A Marginal Economy versus a Growth Economy

By Tim Swanson

Revised June 3, 2014

[Note: this is a follow-up response to the corresponding Let's Talk Bitcoin #116 podcast. A PDF version of this article is available. The opinions in both the podcast and article represent my own and not those of anyone I have interviewed.]

What is the accurate analogy to describe Bitcoin the protocol? Is it like TCP/IP, SMTP and the interstate highway system? Or is it more akin to a developing economy?

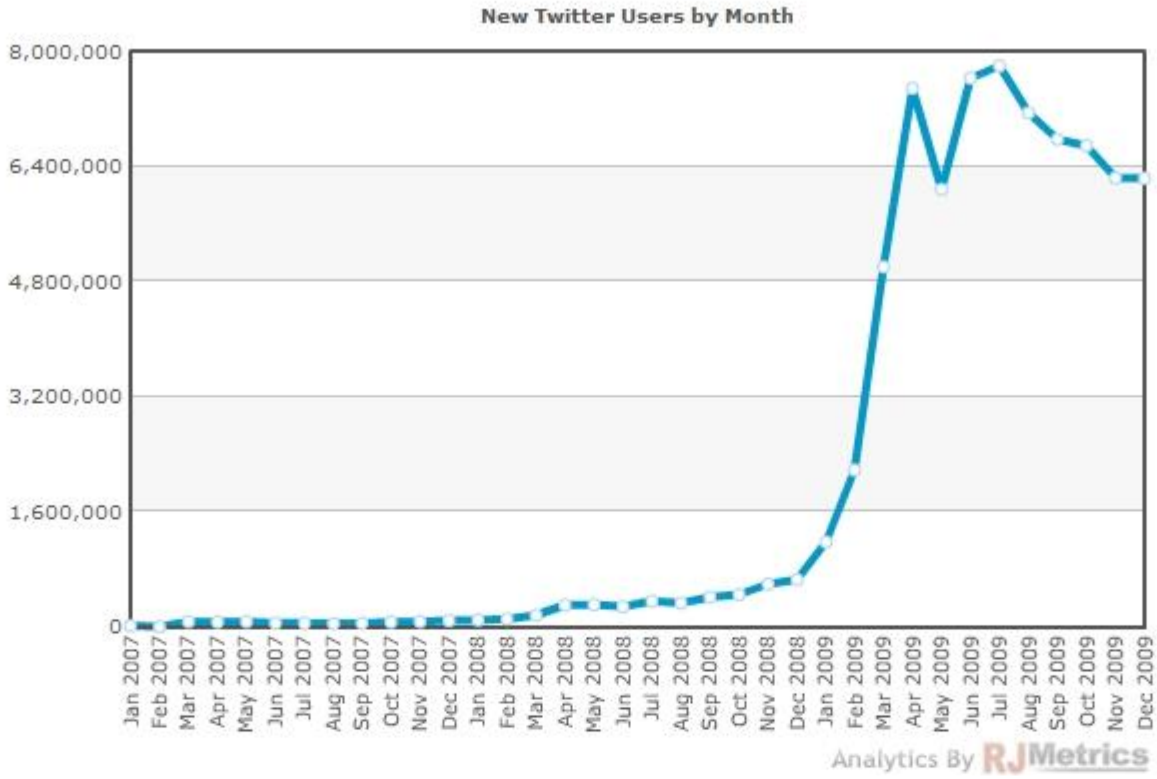
It could be the latter. That Bitcoin could be seen as a small developing economy that is capital-starved, has an underdeveloped industrial base and contains a glut of underemployed human residents. In short, it suffers from many of the same ailments of a poor, developing country. And over time, with investment, education and improvements in protocol (infrastructural) capabilities, the ecosystem may flourish.

If the purpose of Bitcoin is to create a trustless bilateral consensus mechanism to empower the underbanked and simultaneously provide incentives to bootstrap the economy throughout its germination stage, then at some point its users, entrepreneurs and ecosystem will necessarily need to create enterprises that provide real genuine economic engines of growth. Today however, this is not the case and that is one of the reasons for why there is no visible "Hockey Stick" growth curve that takes hold with many other viral applications. As illustrated below, despite the enormous amount of free publicity it has had, that other platforms like Square or Stripe would love to have, there is arguably no pain point that Bitcoin solves (yet) for the developed world.

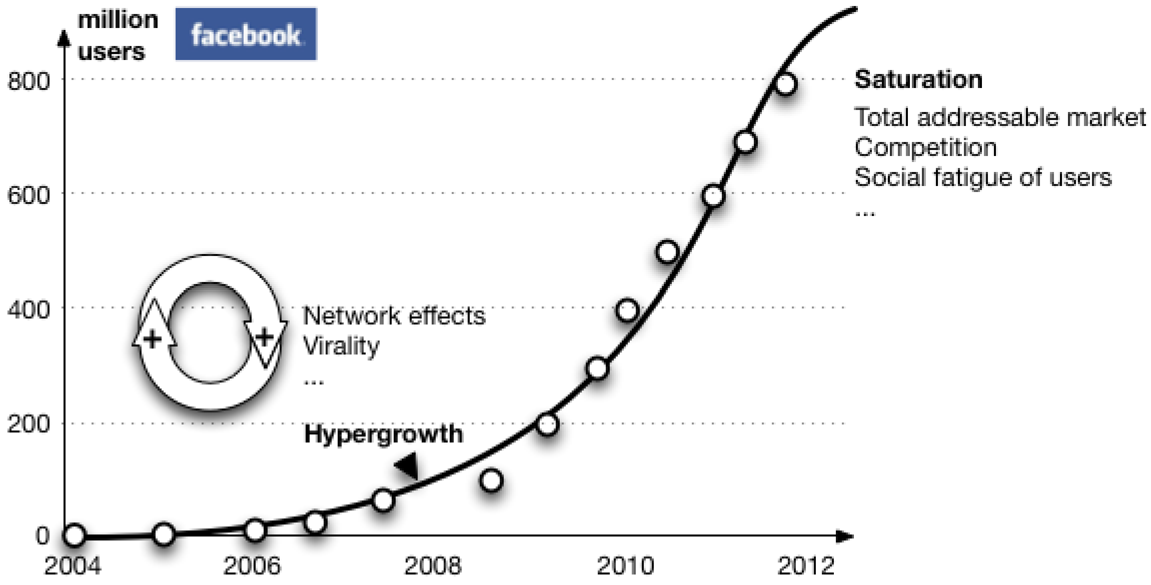
If the stated goal by adopters in the developed world is to supplant the financial functions of Wall Street (which likely will not happen) or compete with the payment rails of Visa (which will also likely not happen) then investors, developers and entrepreneurs need to build replacement businesses and integrate them with the blockchain – and not just publish whitepapers.

What does a successful adoption rate curve look like?

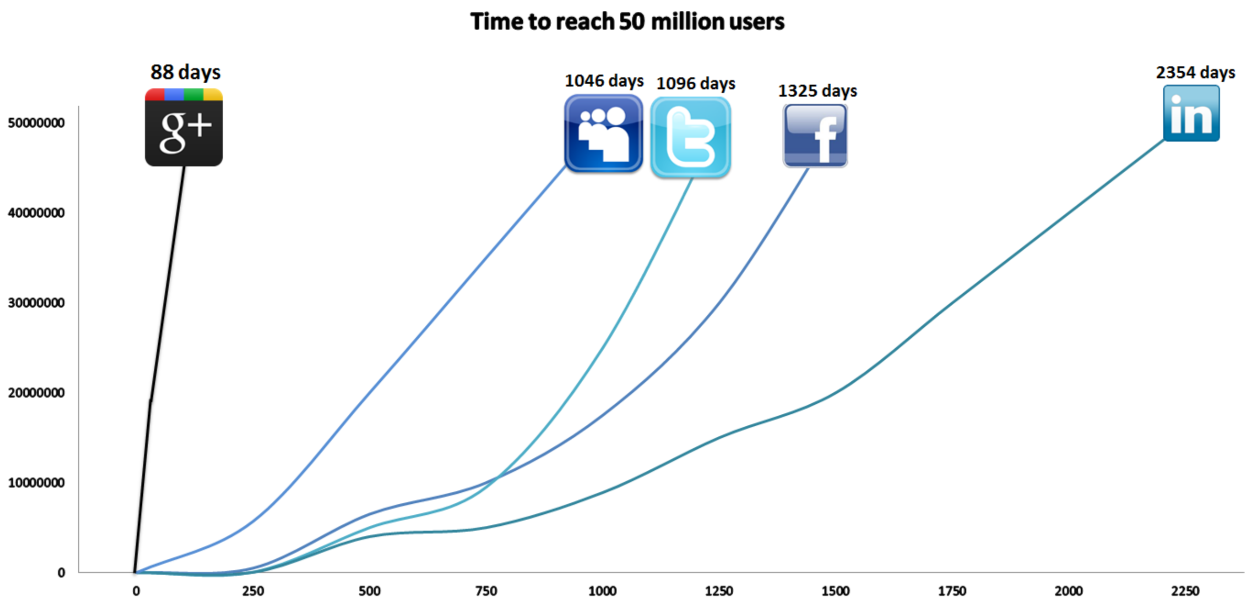
For instance, this chart from RJMetrics illustrates the Hockey Stick of Twitter:



And this was what Facebook's S-curve looked like (source):



What time frame did the large social media platforms reach 50 million users? Below is a chart illustrating this:



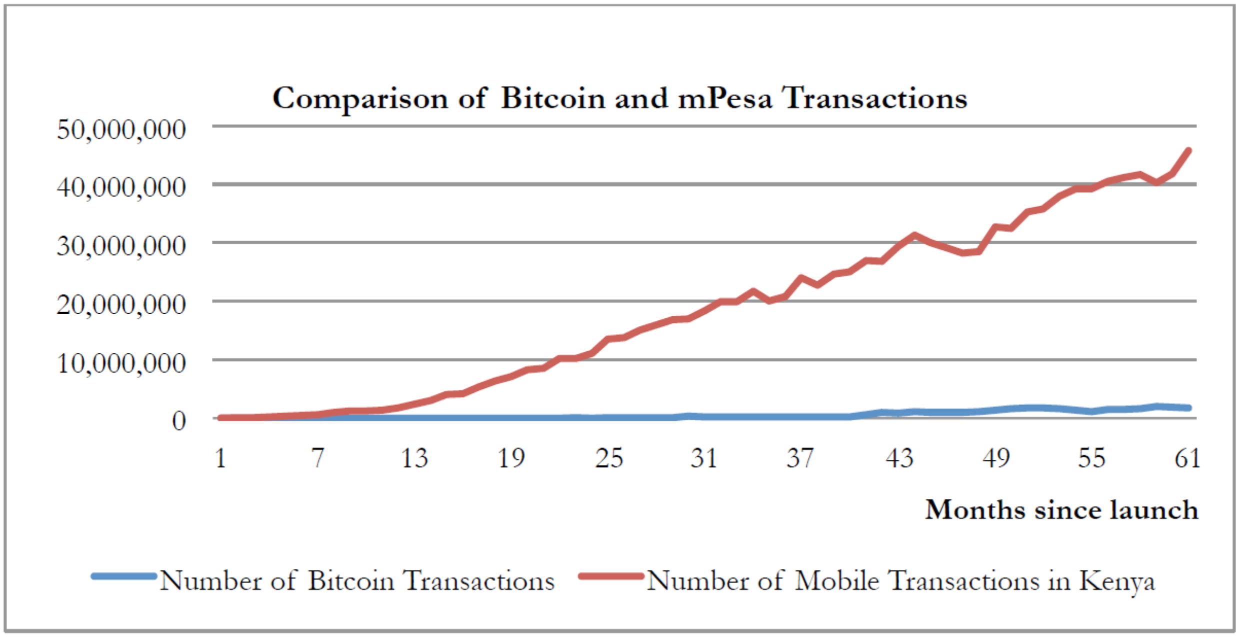
by +Leon Haland
http://goo.gl/bFaCl

I spoke with Mark DeWeaver, who is the author of one of the first books to chronicle China's post-1949 financial history and cofounder of the Quantriarian fund. According to him, "The thing about developing economies is that they usually seem to be held hostage by special interest groups that insist that development must proceed along a path that doesn't threaten their interests. So they tend to end up with what the political scientist Fred Riggs called "prismatic development"— a Potemkin version of the development seen in advanced countries. If it's like a developing country, it could be stuck where it is now pretty much forever."

While this issue will likely fill volumes in the coming years (I have briefly written about it before), there are several special interest groups in the Bitcoin ecosystem, one of which exists as a form of *regulatory capture*: miners. Miners (transaction processors) are the sole labor force and will only hash and protect code that is profitable to them. The proof-of-work security mechanism at the heart of the protocol will likely never be switched to something less capital intensive like proof-of-stake or even tree chains. In other words, while there may be a hypothetical scenario where Bitcoin could evolve to some more energy efficient block verification model, this is unlikely possibility because the majority of miners will likely never agree to it due to their sunk costs. Thus, even though there have been several proposed improvements to the protocol to alleviate and mitigate some of the long-term technological and economic challenges (such as block reward halving), these might not be incorporated because the labor force could simply fork the code and carry on with the *status quo*.

However perhaps these are unfair comparisons. Bitcoin, the network, might not be a developing economy. The definition of a developing economy may apply to Bitcoin just as little as saying it is simply a currency. It could merely be a money-like informational commodity (or perhaps "factum" money as Vitalik Buterin and Max Kaye have proposed), which we still have to figure out how to use; like cavemen discovering fire and burning their fingers – we may be currently in the burning fingers stage. The charts above showed that Bitcoin does not follow the hockey stick curve compared to companies built on the internet. However, if Bitcoin compares to the internet itself then future usage charts may end up comparing more with internet traffic from the late 1960s and early 1970s with Bitcoin "traffic" starting in 2009. Time will tell on that account. Furthermore, let us assume that Bitcoin is a company and we compare it to Facebook. When Facebook was born, the legal environment it operated in was more or less well defined. This is not the case with Bitcoin as it faces many uncertainties in various jurisdictions which could be preventing wider adoption. Therefore a more fair comparison could be in the future, starting at the point when the regulatory framework of Bitcoin and other cryptoprotocols are less nebulous and more concrete by each member of the G-20 (or some other arbitrarily large percentage of the world economy).

One last comparison is with another payment platform which started at roughly the same time, below is Bitcoin (blue) versus M-PESA (red) from David Evans. M-PESA is a popular mobile payment system operated by Safaricom and Vodacom and serves more than 30 million users in East Africa (Kenya and Tanzania), the Middle East and India. 43% of Kenya's GDP flows through the M-PESA system.

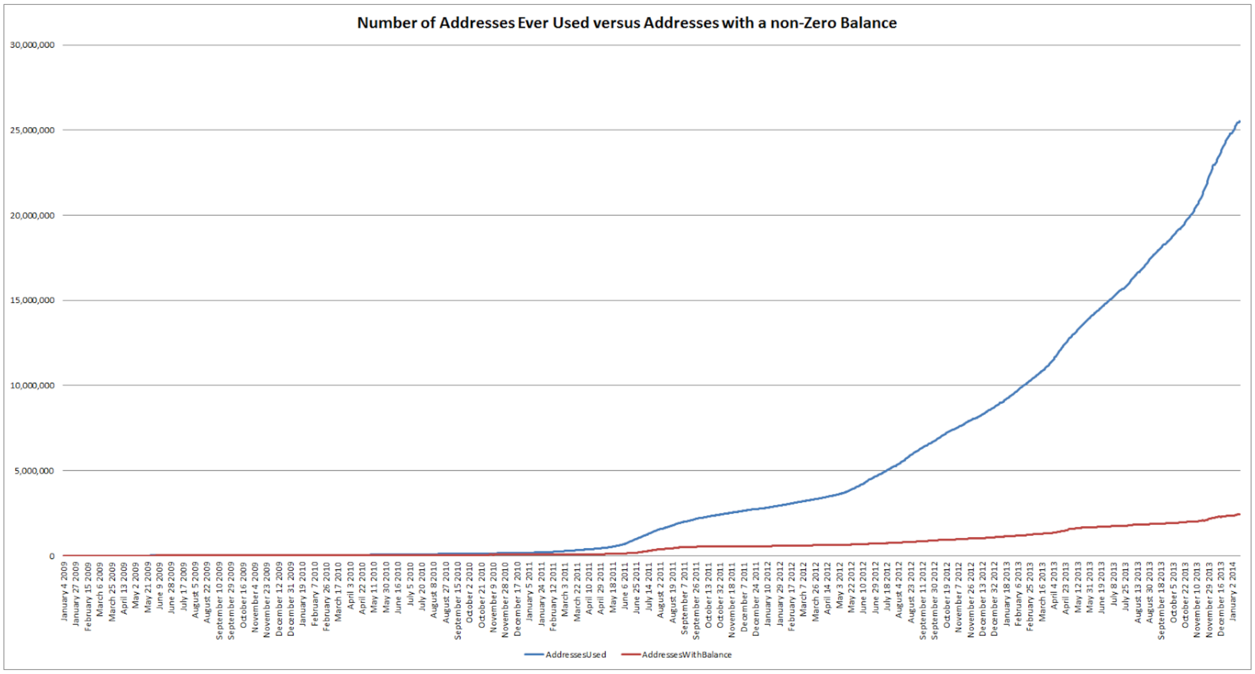


Source: Compilation with data from quandl.com for Bitcoins and Central Bank of Kenya for mPesa

How many users?

The actual amount of bitcoin users is relatively difficult to precisely know (due to its pseudonymous nature) yet a rough estimate of 250,000 – 500,000 is probably an accurate range. Despite the hype there are *not* millions on-chain (yet). For instance, according to the Bitcoin Distribution Chart approximately 309,793 addresses contain 99.1% of all bitcoins (UTXOs). While some individuals and companies control multiple addresses, this likely means that less than half a million people have funds on the Bitcoin network (Jonathan Levin of Coinometrics mentioned this figure at CoinSummit as well). Some of these addresses are invariably controlled by firms like Circle and Coinbase (which create ease-of-use and utility for the network), however because they are off-chain this creates a trusted third party vulnerability negating the primary purpose of a blockchain (though I probably would trust these two).

Furthermore, comparisons with price level increases and address growth are not the same as user growth. I restate below what I have previously written on this topic (see explanation for first chart in Background):



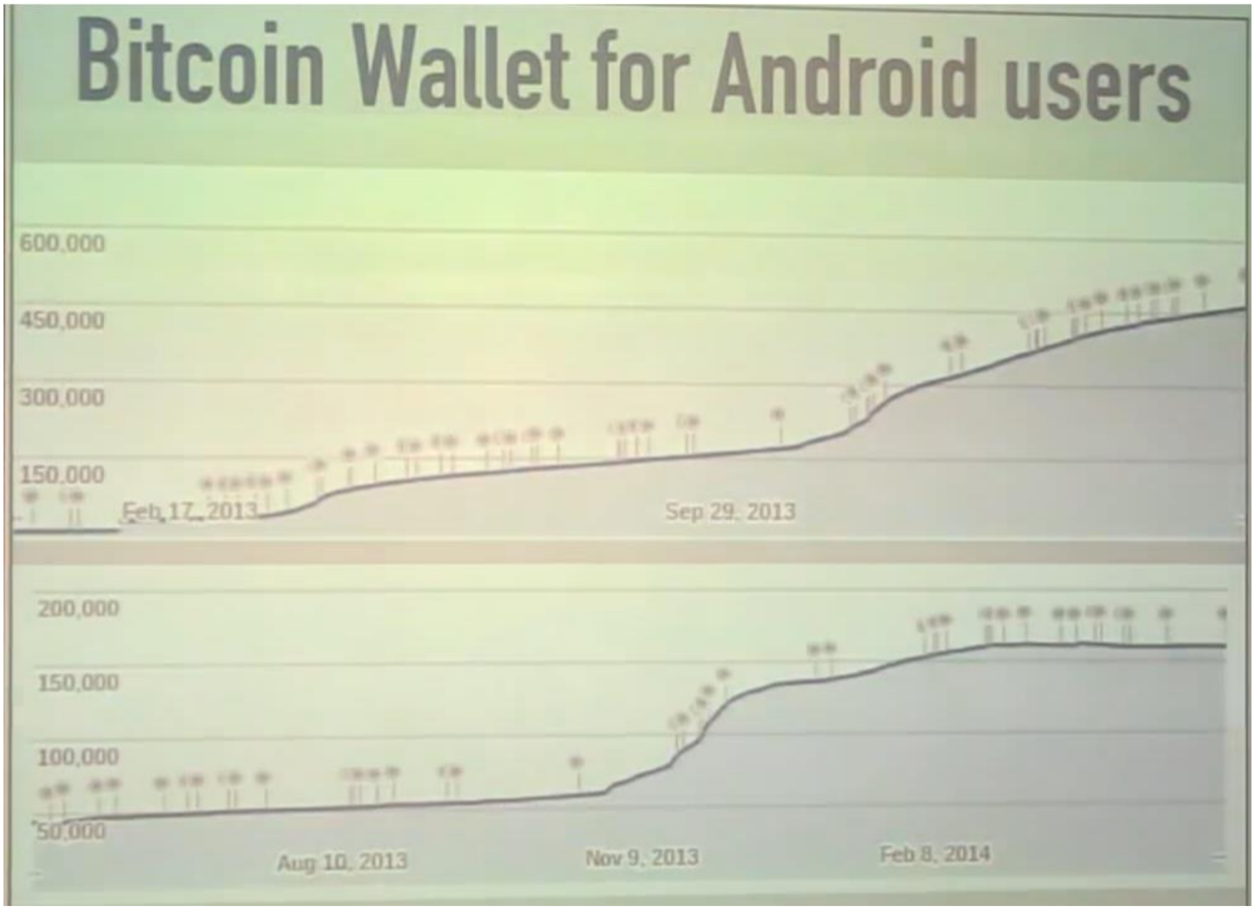
This chart (above), compiled by John Ratcliff, shows the aggregate number of addresses ever used on the Bitcoin network between January 2009 through January 2014. The blue line represents what are essentially spent addresses – addresses used as "intermediate steps" (i.e., using a new address per transaction, or to identify amounts received from particular payers). The red line illustrates addresses with bitcoins (UTXOs): that there are roughly only 2.5 million addresses on-chain with a non-zero sum of bitcoins. This is not the whole number of actual bitcoin holders however because multiple addresses are often owned by one person or company to mitigate the risk of loss in the event that the private key for one or several of these addresses is compromised.

It should also be noted that addresses themselves do not "contain bitcoin," they correspond to signing keys which can be used to redeem unspent transaction outputs (UTXOs). There is a conflated, semantic meaning used in non-technical publications yet from a technical perspective, it is more accurate to use UTXO rather than addresses as "payment buckets," since addresses are essentially just UTXO labels (many thanks to Andrew Poelstra for clarifying this for me).

Permanent beta mode

Many proponents claim that Bitcoin is still in beta mode, that it is too early for a real comparison because infrastructure is still being laid. This may be the case, perhaps the hockey stick will come later. Or maybe, as Mike Hearn (a Bitcoin core developer) hypothesized two weeks ago, perhaps it will remain a niche (akin to desktop Linux):

[insert embedded video: http://youtu.be/2MtUKr05Y3I]



The top graph (from Hearn's presentation) shows the total amount of Android Bitcoin wallet installations. The bottom graph is the total active installations of Bitcoin wallets (first graph minus uninstalls). According to Hearn, "At the end of February Bitcoin stops growing and I argue that this app is a very good proxy for Bitcoin usage overall because the top graph up here matches very well with Blockchain.info and other wallet providers that have been released. It correlates very well with other data that we have. The bottom graph what it shows is that at this point we are losing users as fast as we are adding them."

We cannot know for certain whether it will remain a niche *a priori*, this is an empirical matter. Instead we can only look back on what we have used it for, what needs it solves today – and for most people who have knowledge of a private key, they use it for speculation and hoarding. One way to illustrate and view this phenomenon is through token movement on the blockchain. Below is a visual aid created by John Ratcliff and described at length in this article:

[insert embedded video: https://www.youtube.com/watch?v=SbA913dLfYU]

While it is speculative to guess what the exact motivation for these token holders are, it is clear that only a small fraction is liquid, most is illiquid. Perhaps these tokens were lost, stolen or seized. Maybe the users have psychologically moved beyond merely "saving" tokens to "hoarding" them. While this topic warrants several follow-up papers, "hoarding" does not grow economies either – only savings do because savings are lent out entrepreneurs who attempt to build and create utility. Hoarders may claim that they are providing some kind of reserve demand that creates price pressure thus incentivizing others to come into the market, yet again, this issue raises challenges that intersect with the Prisoner's Dilemma (like someone has to eventually build the museums for hoarders relics) and are best left to other more focused papers on that topic.

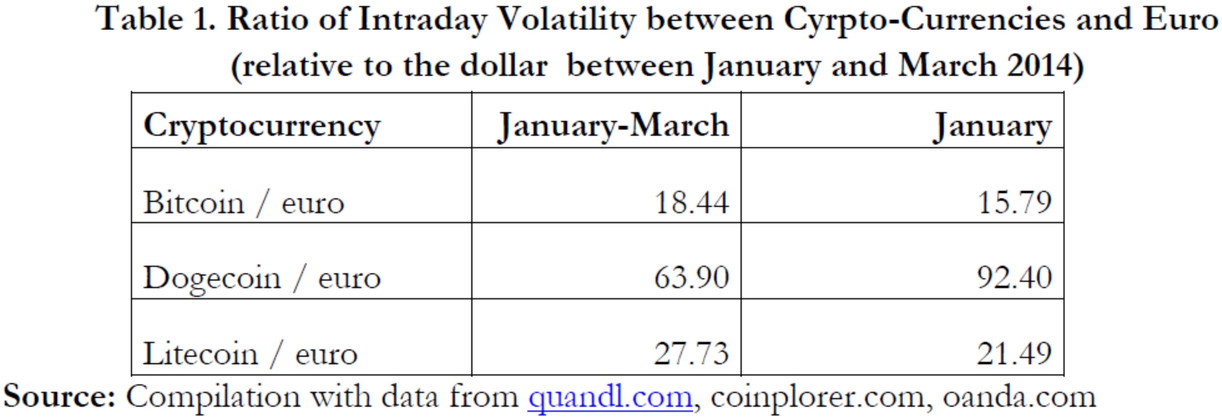
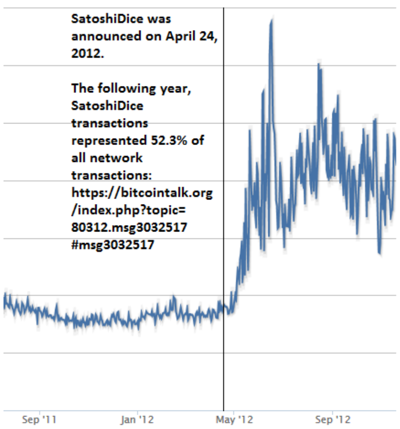


Table 1. Ratio of Intraday Volatility between Cyrpto-Currencies and Euro (relative to the dollar between January and March 2014)

Cryptocurrency	January-March	January
Bitcoin / euro	18.44	15.79
Dogecoin / euro	63.90	92.40
Litecoin / euro	27.73	21.49

Source: Compilation with data from quandl.com, coinplorer.com, oanda.com

What this illustrates then is that bitcoins are not currently fulfilling the role of both a store of value and a medium of exchange. Again, this is a lengthy topic that is probably best discussed by Robert Sams "growthcoin" and Ferdinando Ametrano's "stablecoin" publications which also describe how volatility is a factor. In practice, volatility is a poor property for a medium of exchange to have – bitcoin values were 18x more volatile than the euro in the first quarter of 2014 (see Table 1 from David Evans above). Furthermore, it is the implication of wanting to hold cash for the transaction motive. In practice, people are risk adverse, and the existence of transactions costs mean more costly rebalancing of the medium of exchange that balance the more volatile the medium of exchange. Perhaps as some have suggested, when bitlicenses are issued this summer, new institutional participants will provide larger amounts of volume and liquidity, subduing some of the volatility.



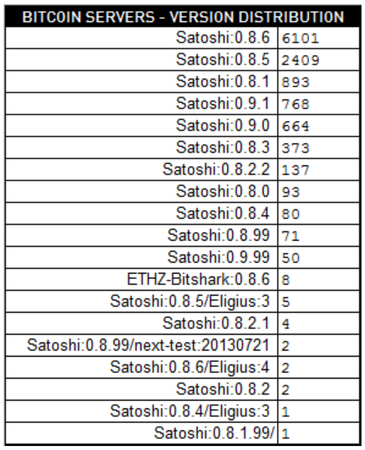
SatoshiDice was announced on April 24, 2012.

The following year, SatoshiDice transactions represented 52.3% of all network transactions: https://bitcointalk.org /index.php?topic= 80312.msg3032517 #msg3032517

Source

If one builds a tool that has few immediate uses besides gambling then it should not be surprising that mostly gamblers use it. As shown in the adjacent chart, this illustrates the before and after of when SatoshiDice came online in the spring of 2012. According to calculations by "Dooglus" and also confirmed in A Fistful of Bitcoins, SatoshiDice represented 52.3% of the entire networks transactional volume within a year. This is not to make a target of SatoshiDice, they provided a service that apparently was quite popular with the existing user base (or perhaps on-ramped new users, or both). However, based on statistics, most people do not gamble or trade in illicit wares for a variety of reasons. Perhaps this is just a temporary phenomenon as the network bootstraps itself, though if history is any guide, few countries developed and joined the OECD strictly because of this type of economic activity.

While the legal and ethical reasons could be debated, that is the topic for a different paper and venue. In practice, if illicit activities were real economic engines instead of mere channels for entertainment, then Macau and Las Vegas would be the economic pillars instead of Shanghai and New York. The latter have a certain *je ne sais quoi*. If Bob want people (customers) who are non-gamblers or patrons of licit-trade, then Bob needs to build tools for them beyond merchant services. Instead of building "dark markets" for illicit trade, one could build and market tools for sustainable economic activity. For instance, one would not fly to Beijing and tell the political class that the reason they are stagnating is due to a lack of casinos and narcotics. In contrast, one way to measure economic growth is through total factor productivity (TFP) – measuring the increases in productivity for each input. Traditionally the way to make the same inputs (human capital) more productive is through education, training and technology. One of the ways to increase the capital productivity within Bitcoin is through merged-mining, sidechains or in some manner allowing user-created assets beyond the simple ledger entry (note: it should be noted that miners and verification nodes do not immediately jump on board with the latest versions either, the adjacent screenshot was taken a month ago).



BITCOIN SERVERS - VERSION DISTRIBUTION	
Satoshi:0.8.6	6101
Satoshi:0.8.5	2409
Satoshi:0.8.1	893
Satoshi:0.9.1	768
Satoshi:0.9.0	664
Satoshi:0.8.3	373
Satoshi:0.8.2.2	137
Satoshi:0.8.0	93
Satoshi:0.8.4	80
Satoshi:0.8.99	71
Satoshi:0.9.99	50
ETHZ-Bitshark:0.8.6	8
Satoshi:0.8.5/Eligius:3	5
Satoshi:0.8.2.1	4
Satoshi:0.8.99/next-test:20130721	2
Satoshi:0.8.6/Eligius:4	2
Satoshi:0.8.2	2
Satoshi:0.8.4/Eligius:3	1
Satoshi:0.8.1.99/	1

Yet this presents a proportional security issue which I describe later below.

No need to twist facts

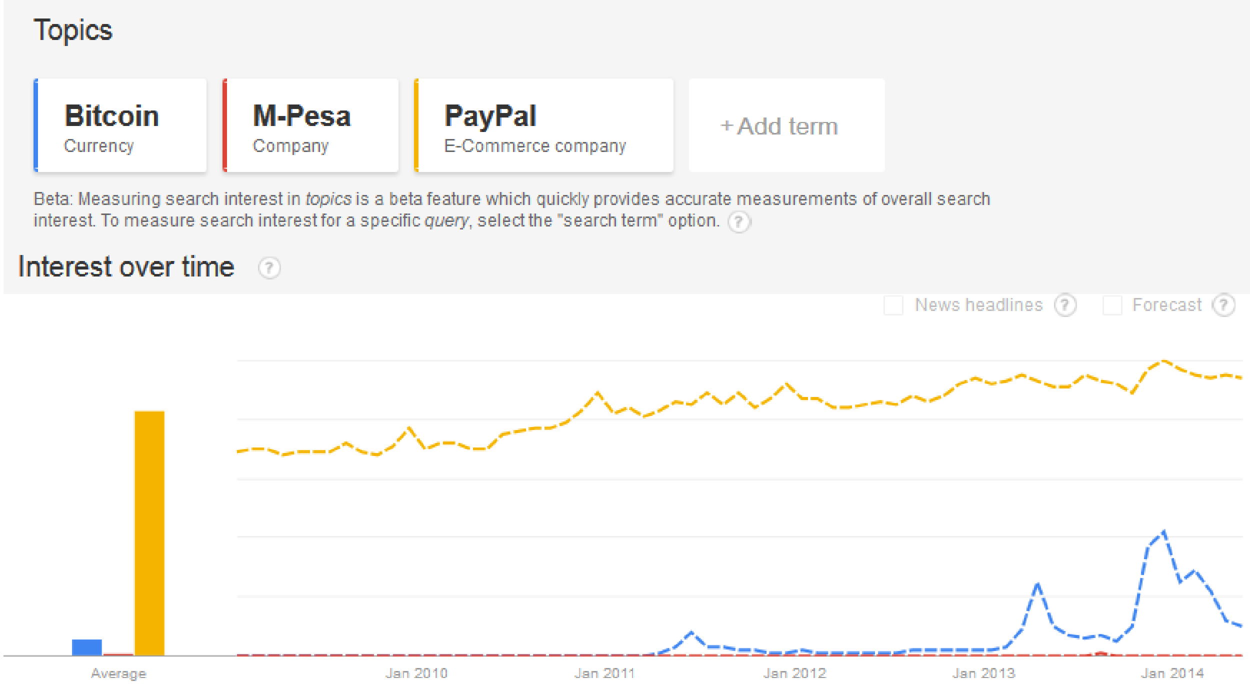
Because of its deflationary nature in the long-run and volatile behavior in the short-run, Bitcoin is not poised to overtake PayPal. There was a recent news report that was uncritically posted at one Bitcoin news site and was upvoted and passed around multiple times. The data it used is cherry-picked. It used the first week of December as shown on Coinometrics, the week in which transactional volume was at an all-time high, to suggest that the "$300 million" in volume would overtake PayPal's. The problem is the volume has fallen to a fraction of that (to roughly 10% of that) and even that number is incorrect because it does not account for mining payments, mixing, gambling and illicit activities. While PayPal likely processes illicit activities, what adopters should want to promote and recognize is actual real commerce and not just entertainment. That's how the average mother and father join networks, because it provides a solution to a real need. So something like houses from Realty Shares, Quickcoin, Digital Tangible Trust, Proof of Existence, OriginStamp, Lighthouse, cloud, compute and storage from StackMonkey, decloud, Bitcloud, StorJ and MaidSafe, payments to merchants selling food, etc. However because of the pseudonymous nature of the blockchain, even with a full traffic analysis, a graph of all the known public addresses would not fully tell us how much actual economic growth is taking place (although researchers may be able to deanonymize other information). Perhaps some is, but there are no known public reports on this yet.

I asked Jonathan Levin, co-founder of Coinometrics about this specific data and according to him:

> While there have been attempts to measure the Bitcoin economy, there is not much convincing evidence of any metrics that are directly analogous to any other system. Transactions on the Bitcoin network serve multiple purposes and should not be taken a qualitatively the same as transactions on other payment networks. We display the daily volume of Bitcoin transactions next to other payment networks as evidence of the potential that Bitcoin has as a payment

system to shift large monetary value. People looking at the number of wallets created on different platforms is not a useful measure of the amount of new users on the Bitcoin network nor the activity. Many people hold wallets with different providers or set up new wallets due to lost passwords etc. We are working hard at Coinometrics to develop metrics that are analogous to real world measures so that investors and businesses can begin to make informed decisions.

The following visual aid (below) shows corresponding interest over time: that Bitcoin usage and demand of bitcoins follows the media cycle (they reinforce one another as Mike Hearn mentioned in the earlier video). This chart compares Bitcoin, M-PESA and PayPal from January 2009 – May 2014 from Google Trends:


Topics

Bitcoin Currency

M-Pesa Company

PayPal E-Commerce company

Beta: Measuring search interest in *topics* is a beta feature which quickly provides accurate measurements of overall search interest. To measure search interest for a specific *query*, select the "search term" option.

Interest over time

Unfortunately Bitcoin has turned a segment of geeks into underwater day traders some of whom are suffering from a Type 1 error, the gambler's fallacy (specifically apophenia); believing that a certain outcome (i.e., a bull market) is necessarily “due” after a long streak of another outcome (i.e., a bear market). And who spend enormous amounts of time and energy creating sock puppets (fake accounts) to pump-and-dump get-rich-quick alts in an effort to compensate for their historically poor trading strategies. And while most alts have a one-dimensional *modus operandi*, some alts provide an excellent method for experimenting with new features, new economic models and new ways of thinking that cannot be conducted with Bitcoin main due to the risk of disrupting several billion in assets. Alts will also probably continue to exist for at least two reasons:

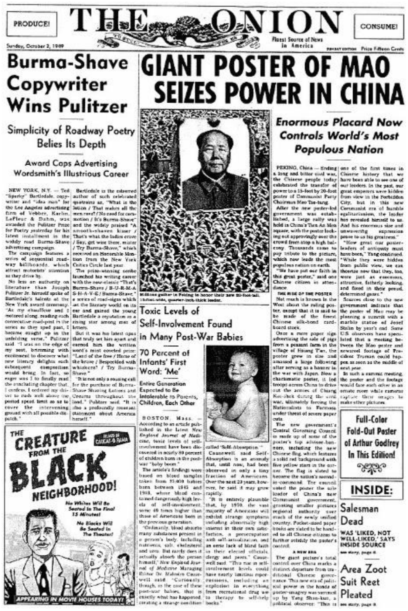
1) Scarce labor
2) Depreciating capital goods

There are few people capable of building a secure blockchain and because Bitcoin operates as a charity organization (socializing labor, privatizing gains) there is no one to pay the developers (yet). Perhaps the new Blockstream (sidechains) project from Austin Hill will be the Red Hat of this space. But currently, the only chains that pay their developers are alts. Thus capable labor continues to go where market rewards are.

The second reason is something many people are familiar with: ASIC mining hardware. ASICs are a depreciating capital good. They only have a certain amount of profitable life time and after this window of opportunity has closed the owners must either unload their capital or turn it towards a profitable alt. And because this code is open-source, some miners have the motivation and capability of creating alts to profit from.

Various individuals on Twitter and Reddit that continue to call for the death of alts are not much different than political administrators in the '60s and '70s who would hold press conferences to "talk down inflation" – this term is called 'jawboning.' It did not work five decades ago and it does not work with alts.

A viable economy or a support group?



PRODUCE! THE ONION CONSUME!

Finest Source of News in America

Sunday, October 2, 1949

SUNDAY EDITION Price Fifteen Cents

Burma-Shave Copywriter Wins Pulitzer

Simplicity of Roadway Poetry Belies Its Depth

Award Caps Advertising Wordsmith's Illustrious Career

NEW YORK, N.Y. — Ted "Sparky" Bartledale, copywriter and "idea man" for the Los Angeles advertising firm of Webber, Karlin, LaFleur & Dahm, was awarded the Pulitzer Prize for Poetry yesterday for his latest installment in the widely read Burma-Shave advertising campaign.

The campaign features a series of sequential roadway billboards, which attract motorists' attention as they drive by.

No less an authority on literature than Joseph Pulitzer Jr. himself spoke of Bartledale's talents at the New York award ceremony. "As my chauffeur and I motored along, reading each consecutive road-post in the series as they sped past, I became caught up in the unfolding verse," Pulitzer said. "I was on the edge of my seat, brimming with excitement to discover what new literary delights each subsequent composition would bring. In fact, so eager was I to finally read the concluding chapter that, I confess, I ordered my driver to rush well above the posted speed limit so as to cover the intervening ground with all possible dispatch."

Bartledale is the esteemed author of such celebrated quatrains as, "What is the lotion / That makes all the men rave? / No need for commotion / It's Burma-Shave" and the widely praised "A smooth-shaven kisser / That's what the ladies crave / Say, get wise there, mister / Try Burma-Shave," which received an Honorable Mention from the New York Critics Circle last year.

The prize-winning scribe launched his writing career with the now-classic "That's Burma-Shave / B-U-R-M-A S-H-A-V-E / Burma-Shave," a series of road-signs which set the literary world on its ear and gained the young Bartledale a reputation as a rising star among men of letters.

But it was his latest opus that truly set him apart and earned him the written word's most coveted prize: "Land of the free / Home of the brave / Bespeckled with whiskers? / Try Burma-Shave."

"It is not only a rousing call for the purchase of Burma-Shave Shaving Lotions and Creams throughout the land," Pulitzer said. "It is also a profoundly resonant statement about America herself."

THE CREATURE FROM THE BLACK NEIGHBORHOOD!

FILMED IN CAUCAS-O-RAMA

No Whites Will Be Seated In The Final 15 Minutes!

No Blacks Will Be Seated In The Theater!

APPEARING IN MOVIE HOUSES TODAY!

GIANT POSTER OF MAO SEIZES POWER IN CHINA

Millions gather in Peking to honor their new 20-foot-tall, 15-foot-wide, quarter-inch-thick leader.

Toxic Levels of Self-Involvement Found in Many Post-War Babies

70 Percent of Infants' First Word: 'Me'

Entire Generation Expected to Be Intolerable to Parents, Children, Each Other

BOSTON, Mass. — According to an article published in the latest *New England Journal of Medicine*, toxic levels of self-involvement have been discovered in nearly 80 percent of children born in the post-war "baby boom."

The article's findings were based on blood samples taken from 55,000 babies born between 1945 and 1948, whose blood contained dangerously high levels of self-involvement, some 40 times higher than those of Americans born in the previous generation.

"Ordinarily, blood absorbs many substances present in a person's body, including nutrients, salt, cholesterol and urea. But rarely does it actually absorb the person himself," *New England Journal of Medicine* Managing Editor Dr. Malcolm Causewell said. "Curiously, though, in the case of these post-war babies, that is exactly what has happened, creating a strange condition called 'Self-Absorption.'"

Causewell said Self-Absorption is an anomaly that, until now, had been observed in only a tiny fraction of Americans. Over the next 20 years, however, he said it may grow rapidly.

"It is entirely plausible that, by 1970, the vast majority of Americans will exhibit strange symptoms including abnormally high interest in their own satisfaction, a preoccupation with self-actualization and an eerie lack of blind faith in their elected officials, clergy and peers," Causewell said. "This rise in self-involvement levels could have nearly limitless repercussions, including an explosion in everything from recreational drug use to therapy to self-help books."

Enormous Placard Now Controls World's Most Populous Nation

PEKING, China — Ending a long and bitter civil war, the Chinese people today celebrated the transfer of power to a 15-foot by 20-foot poster of Communist Party Chairman Mao Tse-tung.

After the new poster-led government was established, a large rally was held in China's Tien An Men square, with the poster looking out approvingly over the crowd from atop a high balcony. Thousands came to pay tribute to the picture, which now leads the most populous nation on earth.

"We have put our faith in this great poster," said one Chinese citizen in attendance.

THE RISE OF THE POSTER

Not much is known in the West about the ruling poster, except that it is said to be made of the finest Chinese silk-bond cardboard stock.

Once a mere paper sign advertising the sale of pigs from a peasant farm in the village of Hsiang T'an, the poster grew in size and amassed a large following after serving as a banner in the war with Japan. Now a charismatic poster, it led troops across China to drive out the armies of Chiang Kai-shek during the civil war, ultimately forcing the Nationalists to Formosa under threat of severe paper cuts.

The new government's Central Governing Council is made up of some of the poster's top advisor-banners, including the new Chinese flag, which features a solid red background with five yellow stars in the corner. The flag is slated to become the nation's second-in-command. The council voted the poster the sole leader of China's new Communist government, granting smaller pictures regional authority over much of the newly unified country. Pocket-sized paper books are slated to be handed to all Chinese citizens to further solidify the poster's control.

A NEW ERA

The giant picture's total control over China marks a distinct departure from traditional Chinese governance. This new era of political power in the hands of poster-imagery was summed up by Yang Shan-kun, a political observer: "This is one of the first times in Chinese history that we have been able to see one of our leaders. In the past, our great emperors were hidden from view in the Forbidden City, but in this new Communist era of humble egalitarianism, the leader has revealed himself to us. And his enormous size and unwavering expression prove to us his greatness."

"How great our poster-leaders of antiquity must have been," Yang continued. "While they were hidden from public view, we can theorize now that they, too, were just as enormous, attractive, fatherly looking, and fixed in their proud, determined gazes."

Sources close to the new government indicate that the poster of Mao may be planning a summit with a marble statue of Josef Stalin by year's end. Some U.S. observers have speculated that a meeting between the Mao poster and newsreel footage of President Truman could happen as soon as the middle of next year.

In such a summit meeting, the poster and the footage would face each other in an ornate room while cameras capture their images to make other pictures.

Full-Color Fold-Out Poster of Arthur Godfrey In This Edition!

INSIDE:

Salesman Dead

WAS 'LIKED, NOT WELL-LIKED,' SAYS INSIDE SOURCE

see story, page 6

Area Zoot Suit Reet Pleated

see story, page 8

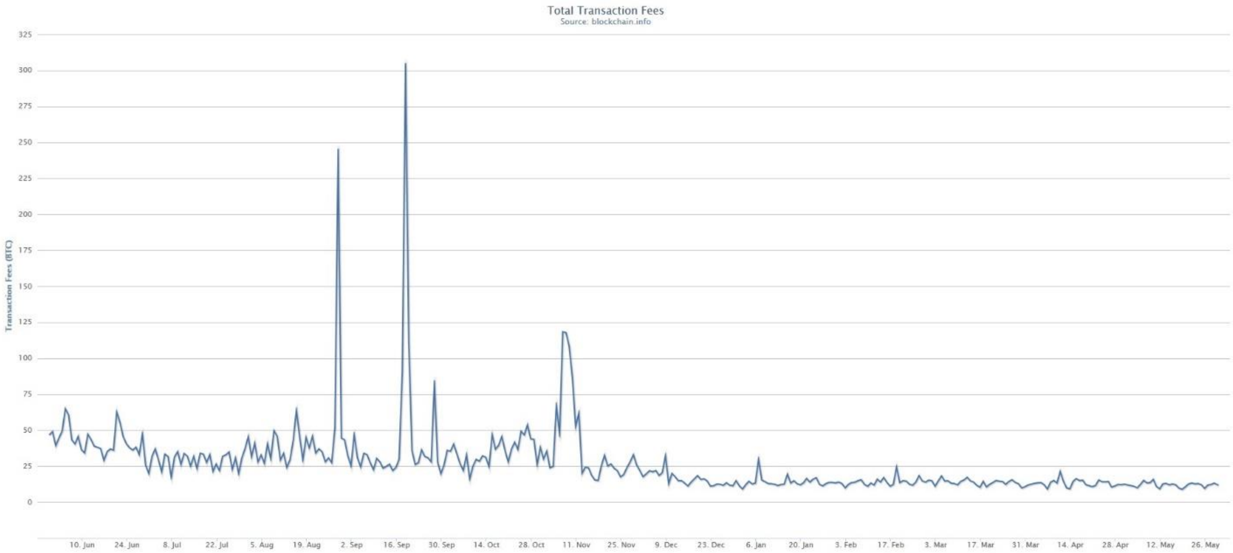
Source

The mythos of Satoshi has been taken to the extreme and turned some advocates into creating a mini cult-like apparatus just as the Red Guard deified Mao during the Cultural Revolution. However this is unproductive and likely only fans the flames of outside criticism which includes the same skilled people that any country or ecosystem needs to survive and thrive. Instead, remove the purple cloak, set down the Kool-Aid and get ready to accept that as an open-source protocol it will likely be used as an agnostic tool. Institutions, enterprises and governments will take what is useful to them and internally incorporate it. And they will probably not change their own existing behaviors or worldview just because someone hopes they do. The direct historical facsimiles would be with the F/OSS movement in the early '90s. A small vocal group of GNU advocates believed that tools like Linux would revolutionize and democratize regimes like China. But in point of fact, the Chinese government simply absorbed the technology and used it for its own goals, erecting a powerful digital funnel called the Great Firewall which allowed them to survive the information age – an age that would bring them a loss of face (*diu le mian zi*). They adapted and most likely other governments and institutions will do the same with this technology. Satoshi, whomever he, she or they are, were brilliant and should be acknowledged for creating this very interesting experiment. However, the clique of self-appointed Satoshi purity police are reminiscent to the brilliant "cult of personality" parody from *The Onion* (above) – it is likely counterproductive.

The abstract and Section 1 of Satoshi's whitepaper describes the trusted third party vulnerability in the payments and exchange space. Similarly, the title of the paper suggests that bitcoins will be used for a peer-to-peer electronic payment system. Satoshi even intended to build a P2P marketplace inside the protocol itself, but later removed the code.

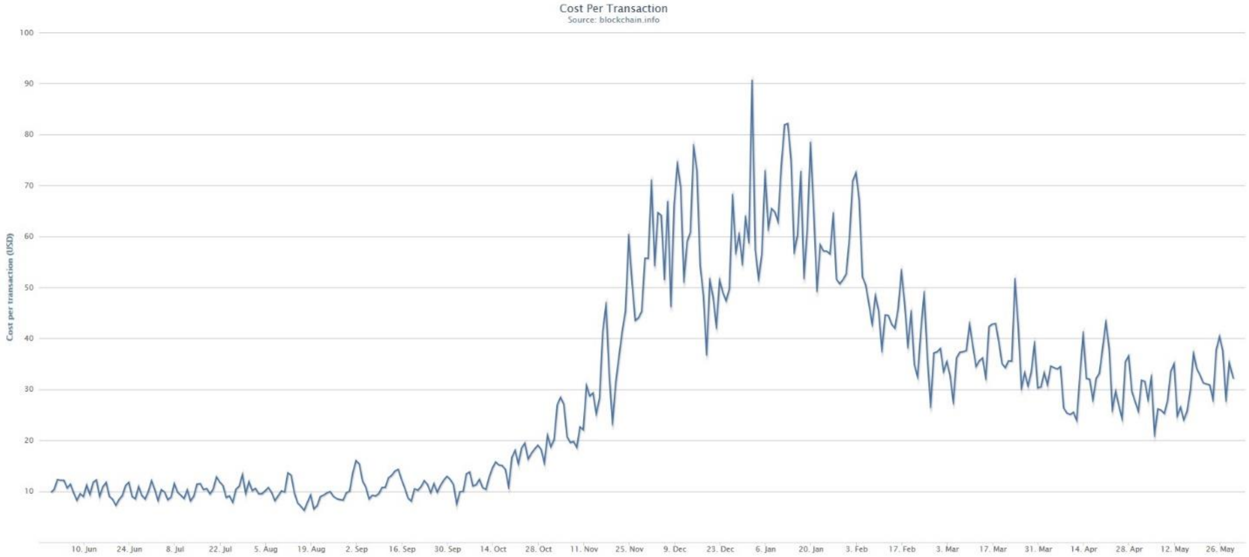
Yet in practice what has happened is that once there was a market rate for bitcoins, behavior switched from a Dogecoin-like faucet service (note: tipping is just a redistribution mechanism, it is a poor market signaling mechanism) to a money-like informational commodity. In short, economically rational actors treated bitcoins (and the protocol) based on its core qualities: a deflationary (in the long-run) inelastic money supply. Spenders are uninterested in having to deal with a volatile currency or one they have to pay to use. This price volatility coupled with the expectation of price appreciation incentivized people to hold it. And once you remove the popular addresses such as the gambling sites, there may be some real economic commerce taking place on the chain, roughly 60,000 transaction per day. That may sound like a lot, but it is not. At the beginning of the year there were an estimated 20,000 to 30,000 merchants and that figure has doubled to more than 60,000 in the past quarter. Yet there is no subsequent increase in on-chain transactional volume (as noted by Hearn in the video above). Though perhaps volume is merely at the early part of the curve where it is not clear what the trajectory is.

Another way to view that is through the total fees that users pay to miners. At the time of the writing, fees represent roughly 0.31% of the total labor force (miners) revenue. Based on endless threads of people complaining about not wanting to pay fees, we see this free-riding ("cheapskate") challenge first hand in the chart below. This chart (source) illustrates the total transaction fees, the total bitcoin value of transaction fees miners earn per day.



Why, as new users discover, should you have to pay a fee for something that is supposedly free? It's not free. This false marketing campaign is a big disservice to the innovative protocol and its hard working core developer team (who are underappreciated by the market). Nothing is free. In fact, because Bitcoin is decentralized, it has an enormous amount of overhead that centralized systems do not have to maintain. As a consequence, the true cost of a Bitcoin transaction is significantly higher, $40 per *tx* at the time of this writing. This is paid for through token dilution, better known as inflation (note: the discussion of inflation versus deflation with respect to Bitcoin has gone on since at least November 2008). Every 8-10 minutes the money supply (monetary base) of the Bitcoin network increases by 25 bitcoins (it will halve again in mid-2016).

Another analogy for looking at this situation is that five years ago what Satoshi effectively created was a charity, Bitcoin, which oversees 21 million gold coins in the form of a trust. In the charities by-laws roughly every 8-10 minutes it is required to donate 50 gold coins to the local neighborhood watch – a volunteer labor force that also doubles as crooning postmen. Every 4 years, the amount that the charity donates divides in half, so that within a hundred years, the entire trust is depleted. These gold coins never actually leave the trust, rather, each coin is divided into bearer bonds, so that one coin represents 100 million individual bearer bonds such that 50 gold coins is technically 5 billion individual bearer bonds. In return, the labor force has to simultaneously do two things in order to be eligible for the bearer bonds, semantically referred to as gold coins. It has to protect the charity from outside attackers (disguised in similar clothes) by filling out reams of Mad Libs until they found one specific page that actually makes logical sense. Assailants too would also have to fill out reams of Mad Libs in order to try and gain access to these bearer bonds. Whoever found that page and crooned it first was eligible to receive the next donation. The page that was crooned was then mailed to each volunteer whom collected the pages in an ever-growing stack. The other task for the labor force if that if someone sends mail requesting one of these gold coins, paying a postage fee in the process, it needs to transmit (croon) the request and any change of gold ownership to all the other laborers. And over time, these services are expected to be compensated not by donations from the trust but by postage fees (transaction fees) from spenders. Whether this happens or not in the long-run is an empirical matter, but as of this writing, this does not seem to be the behavioral trend.


Cost Per Transaction
Source: blockchain.info

The chart above (source) shows the mining revenue divided by the number of transactions. It illustrates what Gavin Andresen (a Bitcoin core developer) pointed out two weeks ago in Amsterdam, that if Bitcoin became more popular (and thus the demand for tokens increases creating token value appreciation), the transaction fee itself (which was recently slashed ten-fold) would likely price out a significant portion of the intended consumer base: poor people. Obviously no one directly paid even $90 at its height in December, the cost was borne by every holder of bitcoin through token dilution.

Why do fees matter? Why not remove fees altogether?

When Bitcoin was first released there were no fees yet later on a fee was added to prevent spam – if it costs Bob nothing to send transactions across the network, then there is no penalty to discourage him from that behavior. Oppositely, if it costs Bob money to spam the network, he has an economic incentive not to do so. And if there is one certainty it's that the behavior of the original Bitcoin actors, it's that they were anything but predictable. Building a tool and expecting it to change a user's behavior is an unrealistic expectation and thus the anti-spam safety mechanism.

What about fees in the future?

The core development team plans to float the fees, "smartify" it so that the fees reflect the supply and demand of the block (the scarce resource). That is to say, there is a public goods problem with Bitcoin. The hashrate is being treated (by the protocol) as a non-exclusionary, non-rivalrous good that can be used by anyone with a private key. Yet there is a scarce resource, a private good called a block which is provided by miners (the labor force). To ration this scarce resource, markets typically implement usage fees. However the way miners are primarily paid today (~99.69% of their income) is through the block reward subsidy. Every 4 years that subsidy decreases by 50% with the belief that transaction fees will replace the block reward. However in practice, this is a wild card because no one currently likes to pay fees but would rather free-load on the charity of miners.

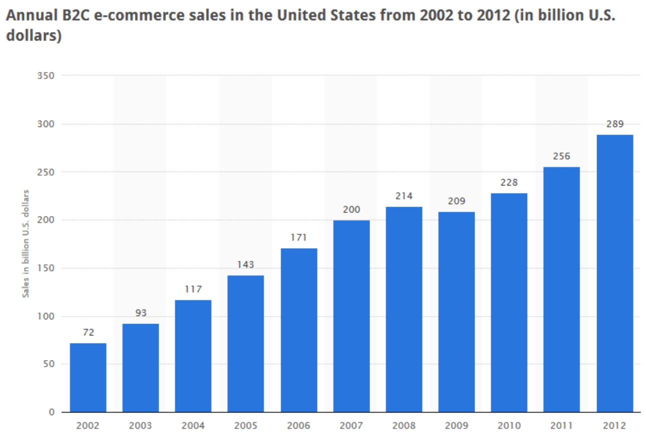
This creates a major dilemma for expansion. Two years from now, when the blockreward halves again in all likelihood the hashrate will decline like it did previously and has done on many other chains, including notably Dogecoin. There are exceptions to why Bitcoin survived and grew following the first halvingday and of course price increase expectations could incentivize the labor force (miners) to continue providing security and transactional utility. Yet there are at least two problems that the network will face by that time:

1) Colored coins decouple the value of the network from the reward miners get for securing it (good comments from here, I am not crypto-tim)
2) Fee free-riding

I recently described (not my title) the first issue, which as new financial instruments such as smart contracts are added and are represented by a fraction of a bitcoin through a colored coin schema, that there is currently no automatic way to proportionally incentivize the security of that same asset. For instance, if Bob issues $20 billion in bonds through colored coins and the Bitcoin network is only rewarding $10 billion worth of security, then there is an incentive for Bob to conduct a 51% attack on the network in an attempt to swap the debt with a debt-free chain he created in a double-spend attack. Obviously this is speculative but so as long as MV=MC (the marginal cost of a token equals to the marginal cost of securing it) then there is little wiggle room.

The reason there is little wiggle room in the security subsidization game is because of existing behavior. We expected people to use the network as a payments platform, this did not occur. We expected people to create utility that would on-board the developed world, but instead built apps for other – perhaps temporary – entertainment activities. We expect people to pay higher transaction fees to offset the diminished seigniorage subsidy and this may not happen. Thus, when colored coins, metacoins, smart contracts and other financial instruments are added to the chain, this could create a network of its own undoing (though probably will not as the code could change, engineers are creative).

Just the first inning?



This is not to say that Bitcoin is imminently doomed or will fail – and again – there are known solutions to nearly all of the technical challenges above. Furthermore its network effects and dedicated community will keep it going for many years to come. Nor is the takeaway that I am "anti-Bitcoin" – rather I think that once the hype and hyperbole is dispensed of, the underlying tech (especially the "2.0" variety) is clever and potentially transformative later this decade for certain segments.

In addition, even though it has been a five and a half years since the genesis block it does not mean that the ecosystem has been fully rolling that long. Significant angel and VC investments first started just over a year ago and deals this year are even larger than all previous years combined with a potential for $300 million in VC. It also took a while for internet startups to become useful too. For instance, ecommerce in the US did not catch on until after 2000 (source) and similarly has been going gangbusters in China where it is expected to reach $300 billion this year.

Perhaps what is happening are baby steps, not in the developed world but in the developing through services such as BitPesa, BitPagos, Maicoin, Coins.ph, ZipZap, Coincove and 37Coins. This is where immediate user value could lie for trustless bilateral exchange. Yet even the high expectations and potential within the overseas remittance markets should be tempered with the compliance realities and social engineering challenges that need to be overcome for these cross-border channels (note: the Uganda story turned out to be a false start). However, even if the infrastructure is available, it does not mean adoption. I spoke with James Duchenne, an attorney who grew up in Mauritius and co-founder of Satoshi Legal, according to him:

> Anyone that's lived in or been to Africa can attest to the enormous cultural differences that exist. Thus, to me, the #1 barrier to entry for bitcoin type adoption in Africa is not infrastructure, it is culture & trust. The average African has a culture of "need" and not "want" - the "need" is controlled by those in power and a tacit toleration of corruption is prevalent. Thus, people trust tangible things or things trusted by "trusted people." Anything complex has a very hard time to get off the ground in a grass roots movement unless those in power (the trusted governors) have something to gain from it.

Thus those specific use-cases are mostly likely not relevant in San Francisco, New York, London or other high developed regions with existing effective rails. Simultaneously it may not be fair to expect people starting to use Bitcoin *en masse* before the exchanges, wallets and other basic infrastructure is working properly and is sufficiently easy to use. Mobile is the platform of the future and secure storage is still an issue. However quick, seamless mobile banking is already a reality in some places including notably China with Tenpay and Alipay and Western companies like Google and Apple are rolling out their own mobile payments platforms. Therefore maybe future research should start to look at activities more closely in other parts of the developing world. Who else is building Bitcoin ecosystems in those places?

55% of West Africans live on less than $1 a day. Could these firms create a competitive payments platform in regions where residents make less money than the transaction fees of Bitcoin?

Perhaps the "killer" products and services are gaining traction in the places least expected and are already serving real use cases but they are just still small and invisible to us. Email did not become popular with mass appeal until Hotmail, Gmail and Yahoo made it easy to use even though the protocols and clients (e.g., SMTP, Eudora) were already in place. And maybe there is ways to experiment with funding initiatives, for instance MultiBit wallet will start to charge users 1000 satoshis (~$0.05) for every transaction. Perhaps this will become a modified SaaS model for open source software. Every time Bob uses software for X minutes Bob will pay Y cents to the developers. Pay as you go.

While volatility will likely be an issue with bitcoin in the future, new financial services and platforms are being developed by companies such as Bitfinex, CampBX, Coinfloor, Atlas ATS, Coinsetter, Vaurum, itBit, ICBIT and LedgerX which may eventually allow exposure to other financial instruments such as a hedging against these movements (note: not all of these are creating hedging products). And lastly, entertainment is easy to start with when the basic business model and infrastructure is still pending. Despite my criticism, there is precedence with grey market activities like gambling as a boot-strap app, that is also how Youku got popular. Instead, more patience could be required as commentators could be overestimating in the short run and underestimating in the long run.

There may also be potential for the underlying tool (the blockchain) to be used for NGOs, for administrations in developing countries and in dozens of other areas. The Startup Cities Institute has created Munibit for this specific purpose yet incentivizing boots on the ground, convincing armchair market experts on Reddit to get on an airplane and fly to where the underbanked live, is an uphill task, yet stranger things have happened (like Bitcoin getting this far).

Or maybe there is no "killer app" to be found; perhaps in retrospect it is the protocol itself which allows businesses to remove redundant administrative overhead or maybe it is just the rails that organizations end up gravitating towards (though Ripple and proof-of-stake are competitive options on this front as well). Similarly there may be benefits that the token provides as a store of value for high net worth individuals (HNWIs), institutions, enterprises and governments. Building a business around a product based on how the consumer *actually* behaves today versus how you *want* the consumer to behave will likely save a lot of headaches in the future. I think this is why BitPay may ultimately move towards API and tech solutions such as Copay and multisig (there are several new infrastructure plays including HelloBlock, Blockr, BlockCypher and Chain) and maybe why BitGo was recently able to attract a highly experienced product manager – enterprises and institutions may be interested in the store of value aspect and they have a lot more capital than sock puppets and gamblers.

If you are interested in creating a start-up in this space to on-ramp utility, innovation and ease-of-use to the network there are several incubators and accelerators to help out:

- Plug and Play Tech Center
- 500 Startups
- Boost VC
- CrossCoin Ventures
- Techstars
- YCombinator

- Seedcoin

Will you create Bitcoin’s hockey stick growth?