**Slicing data: what comprises blockchain transactions?**

By Tim Swanson

Published: January 22, 2015

Over the past month we have seen nominal transaction volume on the Bitcoin network reach several all-time highs. Enthusiasts on social media have proposed any number of theories including a rise in retail payments or commercial volume.

Yet upon further inspection, there does not appear to be a silver bullet answer.

We know, for example, that these transactions can originate or be comprised of faucet outputs, mining rewards, coin mixing, gambling, movement to 'change' addresses and simple wallet shuffling.[1]  So with this type of identification problem, how can analysts distinguish the signal from the noise?  Or as Peter Todd and others explained last month, for a few hundred dollars a day, it is possible to inflate the transaction volume by an entire order of magnitude.[2]

For instance, questions have arisen over a series of what some call "long chains."  Last month several commentators on a popular thread on *Hacker News* identified thousands of small transactions originating from a single source.[3]  The source was continually sending transactions and paid transaction fees for each of them.  The reason this struck many as odd as a rational actor would simply bundle the transactions together to save on transaction fees.

While there are likely different motivations for doing so, one reason for why this was occurring was that the originating source was attempting to delink or otherwise mix and tumble coins to make it difficult to "dox" or identify the originating source.  But it could also be a faucet and at one point even pools paid out miners using chained transactions, perhaps some still do.

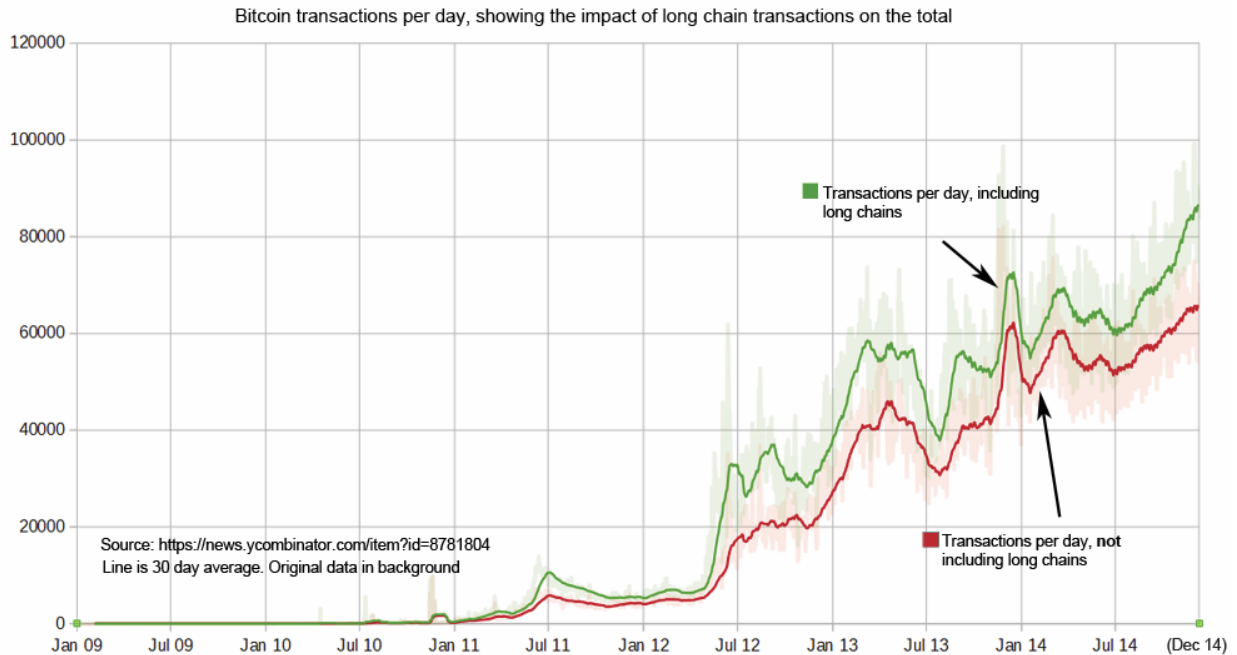What does this look like?  Below is a chart created by user "FatalLogic" in that thread:

Bitcoin transactions per day, showing the impact of long chain transactions on the total

*Image source: Hacker News*

The green line identifies the overall transaction volume on the Bitcoin blockchain, whereas the red line follows the rule, the heuristic that removes these "long chains."

Is there a definition of long chains?

Two weeks ago Blockchain.info published several similar charts excluding "Long Chains."

According to Jonathan Levin, formerly of Coinometrics:[4]

> Blockchain.info have implemented a heuristic to identify high velocity activity that is probably unrelated to real world commerce. Every day the internal counter resets and counts how many times transaction outputs were spent on the same day. So if a wallet paid someone 1 btc in one transaction output and they then transferred that to cold storage that would be a chain of two. However there are some chains where the chain of spent outputs of a given day exceeds 1000. Each day, on average, the sample size is 144 blocks.  Therefore, for chains of more than 144, the chain of transactions involve zero confirmation transactions (i.e., are not relying on the blockchain for their security). In other words, it is a measure of velocity.

> These long chains show that there are some parts of the economy that are flipping outputs almost 10 times a block with chains of over 1000 in a day. This may not relate to real world commerce or security processes, probably more likely to be gambling or mixing. In Satoshi Dice often the bettor just takes their winnings and gambles again with everything being done with 0 confirmations. Likewise with mixing there is little need to wait for confirmations and the priority is obscuring the origin of the transaction outputs. Finally this is unlikely to capture a lot of activity run by the centralised services since their objective is fee minimisation.

Furthermore, according to the description on Blockchain.info's site, "A chart showing the total number of bitcoin transactions per day excluding those part of long chain transaction chains. There are many legitimate reasons to create long transaction chains however they may also be caused by coin mixing or possible attempts to manipulate transaction volume."

The first chart below is the original *unmodified* chart of total transactions on the Bitcoin blockchain:[5]
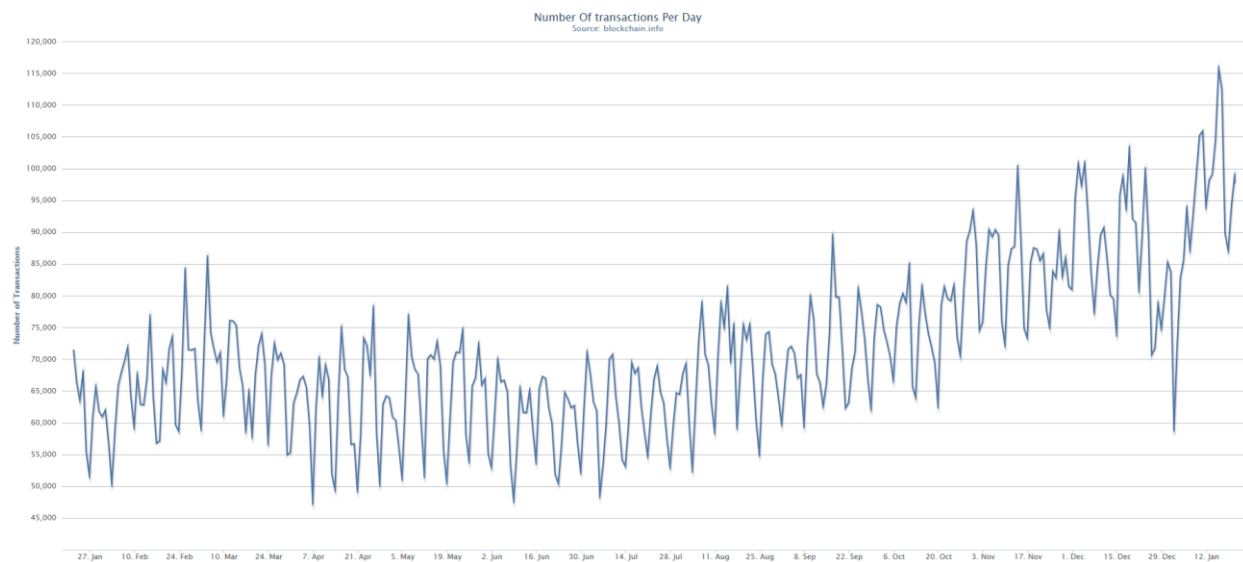


Using the same Y-o-Y time frame, below is the newly *modified* chart, using the Blockchain.info heuristic that removes these "chains" longer than 10:[6]
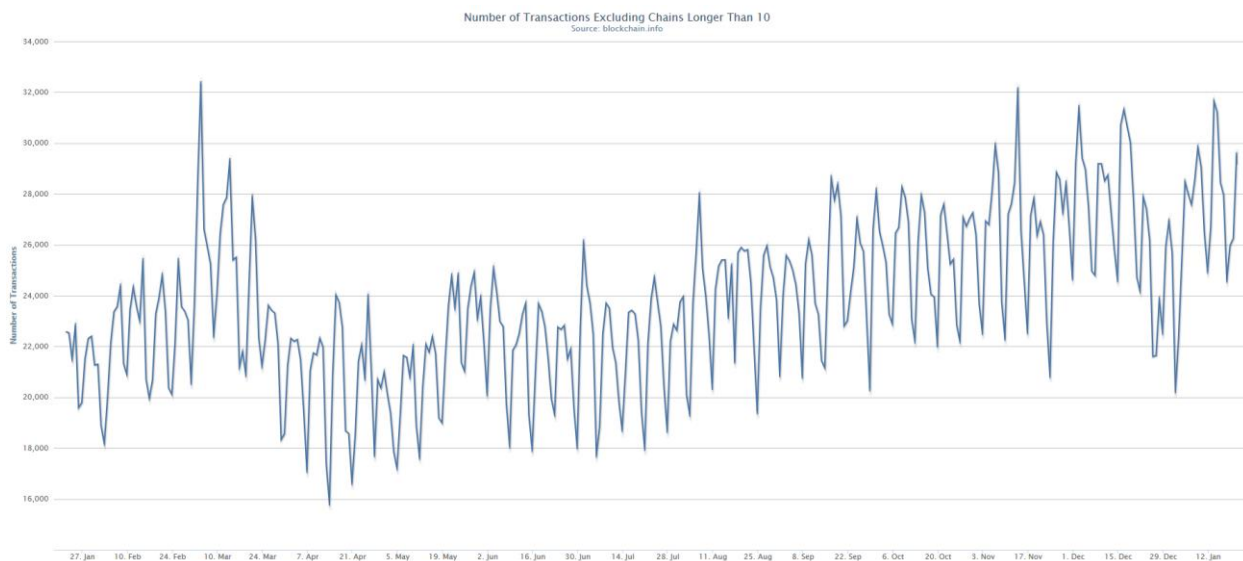


As we can tell above, by removing these "long chains" the volume decreases by 3x, yet there does appear to be an upward trend over the past several months.

I spoke with Atif Nazir, the CEO and co-founder of Block.io. In his view:[7]

> The term "longest chain" is vague – it would be misleading to say it is just coin mixing. The volume could be a series of transactions where the user cannot spend to the desired destinations in the same transaction. This could be a limitation of their wallet software's user interface, or the backend of the software itself.

> For instance, if a faucet is built on Block.io, the owner spends coins rapidly, sometimes breaking them into a couple transactions if they are efficient, and at other times into hundreds of transactions that spend unconfirmed change in rapid succession. We have seen chains of unconfirmed spends as long as 1,000 transactions, and they could be longer if blocks are not found.

> In general, achieving provable privacy through coin mixing and coin shuffling is hard as long as you stay on the same Blockchain. With the current methods, you can look at a destination address and say, with some certainty, "hey, this guy is the one who stole the Bitstamp coins."[8]

> In the absence of a definite, no-non-sense way to look at "long chains" of transactions, the safest assumption would be to consider them as unconfirmed chain spends, where the user wants to spend transactions very quickly deliberately or due to their software's limitation.

Another potential source is even smaller.

For instance, Sidney Zhang, co-founder of HelloBlock has noticed that:[9]

> Another interesting thing is people are sending dust transactions on the network as advertisements for high-yield investment program (HYIP).[10]

> This transaction, 92aa, is an example of an ad (and the message was removed by blockchain.info).[11]

> What they do is they will look for transactions happening on the blockchain, pick a collection of addresses and then send 1 satoshi to them and then they will attach a "public note" on blockchain.info. The message is normally like earn 7% per day at xyz.com. The public note in this case was removed, probably reported as spam

> The second, 1cca, is an example of a faucet. If you look at the tag "win free bitcoins every hour!" it is the address for freebitco.in.[12]

> It is unlikely the long chains come directly from consumers because consumers don't spend money rapidly.

> A more likely scenario is it is a 'shared' hot wallet operated by a service (e.g., Coinbase, Circle). A possible explanation then emerges - off-chain gambling sites such as Primedice / Moneypot / Betcoin casino and others operate hot wallets.

> In terms of scale, very small casinos may receive approximately 30+ deposits a day. A larger casino easily operate with 1000s of deposits a day and hundreds of withdrawals.

> One interesting behavior is that, bitcoin gamblers never keep funds in a casino. They tend to deposit, play and then immediately withdraw without leaving funds there

overnight. That could create a huge amount of activities from the same hot wallet. Thus creating a large chain.

Last year Ken Shirriff also pointed out a few of the notable pieces of "spam" that permanently reside on the blockchain including images.[13]

What does this look like altogether?

For additional analysis I reached out to Organ of Corti who plotted out these differences onto two different charts.[14]
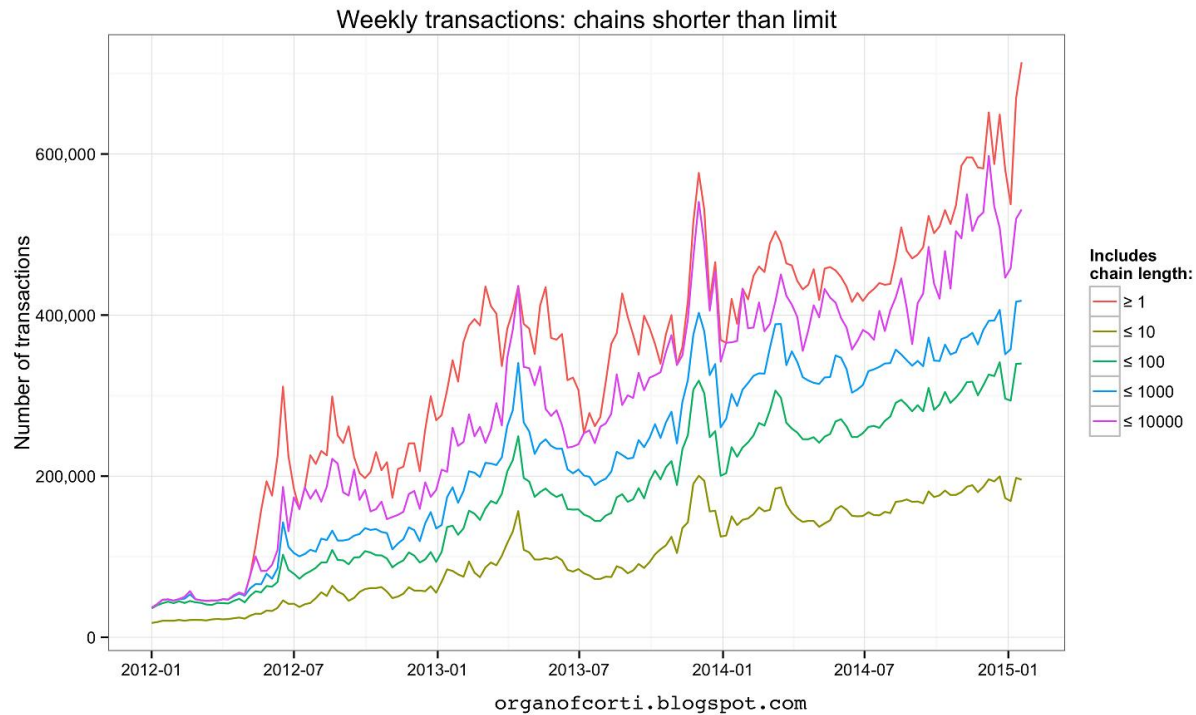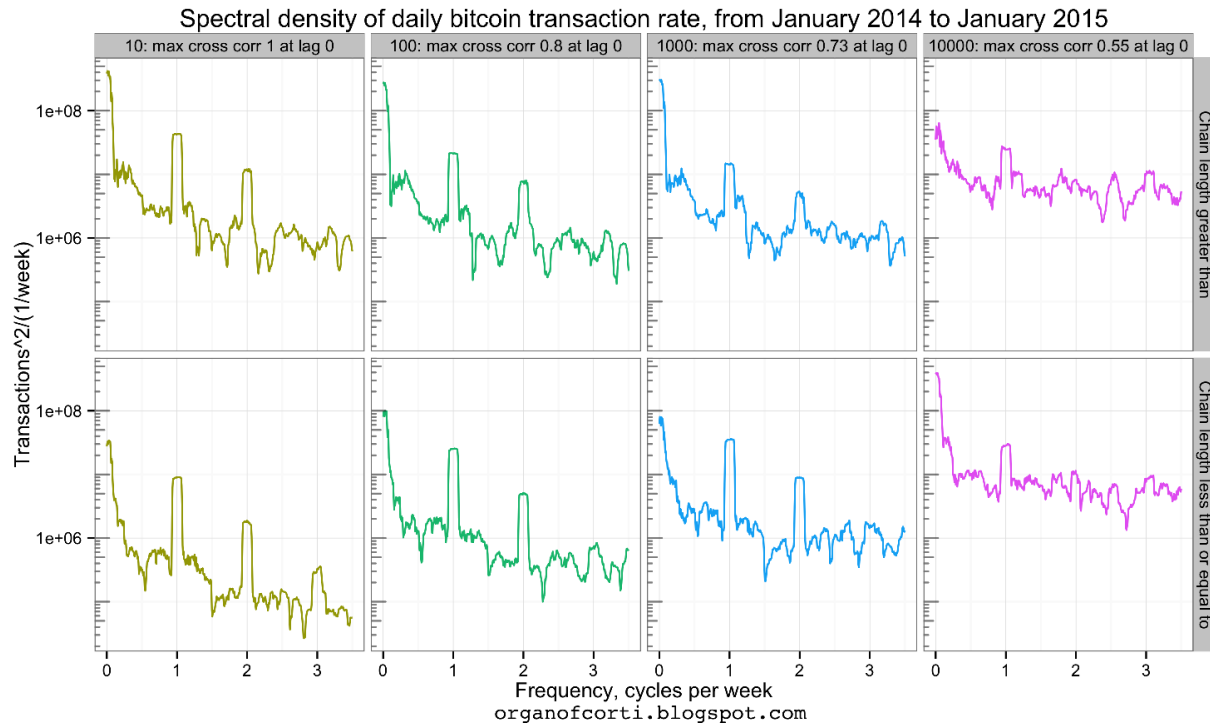


As shown above, these match up with the heuristic used by the original *Hacker News* post as well as that of Blockchain.info.  In Organ's view:

> If long chains of transactions are used by entities of a very different nature to single transactions or short chains of transactions, then we might expect to see differences in transaction rates and transaction rate cycles between the short and long chain groups.

> Starting with a visual comparison of the two groups, the most significant difference between the longer and shorter chain groups is variance. This is to be expected since one long chain of transactions increases transactions rates more than a single, unchained transaction.

Does the yellow line at the bottom represent the actual "real" volume?  Perhaps, but maybe not.

In addition, Organ put together a spectrogram to analyze this weekly cycle that is visually apparent in all the charts:

Spectral density of daily bitcoin transaction rate, from January 2014 to January 2015

organofcorti.blogspot.com

Another way to look at it is through a spectral density chart, according to him:

> Perhaps a more useful test is to check for periodicity in the data. We know from previous work that currently transactions show a daily and a weekly cycle. I'm using Blockchain.info's data which is daily, so a spectrogram will only reveal a weekly cycle.
>
> The last plot shows the spectrograms for chains longer and shorter than 10, 100, 1000, or 10000. These show a periodicity similar to that for all transactions of one cycle per week.
>
> We can also compare transaction of chains longer and shorter than 10, 100, 1000, or 10000 by calculating the cross correlation function. In each case the maximum correlation is at lag 0 and is much higher than the upper bound of the 99.9 confidence interval, so the periodicity of the transaction rates of each group (chains longer and shorter than 10, 100, 1000, or 10000) are similar to, also suggesting that time of use for shorter and longer chain transactions are similar.
>
> Further, time series decomposition showed the same starting and finishing days of each weekly cycle.
>
> I think that a working week cycle implies that the larger number uses of longer chain transactions are from businesses with a normal working week, and the correlation in the periodicity of the shorter and longer chains of transactions suggests the largest use of both longer and shorter chains of transactions are by entities with a work days and weekends.

Is there anything that explains the increase then?

6

**Other sources**

Earlier this month a new game called SaruTobi was approved for inclusion into the iOS store.[15] The game tips its users bitcoin on the blockchain (in contrast, ChangeTip does so off-chain). During its debut week, before running out of coins, according to its first public address, SaruTobi sent out more than 5,000 transactions most of which during an 11-hour time period.[16] Within its first two weeks it paid out roughly 6.4 bitcoins with more than 50,000 transactions.[17]

Another continual source of on-chain usage comes from Counterparty, a "2.0" platform that effectively sits on top of the Bitcoin blockchain and uses bitcoins for each counterparty transaction (e.g., it is an embedded consensus mechanism). Below is a visual of the daily transaction volume over the past year:[18]


Counterparty Transaction History
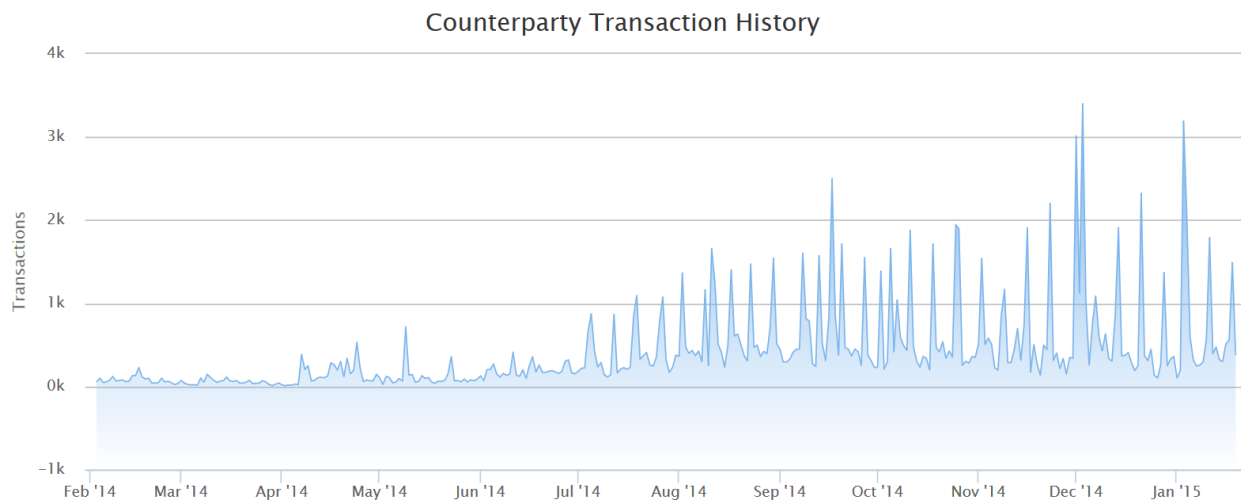
*Source: Blockscan.com*

The variation follows some of the daily (and weekend) patterns we have observed with Bitcoin in general (e.g., less activity on "Sundays") but at certain days and times there are peak usages of up to 3% of the Bitcoin network.[19] One explanation is that Counterparty is a popular platform for issuing tokens during crowdsales. For instance, the double peaks in December are most likely related to the Gems crowdsale, in which 2,633 BTC were exchanged for 38 million "GEMZ" (the native coin of the Gems system).[20]

As I briefly described last month, over the past year, a BitcoinTalk user, "dexX7" has been parsing other data, usually related to alt platforms such as Counterparty, Mastercoin, Colored coins and proof of existence.[21] Recall that these 'altcoins' are actually in practice, just watermarked bitcoin transactions. In order to use these platforms, a user has to interact with the Bitcoin network (e.g., they are embedded consensus mechanisms). Below is a chart he recently sent me that dissects this composed parts:[22]

Meta-transactions embedded in the Bitcoin blockchain

block height: 340.018
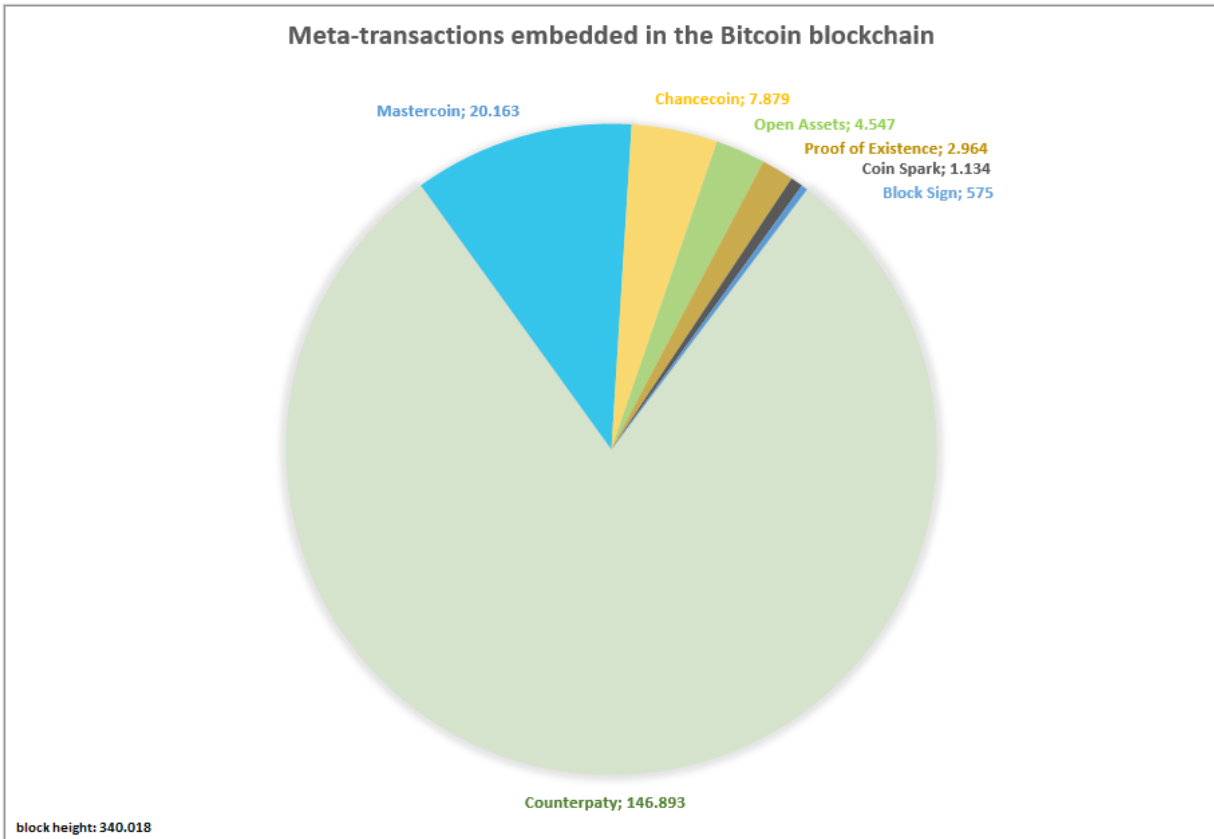
| | Transactions | Unspent outputs | Unspent multisig outputs | Spent multisig outputs | Multisig outputs |
|---|---|---|---|---|---|
| All | 57.489.982 | 16.511.696 | 217.416 | 31.820 | 249.236 |
| Counterpaty | 146.893 | | 181.624 | 13.868 | 195.492 |
| Mastercoin | 20.163 | | 12.989 | 8.280 | 21.269 |
| Chancecoin | 7.879 | | 5.043 | 8.073 | 13.116 |
| Open Assets | 4.547 | | 0 | 0 | 0 |
| Proof of Existence | 2.964 | | 0 | 0 | 0 |
| Coin Spark | 1.134 | | 0 | 0 | 0 |
| Block Sign | 575 | | 0 | 0 | 0 |

- Data captured at block height 340,018
- There were at least 184,155 identifiable meta-transactions
- There were 57,489,982 transactions in total
- There were 16,511,696 unspent outputs

This only includes the transactions dexX7 was able to identify. Counterparty, Mastercoin and Chancecoin use almost entirely "bare multisig" scripts as medium to embed and transport data. In contrast, Proof of Existence, Open Assets, Coinspark and Block Sign use OP_RETURN (note: there is still an active discussion between using 40 bytes and 80 bytes).[23] Open Assets and Coinspark are a type of colored coin implementation and both Proof of Existence and Block Sign are a type of notary service (previous charts are available in an album view).[24]

Some other analysis from dexX7:

Almost all Counterparty transactions carry data via bare multisig and there are about 5000 non-multisig Mastercoin transactions. There are furthermore 17620 unclassified, unspent multisig outputs and 6286 unclassified, spent multisig outputs.

Almost all of those unclassified multisig outputs were created by Wikileaks and actually carry some data too.[25]

Proof of Existence, Open Assets, Coin Spark and Block Sign account for 7363 OP_RETURN transactions. The total number of all OP_RETURN outputs, according to webbtc.com, is close to 11960, so more than 60 % can be mapped to those four.

Another slice of daily and weekly transactional volume comes from pay-to-script-hash, better known as P2SH.  This was originally BIP 16 proposed by Gavin Andresen and incorporated into the protocol in 2012 to "let a spender create a pubkey script containing a hash of a second script, the redeem script."[26]

This has replaced 'bare' multisig as a means for securing bitcoins.  While its use and adoption started off very slow, more than 6% of all bitcoins are now stored in this manner including Bitstamp via its recent integration with BitGo:[27]
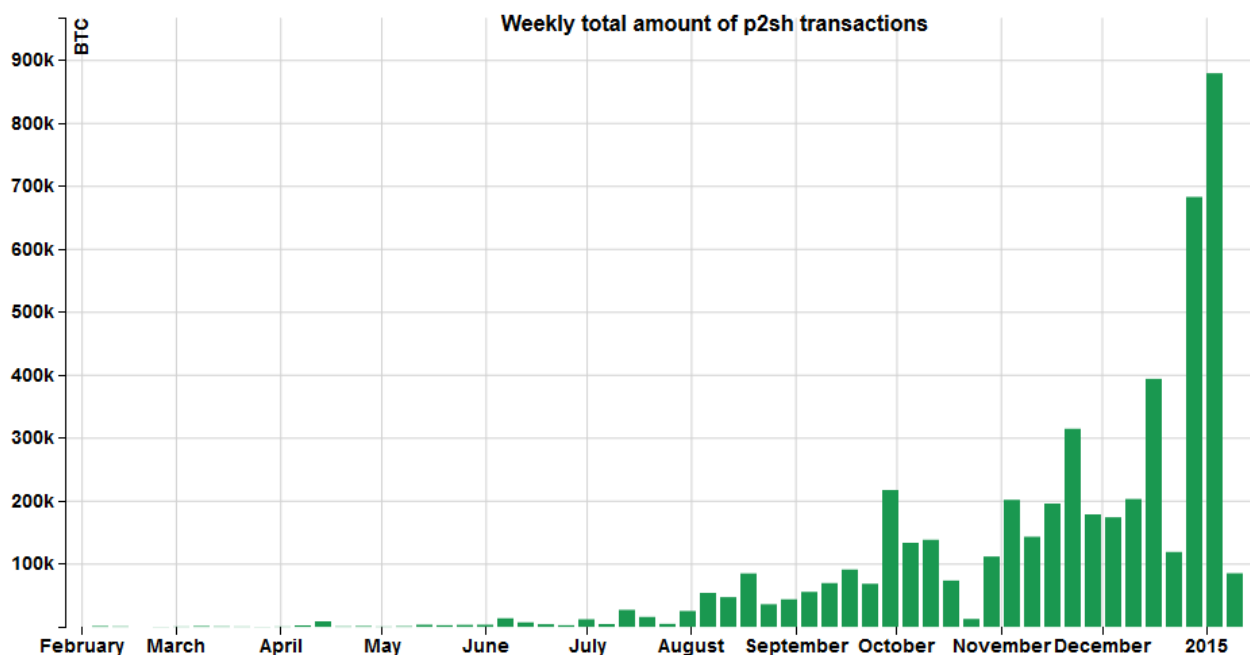


*Source: P2SH.info*

**What about retail volume?**

As has become apparent, it cannot be said that an increase in transaction volume is (probably) due to any one specific variable. Yet, according to a popular narrative, the quadrupling of acceptance by merchants this past year (from ~20,000 to 82,000), may have led to increased spending by consumers and therefore account for the increase.[28]

Last month, Jorge Stolfi a computer science professor in Brazil analyzed the BitPay addresses (BitPay reuses addresses) based on the Walletexplorer dataset.[29] Below is a visual of what BitPay has received over the past two years.
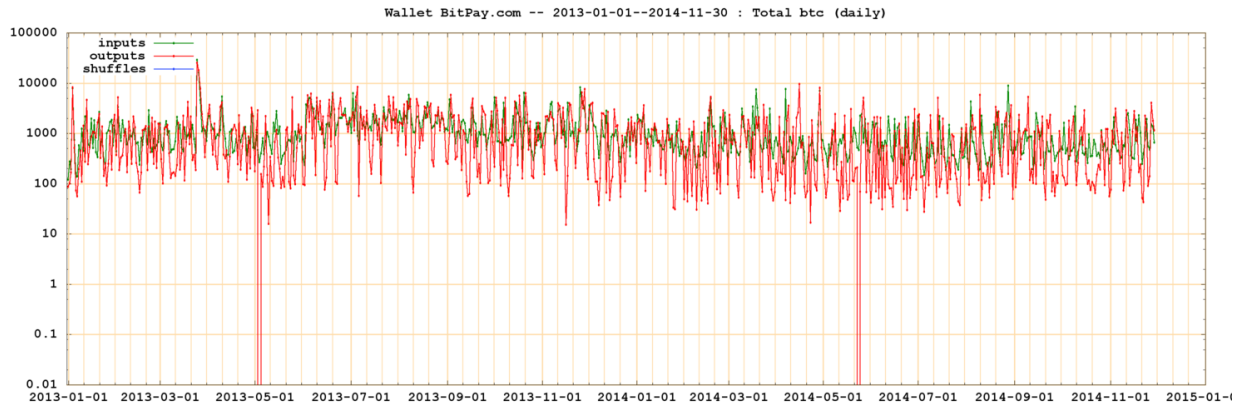


*Source: Jorge Stolfi and Walletexplorer.com*

According to Stolfi:

> The green line on this graph shows the number of BTC deposited each day into that wallet.[30] This graph is rather strange since the number is practically constant since January 2013, about 500–1000 BTC/day, and shows no weekly pattern. And no Black Friday spike either.

In his analysis Stolfi also noticed two different types of orders processed by BitPay, what he labels "wholesale" versus "retail." The "wholesale" coins are likely miners selling their block rewards in bulk whereas "retail" is consumer behavior (e.g., buying coffee, food, tickets).

Furthermore, if this wallet heuristic is valid, according to Stolfi:

- BitPay now processes about 1000-1500 "retail" payments per day, averaging less than 1 BTC each;
- The number of retail transactions processed by BitPay has grown 3x since mid-2013, and has been flat through most of 2014;
- The amount of BTC processed by BitPay (including "retail" and "wholesale" payments) has been quite constant since Jan/2013, about 500-1000 BTC/day
- In terms of dollar value, the amount processed by BitPay (including "retail" and "wholesale" payments) has increased a lot from 2013 to 2014, but has fallen 50% or more since February, as the BTC price fell.
- Black Friday had a modest effect (2x to 3x) on the number of "retail" payments, but had no effect on the total BTC/day (which is dominated by the "wholesale" payments).

And what about off-chain retail transactions?

Below is a public chart from Coinbase that visualizes the off-chain activity that takes place on Coinbase's platform.[31]
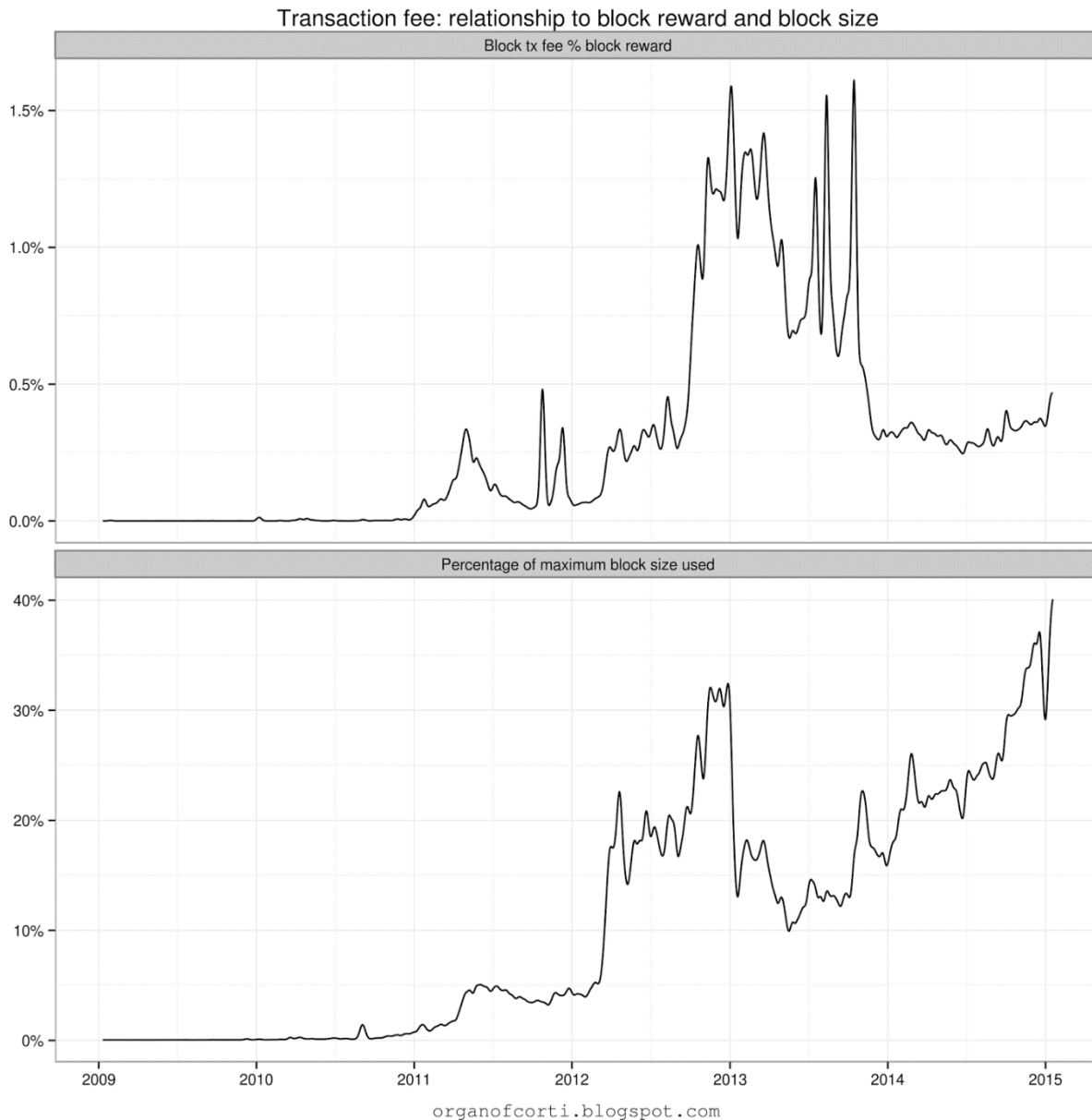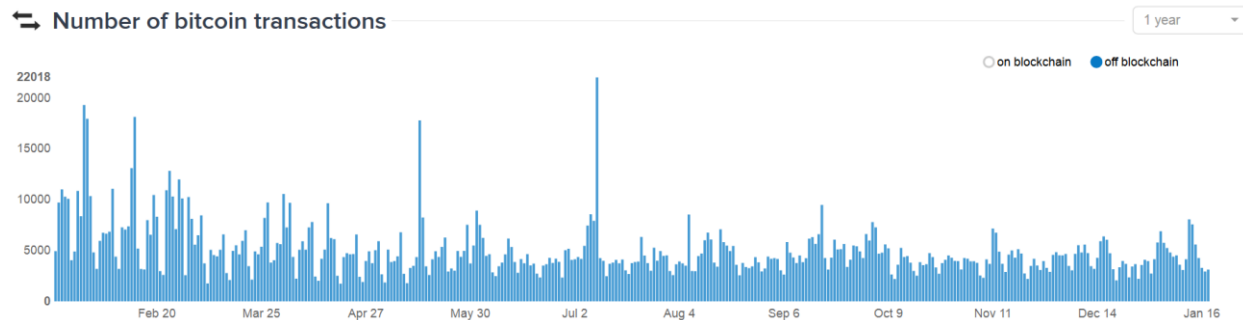


*Source: Coinbase.com*

The noticeable pattern of higher activity on weekdays versus the weekend is apparent irrespective of holidays.  Consequently, on most days these self-reported numbers comprise between 3-5% of the total transactions on the Bitcoin blockchain.  However, as Jonathan Levin, has pointed out, it is not clear from these numbers alone are or what they refer to: Coinbase user to user, user to merchant, and possible user wallet to user vault?

**Fees**

Another way of looking at whether or not transaction volume is increasing is through the "fees" to miner metric (recall that these are not real "fees" as they are not mandatory yet and may be more akin to "donations").[32]  Maybe transaction volume based on the methods above does not fully capture hypothesized growth.

Transaction fee: relationship to block reward and block size

Block tx fee % block reward



Percentage of maximum block size used



organofcorti.blogspot.com

Above is a new chart from Organ of Corti which visualizes the transaction fees included with each block over the past 6 years.[33]  If on-chain retail commerce was increasing, it would likely in turn be paid for via some fee mechanism yet this is not apparent.  This is not to say that utility has not increased for certain participants.  Volume as a whole has clearly increased as shown by the second image – yet these are users who likely opt to send a fee-less transaction to the mempool (these transactions typically take several hours or perhaps a day to be included within a block).

What is another explanation?

It does illustrate that the other narrative – that fees replacing block rewards – has not yet begun to occur.  Maybe it will not.

For instance, last year Robert Sams and Vitalik Buterin highlighted the economic costs that are being overlooked to maintain the infrastructure, that fees would unlikely be able to adequately compensate miners.[34] And Dave Hudson independently explored what has actually occurred in practice, providing visualizations of the empirical data that highlights and reinforces their marginalized viewpoint.[35]

To put it another way, if more users were actively using the blockchain to transmit value, then it would likely be apparent via an aggregate increase in fees.
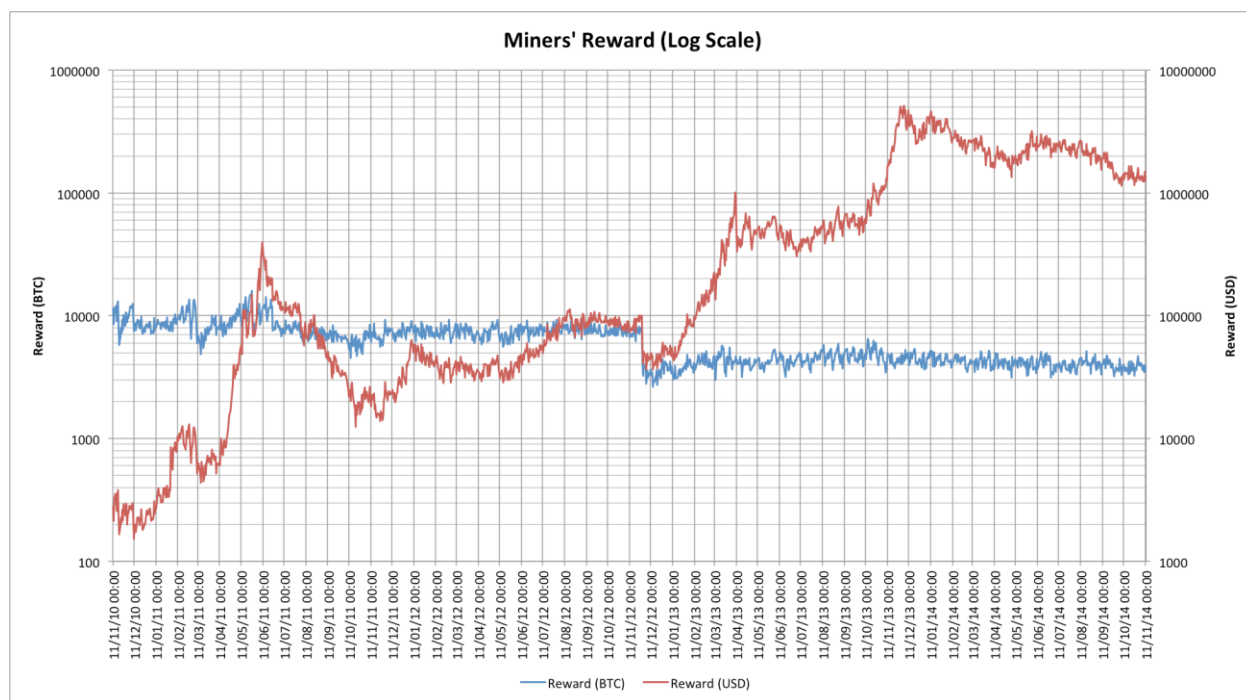


*Source: HashingIt.com*

As shown above during a four year time span, miners, the actual labor force of the network, are not seeing the narrative play out as it is supposed to (block reward plus fees to miner). Denominated in bitcoin (the blue line), miners have not seen the increase in fees or revenue that many of the same social media promoters claim will happen. Whether this changes is unknown.

Again, recall the current narrative that in the end, transaction fees will purportedly replace the block reward.[36] But the causality is the opposite direction than assumed by most: fees people are willing to pay determine the number of miners. Not the other way around. The takeaway is that simply put, fees may not rise to cover the current block reward amounts. It may be that the block reward falls and miners just drop out and net transaction fees never increase reducing the security of the network but this is a topic for another article.

**What does this all mean?**

For perspective I spoke with Ernie Teo, a research fellow at the Sim Kee Boon Institute for Financial Economics (which hosted a cryptocurrency conference in November).[37] According to his team:

We observe similar trends to what has been mentioned in your article. We see a large increase in the one satoshi (or less) addresses over time. This could also be due to the long chain "spammer" you have described above. A few more things we can note from our upcoming analysis on the distribution of bitcoins over time:

- 50 coin addresses, these are the only addresses in the very beginning due there being only miners on the network. However we see that this does not fluctuate a lot overtime and it indicates that most miners tend to cash out once they mined.
- Large increase in number of addresses with less than 1 bitcoin. This indicates more "retail" type buyers.
- Not much change or fluctuations to the large addresses.

I think it is probably true that not a very large proportion of the transactions are retail transactions. In the long run, it doesn't help the network. We can only wait for the next big innovative app that can boost retail-type usage.

How else can this be visualized?

John Ratcliff recently published several new charts describing "the State of the Blockchain Address(es)" in which he delves into token movements and in particular "zombie" addresses (addresses that have not been active in 3 or more years).[38] They are illuminating and we both disagree on conclusions that can be drawn from them.

For instance, he updated one chart that I previously described as showing more than 70% of coins have not moved in more than 6 months:[39]
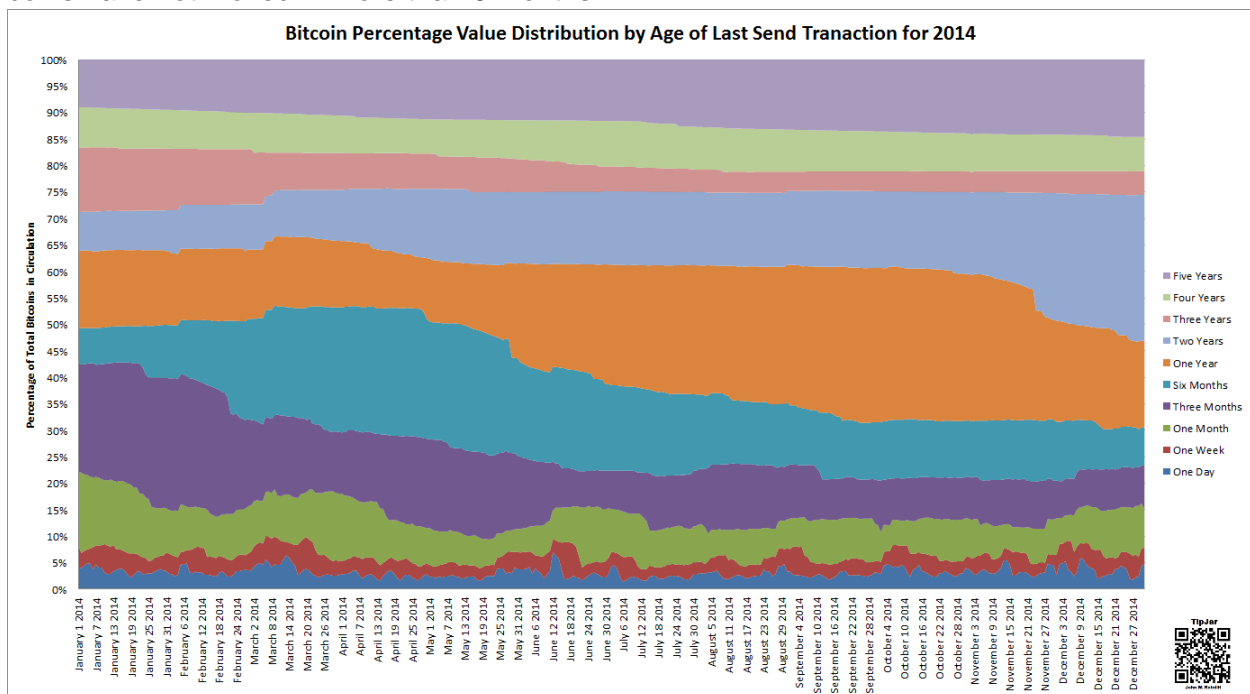


*Source: John Ratcliff*

What does the chart above illustrate?  If it is velocity then what the color bands reinforce my explanation from two months ago: that the majority of coin holders that were purchased in the November / December 2013 bubble are now underwater.[40]  We see the transition over the year, in which these coin holders, rather than spending and realizing a loss, hold on to them throughout the months.  Hence, why we likely see another uptick to an "older" band starting in mid-November 2014 – the anniversary of the beginning of the most recent bubble.

This explanation is further reinforced by the demographics of bitcoin holders: mostly middle to upper-middle class residents of developed countries – most of whom have "low time preference" (e.g., speculators) and therefore do not need or want to spend bitcoins immediately because they have other means of payment (e.g., credit cards) and can therefore hold onto their coins longer than someone with "higher time preference" (e.g., less affluent individuals living paycheck to paycheck who in theory would have to continually, immediately spend bitcoins). Another potential explanation is the disposition effect, but this is also a topic for a different article.[41]
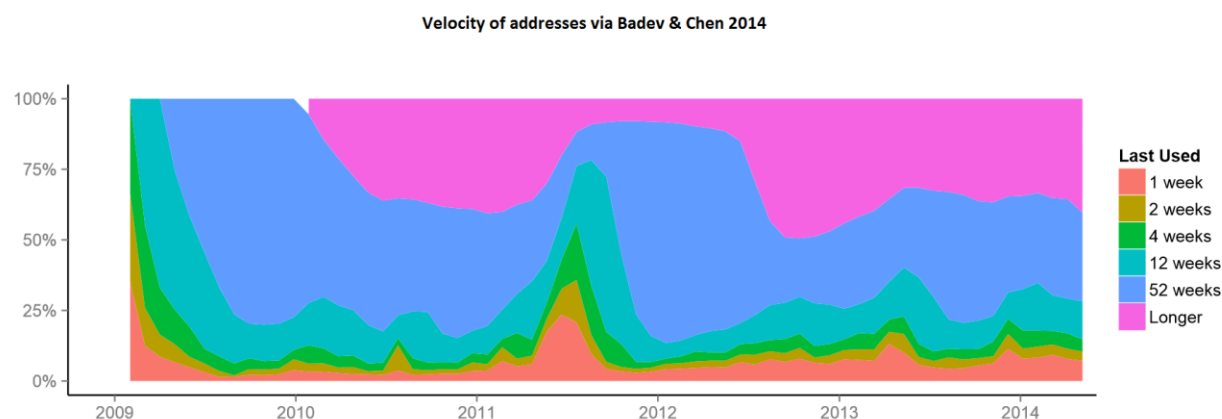


Source: Badev and Chen

The chart above (originally Figure 15) was published this past month by two researchers at the Federal Reserve.[42]  They independently used a similar methodology that Ratcliff has undertaken.  In their view:

> Figure 15 examines the degree of activity for the addresses in the network. For each date we partition the volume of addresses with positive balances according to their last activity. For example, the addresses that have transacted in the last week are likely to be frequently used (shown with the strip in the bottom). On the other hand, some of the addresses have not been active in the past 52 weeks. Those are likely to serve saving or investment purposes and much less so for transacting. From Figure 15 we can see that the volume of "investment" addresses (not used in the last year) has been steadily decreasing. Still, however, around 75 percent of the addresses in operation with positive balances have not been used in a transaction in the last four months.

While the rest of their report is illuminating, in their concluding remarks, they also do not see retail transactions as comprising more than a marginal amount of volume:

Broadly speaking, our empirical exercise documents general patterns of Bitcoin usage, and examines the use of Bitcoin for investment and payment purposes. We find that while the number of daily users may have doubled every eight months, the transaction volume is negligible compared to the domestic volume of U.S. payment systems. Our analysis of data from the Bitcoin system further suggests that Bitcoin is still barely used for payments for goods and services. In addition, the patterns of circulations of bitcoins and the dynamics of the bitcoin exchange rate are consistent with low usage of Bitcoin for retail payment transactions. Finally, we provide evidence that the exchange rates between bitcoin and other currencies are not well aligned, which we interpret as a lack of depth of the exchange markets and as costly exchange rather than unexploited arbitrage opportunities.

Perhaps these trends will change. Maybe, as some claim, retail volume will increase. But as shown above and through Total Output Volume we know what the maximum "purchasing power volume" of transactions is, this has not been a mystery.[43]

While merchant adoption continues to increase, consumer adoption for retail purchases appears to be flat (as shown by both BitPay and Coinbase numbers). Future analysis may need to look at correlating these trends for brick and mortar merchants. Without regular use at the register and point-of-sale, there are a number of anecdotal stories of retraining and fumbling that will go on with floor employees with respect to accepting bitcoin.[44]

Perhaps again, this will change in the future (e.g. Impulse, v.zero),[45] but going forward a full traffic analysis such as the type created by Sarah Meiklejohn *et al.* two years ago would help the industry as a whole determine what consumer behavior looks like with greater accuracy.[46] And this is important for a project whose white paper promotes itself as a payment network for online commerce (see section 1).

So what conclusions can be drawn from this?

As noted at the beginning, there does not appear to be one specific variable that explains the recent increases over the past several months. For example, most tipping from services like Bitui in China and ChangeTip internationally, is already done off-chain (e.g., the independent site 'ChangeTip stats' describes activity on the company database).[47] SaruTobi is too new to account for all but the last few weeks of growth and DarkWallet activity will likely be "long chain" related. Perhaps offline P2P transactions from OpenBazaar should be identified, aggregated and brought into future analysis.[48]

Future analysis should also look to factor in or filter out activity related to "change" addresses. For instance, the short-term 'velocity' seen in the daily and weekly bands of Ratcliff and Badev & Chen's charts could be overstated due to coins which do not actually swap hands with new individuals but are rather "spent" to themselves due to how "change" is handled by the protocol. Furthermore, as has been described in Dave Hudson's modeling of block sizes, it cannot be said that an increase in on-chain volume is axiomatically "good."[49]

All we can say for now is that there is an increase in usage from multiple sources, but not likely from on-chain retail commerce which has remained flat for about a year.

This is still a dynamic space and perhaps it may be months or even years before we will be able to fully identify all the major contributors to volume changes.

## Acknowledgements

Special thanks to dexX7, Raffael Danielli, Michael Dann, Dave Hudson, David Lancashire, TM Lee, Jonathan Levin, Atif Nazir, Organ of Corti, Jorge Stolfi, Ernie Teo and Sidney Zhang for their constructive feedback and time.

## End notes

[1] At its peak in the first quarter of 2013, Satoshi Dice (a gambling service) represented roughly 48% of all transactions on the Bitcoin network.  This is visualized by dexX7.

[2] See Peter Todd's tweet and Questions Linger as Daily Bitcoin Transactions Pass 100,000 Milestone from *CoinDesk*

[3] See the original comment from 'sanswork' in thread covering "Bitcoin adoption in 2015" from *Hacker News*

[4] Personal correspondence, January 19, 2015

[5] Number of transactions per day from Blockchain.info

[6] Number of transactions excluding chains longer than 10 from Blockchain.info

[7] Personal correspondence, January 18, 2015.  See Block.io

[8] Analysis: Bitstamp Hacker Almost Stole Additional $1.75 Million from *CoinDesk*

[9] Personal correspondence, January 18, 2015.  See HelloBlock.

[10] For a brief overview see High-yield investment program

[11] The relevant "ad" address can be viewed at
https://blockchain.info/tx/92aa4e600f15d8e5353b180010a270d4f173a7226cc6dd3f40bd5a7bd20e0082

[12] The faucet address is located at:
https://blockchain.info/tx/1cca64709d2b1679a1a64253afe01f41e2b684ef7d9cbce67fedb764c5bc78c6 and its 'parent' is the following address: https://blockchain.info/address/175o52E64wHQumzfLFnKrPaukJsvo9pgMb

[13] Hidden surprises in the Bitcoin blockchain and how they are stored: Nelson Mandela, Wikileaks, photos, and Python software by Ken Shirriff

[14] Personal correspondence, January 20, 2015.  See Organ of Corti.

[15] Apple Approves iOS Game That Tips Players in Bitcoin from *CoinDesk*

[16] SaruTobi's first address conducted 5,255 transactions:
https://blockchain.info/address/17ZgzoQUAiCrCgSieYfGhAvToW9kn6uaLt

[17] SaruTobi's second address conducted 6,676 transactions:
https://blockchain.info/address/1GumHq1f5XVnxBjnz78uRgJad2nyE5TgjS and then its third and as of this writing, most current address, has done 41,677 transactions:
https://blockchain.info/address/3MXxfNZoifLYdS8wJTpvfeDNPt9ZWuMAaN

[18] See Blockscan Counterparty Transaction History

[19] See Counterparty CEO tweet and The Composition of Metacoins on the Bitcoin Network by Tim Swanson

[20] GetGems Token Sale Wrap Up - Thanks x38,135,367! by Tom Kysar

[21] The Composition of Metacoins on the Bitcoin Network by Tim Swanson

[22] Personal correspondence, January 21, 2015

[23] See the conversation Change the default maximum OP_RETURN size to 80 bytes #5286 at github

[24] An album overview of select metacoins by dexX7

[25]  See Hidden surprises in the Bitcoin blockchain and how they are stored: Nelson Mandela, Wikileaks, photos, and Python software by Ken Shirriff and this address containing embedded data:
https://blockchain.info/tx/6c53cd987119ef797d5adccd76241247988a0a5ef783572a9972e7371c5fb0cc

[26] For a brief overview see Pay to script hash and developer guide to Transactions

[27] The Bitstamp and BitGo Partnership Is a Watershed Moment for Bitcoin from BitGo

[28] State of Bitcoin 2015: Ecosystem Grows Despite Price Decline from *CoinDesk*

[29] See Are there changes in the volume of retail transactions through Bitpay this past year? by Tim Swanson and WalletExplorer.com

[30] A permanent copy of the image is located on Jorge Stolfi's site.

[31] Coinbase charts

[32] The Collective Action Problem of Mining Fees by Tim Swanson

[33] January 18th 2015 Block Maker Statistics by Organ of Corti

[34] See The Marginal Cost of Cryptocurrency and Some Crypto Quibbles with Threadneedle Street by Robert Sams; Vitalik Buterin has discussed this several times on the official Ethereum blog.  In addition, I discussed this at length in Chapter 3 in *The Anatomy of a Money-like Informational Commodity*.

[35] The Future Of Bitcoin Transaction Fees? by Dave Hudson

[36] The Collective Action Problem of Mining Fees by Tim Swanson

[37] Singapore Event Puts Bitcoin on Mainstream Finance Agenda from *CoinDesk*

[38] The State of the Blockchain Address(es) by John Ratcliff

[39] Analysis: Around 70% of Bitcoins Unspent for Six Months or More from *CoinDesk*

[40] Approximately 70% of all bitcoins have not moved in 6 or more months by Tim Swanson

[41] For a brief overview see Disposition Effect

[42] Bitcoin: Technical Background and Data Analysis by Anton Badev and Matthew Chen

[43] Total Output Volume from Blockchain.info

[44] My Amsterdam Letdown and Why Bitcoin's Real Value May Lie Beyond the First World from *CoinTelegraph*

[45] BitPay recently announced its whitepaper on "Inter-Channel Payments" also called "Impulse."  See also the v.zero project from Braintree, Braintree Activates Bitcoin Payments for US Merchants from *CoinDesk*

[46] A Fistful of Bitcoins by Meiklejohn *et. al.*

[47] See Changetip real-time usage stats

[48] A few statistics are available at BazaarBay

[49] See 7 Transactions Per Second? Really? and The Myth Of The Megabyte Bitcoin Block by Dave Hudson