making the problem worse, not better. It is the equivalent of central bank QE [quantitative easing], or pushing on as string. Just as an oversupply of central bank produced money causes the value of each unit of money to decline, so does an oversupply of crypto ledger miner produced crypto trust cause the value of each unit crypto trust, which we can measure in units of ghash, to decline. The problem is not the aggregate supply of crypto trust. The problem is aggregate demand for crypto trust. Until demand for crypto trust improves, either from monetary or non-monetary borrowers, we can expect the same fate for

crypto trust in the crypto economy as we are seeing for fiat money in the legacy central bank fiat economy.

Another way to visualize this phenomenon is the chart below:



John Ratcliff recently published an explanation about zombie bitcoins (coins, or rather UTXOs, that have not been active in more than 18 months) which is where the chart above comes from. Each color band represents the last time a private key corresponding to these UTXOs was used.

Thus, one take-away from this chart is that liquidity – as shown by the One Day, One Week and perhaps One Month bands – represents between 100,000 to 2,000,000 bitcoins. What is the actual number? Without a full traffic analysis we probably will never know.

But we can tell from spikes that the largest movements take place during volatile time periods, specifically during price run-ups. So, for instance, in the spring of 2013 there was enormous Western media attention and a subsequent boom that peaked in mid-April (when Mt. Gox had to temporarily shut down). Similarly, in November and early December corresponds with additional global media coverage and Chinese adopters coming online – with prices peaking on December 4th. Or in other words, transactional volume rises and falls with price levels – that the bulk of on-chain activity corresponds primarily to day trading and speculation. This, despite the fact that Ratcliff notes, that prices during this 18 month time span increased 4,000%.

That is to say, even though there are more than 100,000 merchants that accept bitcoin and even though token valuation has risen logarithmically, UTXO holders as a whole prefer speculating over conducting actual commercial activity. What could change this behavior?

Maybe nothing will because Bitcoin is a recreation of a medieval agrarian economy; few people spend, in part because the network codifies what is essentially negative time value of money.

Money and credit

There is an endless stream of papers and books on the topic of what constitutes and attributes of money. Arguably one of the most thorough explanations of what money is and how it arose is, *The Ascent of Money* by Niall Ferguson which was later turned into a good PBS series.

Despite what some Bitcoin advocates claim, gold itself was not used on a large scale since time immemorial. In practice, there were numerous types of physical assets ranging from metals to stones. England even used a system of money known as tally sticks for several hundred years. And the reality is that prior to the birth of civilizations, many tribes and villages operated with barter and gift systems with themselves and one another (some never even created something akin to "money").

As noted by Ferguson, up until the Renaissance, there were no real financial instruments or professionalized banking or hedging methods in the West. Bonds, joint-stock corporations and insurance companies evolved throughout time (all post-Fibonacci). And consequently, this is reflected in the dearth of economic output at the time. That without a way to expand credit – to create loans to start businesses – the pie cannot be enlarged. In his words, "Credit and debt, in short are among the essential building blocks of economic development, as vital to creating the wealth of nations as mining, manufacturing or mobile technology." In contrast, poverty (subsistence) more often, "has more to do with a lack of financial institutions, with the absence of banks, not their presence."

Thus, I would argue that ultimately Coinbase could turn into a fully-fledged bank, providing interest to bitcoin holders to be able to loan out bitcoins (much like BTCJam does). And they could do this through a fractional reserve process. In fact, Huobi's new Hong Kong branch (BitVC) is heading in that direction; users can lend funds to Huobi for interest and Huobi will then lend it out to users to trade on margin. Contrary to what many Bitcoin adopters contend, fractional reserve banking itself is not inherently a bad thing but that is a topic for another article.

However, for the time being, Coinbase and others – while on-ramping a lot of new users and providing utility through ease-of-use functionality – have a long way to go before this occurs. For instance, this past week Coinbase announced instant buyback (once you spend bitcoins, you can buy more). However, the reddit comment below sums up actually what happens:

[–] **coelomate** 13 points 1 day ago

The optics of this from the outside are terrible.

With many sellers instantly converting to fiat, this literally turns coinbase into a giant transaction fee with no bitcoin necessary to get from A to B.

On top of that, what might feel rational to you as a bitcoin supporter looks like zealotry and fanaticism from the outside. You really want to immediately buy back the coins you use, to try and stimulate commerce without needing to spend bitcoin? Sounds like a mix of hoarding and pumping and dumping...

permalink save report give gold reply

Again, there is a difference between the economy Bob wants to have versus the economy Bob currently has. Today Bitcoin, as I have argued, is at most an emerging market akin to a pre-industrialized agrarian economy with enormous frictions. Internally it is an inflexible command economy that outsources and arbitrarily rations its scarce resources (block rewards) irrespective of economic conditions (e.g., Bob, the miner, is rewarded whether or not he processes transactions). Front loading rewards the first four

years without processing any transactions is an unsustainable activity. In fact, as Jonathan Levin, co-founder of Coinometrics, notes in his upcoming paper, *Creating a decentralised payment network*, he found that "[i]n total over the network history there have been 84,469 blocks with no transactions." Yet because there is no one at the helm, no entrepreneur to rationally allocate block rewards or market value for those rewards the first year, ultimately 4.2 million bitcoins were given out for naught.

Many adopters note that this was done to help bootstrap the economy and that the initial distribution of bitcoins through the block reward is purportedly not how bitcoin will operate in the long run. And that at some point Bitcoin's internal economy will somehow be incentivized by transaction fees only – or at least that is theoretical transition (see Reducing and removing block rewards). But the fact that miners were rewarded irrespective and arbitrarily of their actual work is very similar to how top-down command economies work rationing wages. This is a topic that will likely be debated over the coming years.

For additional perspective I spoke with Martin Harrigan, a software developer and founder of Quantabytes, a cryptocurrency analytics start-up. In his view:

> The initial distribution of bitcoins is a one-time process that is distorting our understanding of the Bitcoin economy. I think that the peaks in transaction volume during the price run-ups are a form of secondary distribution: early adopters are distributing their bitcoins, for profit, to new users. This is a vital part of Bitcoin's distribution process and may continue for as long as there are periods of significant price increase. It may be that institutional investors will take-over a significant portion of this process for several years. Then, at some point, when the technology, infrastructure, regulatory frameworks, and our understanding of cryptocurrencies has matured, the price will stabilise and Bitcoin will return to individual users as a stable transactional currency in the traditional sense.
>
> Of course, I'm speculating wildly here. My point is that we don't have a good null model. We're not seeing "hockey stick growth" but maybe that's okay. Many start-ups need this type of growth to survive -- I don't think Bitcoin does. During the Bitcoin crash of 2011 the price dropped 93% and didn't recover until 2013. The difficulty also dropped and remained stagnant for a year and half. Although I can't quantify it, the "mood" on the Bitcointalk forums was grim. The equivalent event would have been fatal to most start-ups.

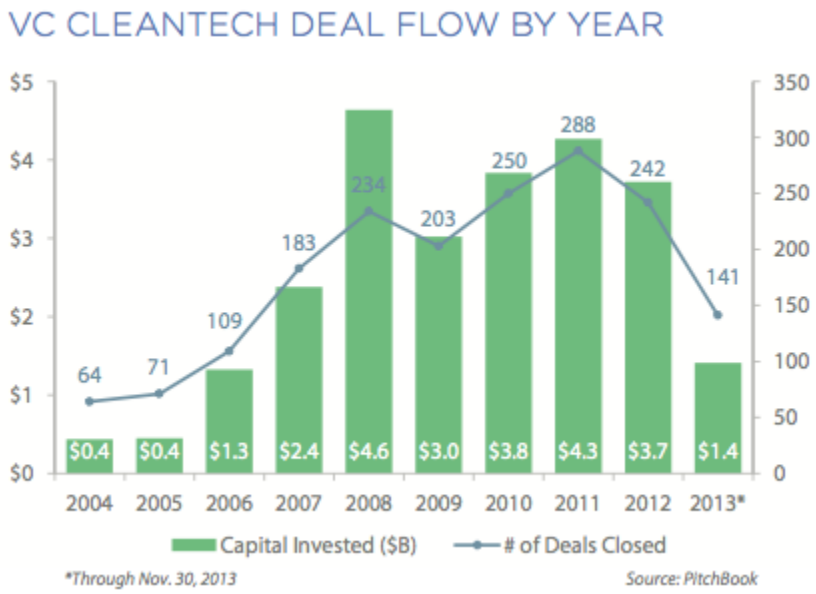
Perhaps at Harrigan noted, this will change in the future. And perhaps those frictions are still lower than the cost of doing business in certain regions (like the Philippines). And this is not to single-out Coinbase. I still think they are one of the best companies in this space, I even consider them one of the most promising in part because they are trying to create value (and have). But that does not mean this particular service is frictionless. For instance, David Evans recently delved into the specific transaction costs of various platforms and explained how the actual roundtrip cost of Coinbase is 2% + $.15, not the 1 percent that is frequently cited (Evans also had another good explanation of how Coinbase and merchants like Overstock work).

Building a continuous series of bubbles or building utility

One of the common refrains about altcoins and appcoins in general is that none of the underlying systems are able to give out real equity and thus cannot have P/E expectations – neither does bitcoin, nor will it. This is a bug and it is why I argue that using the "TCP/IP" analogy is probably incorrect. The

internet is an amalgam of private-public intranets cobbled together and cost real capital to build. It was not built with magic; real incentives had to be provided to build it. Imagine if those incentives decreased 50% every 4 years? That's Bitcoin's internal economy. The Bitcoin network cannot operate without bitcoins – the app or currency or commodity (choose your definition). The two are united together. Yet TCP/IP, the protocol, can still work even if substantial portions of the network fail; it is not tied to a specific set of hardware or token (TCPIPCoin).

This is not the first time a set of unrealistic expectations have been created in the past 10 years.



So what kind of bubble is bitcoin then? Some claim that it "crashes upwards" which makes no rational sense at all. Bitcoin (the token) is not immune to the laws of economics. Perhaps as illustrated above (source), the current investment cycle in Bitcoin is more akin to Cleantech circa 2005? What this means is that, as noted in my previous article, even though many of the startups are clever, they may lack sustainable business models. Once this froth is removed, the businesses that survive will likely be those that are actually creating real pain killers (utility) to real needs; perhaps reusing the infrastructure of the network (like merged mining proposed by Blockstream or that of Cryptowerks) to process contracts and titles. Again, all of this is speculative, yet it warrants attention because Cleantech also had a similar dedicated ideological group of early adopters that created economic activity (though, not much growth yet) and wanted to change the world. And despite their best efforts it popped.

In conclusion, expanding credit alone is not the answer to Bitcoin's stagnant economy. For instance, China's money supply grew leaps and bounds since November 2008 (when it implemented a series of stimulus packages). It also signed bilateral currency agreements with new countries every year which led many outside commentators to erroneously conclude that this somehow leads to mass adoption of the RMB. Yet the stark reality is that the RMB only accounts for 1.4% of global payments compared with the dollar at 42.5%. This is unlikely to change either. However, even in its current doldrums, the Chinese economy still produces real goods and services to the tune of trillions of dollars per annum. Obviously it is unfair to compare Bitcoin, a five-and-a-half-year old "startup" to China. Yet the emerging market aspect, the reuse of capital stock, the implementation of new financial instruments, the training

of unskilled laborers and ultimately the creation of needed utility to outside parties can be viewed as facsimiles to learn and grow from.

As noted by John Kenneth Galbraith in the last article, there is only so much capital that can be extracted from the "fleece-me" crowds of reddit. Significantly more capital is needed to scale operations to enterprise-level reliability. While some advocates believe eschewing the *ancien* regime of venture funds and private equity is the way to move forward, this is short-sighted.

Below is a list of companies I think have potential to create value in this digital ecosystem – embryonic solutions to this quagmire (I hold no equity in them):

- API: Chain, Blockr, HelloBlock, BlockCypher, HiBitcoin
- Analytics: Coinalytics, Coinometrics, Blocktrail, Quantabytes
- KYC: CoinTrust, Block Score, Coin Validation
- Decentralized cloud: MaidSafe, StackMonkey, decloud, Bitcloud, StorJ
- Lending: BTCJam, Bitreserve, Bitfinex
- Peg: Netagio, Ripple Singapore, Digital Tangible Trust, Melotic