Learning from Bitcoin's past to improve its future

Tim Swanson[1]

Revised: April 27, 2014

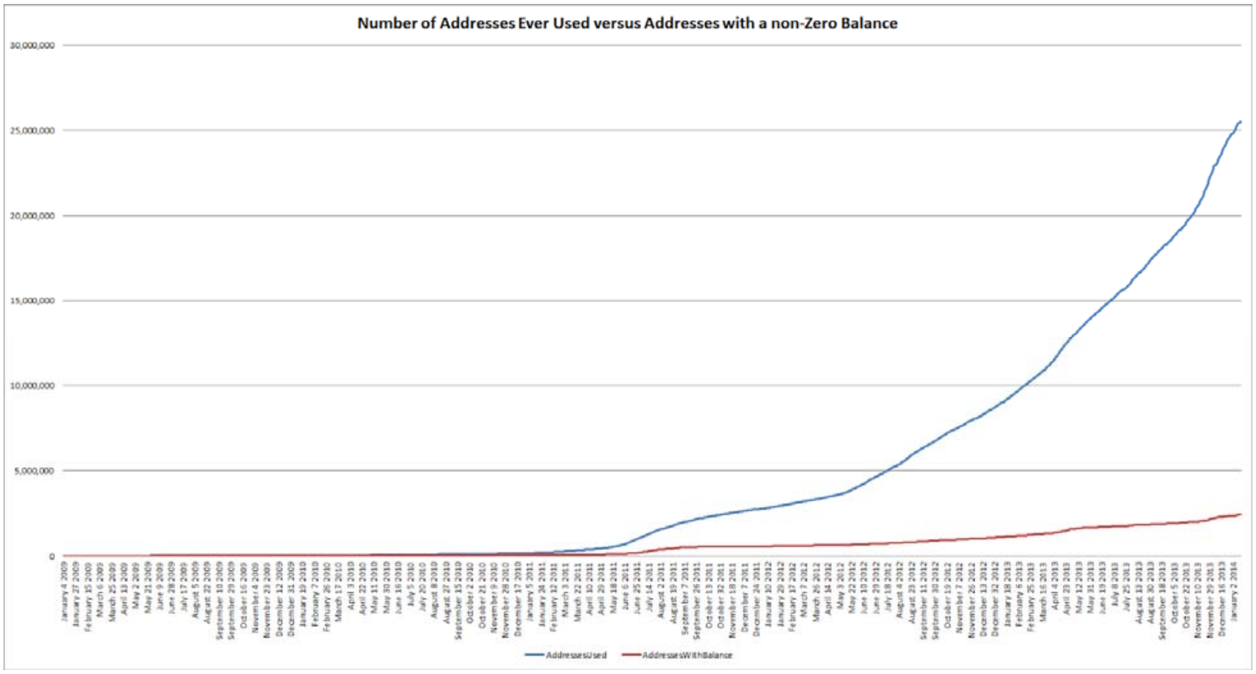
Abstract: Estimating the success of any technology platform necessarily requires understanding the quality and amount of marketshare – or in the case of new technologies, the size and activity of user base such a platform may have. It is presently unclear how many active users of the Bitcoin network and complementary services, rather than total number of users who have ever interacted with the platform. Studies estimating the conversion rate to this new platform based on currently available metrics are publicly unavailable or simply do not exist: network data furthermore points to relatively low flat adoption rates. Early participation on the Bitcoin network in the form of "mining," initially involved little more than a common laptop; yet scaling techniques have disincentivized most individuals participating in this manner due to high costs associated with establishing economically viable mining operations and rapidly diminishing returns arising from a rapidly rising global hashrate. Finding plausible reasons for low-usage rates among ordinary consumers including a dearth of available productive "apps" and the cost of securing information, are discussed as possible impediments to wider adoption. The creation of additional incentives are discussed for providing on-ramping solutions onto the platform.

Background

While the Bitcoin community is a very vocal, energetic group, despite immense global media coverage and $1-2 billion spent on funding infrastructure and services, it is arguable that its conversation rate (CVR) – a ratio of the number of users of Bitcoin per dollar invested or per minute of media attention – is still relatively small.[2] Part of it is a user-design (UX) and on-ramping (education) adjustments, some of which will likely be ironed out as the space matures, yet there are other factors at play.

Admittedly measuring the impact of media appearances for any platform is historically difficult: both John Wanamaker and William Lever, pioneers of modern advertising purportedly stated a century ago that "half the money I spend on advertising is wasted; the trouble is I don't know which half."[3] Tracking which demographic segments are exposed to and adopting crypotcurrencies will likely become an increasingly germane research topic in the coming years especially for start-ups looking to build beyond niches.[4]

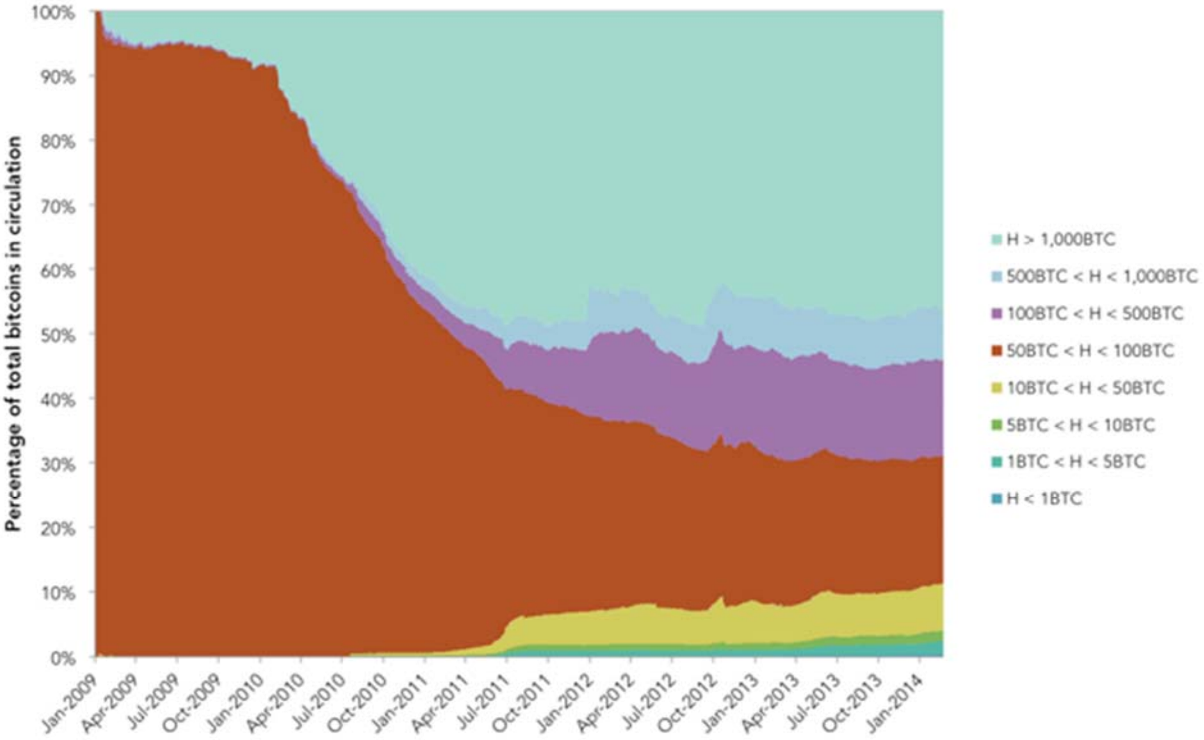
For instance, instead of asking how big the Bitcoin user base is, a more accurate question is, how small?



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 "throw-away" addresses – addresses used as intermediate steps (i.e., using a new address per transaction, or to identify amounts received from particular payers).[56] The red line illustrates addresses with bitcoins: 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).[7] 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.

While there are over 1 million wallets on Coinbase and likely as many on other hosted wallet services; these however, are centralized off-chain solutions.[8] Still, these edge services provide a valuable service (e.g., microtransactions, near-instant trades) that apparently market participants are willing to use relative to on-chain solutions as shown by the fact that Coinbase opened 1 million wallets in roughly 14 months, a rate roughly on par with another, Blockchain.info (which claims to be "on-chain") which did it in 17 months.[910] The utility and ease of use offered by reputable off-chain providers may constitute one large component for the rise in bitcoin usage and therefore increase the quantity of market demand.



The chart above, compiled by Jonathan Levin illustrates the consolidation of bitcoins over time. In his words:[11]

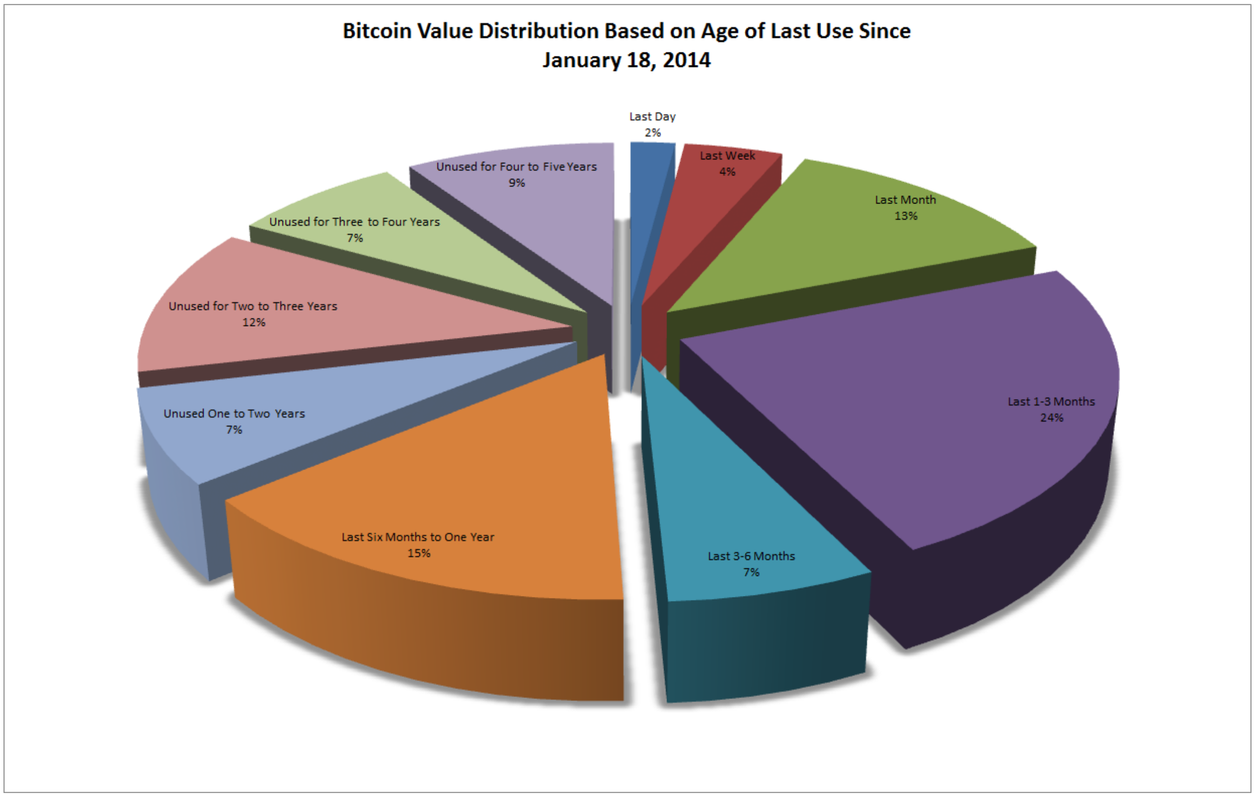
> Post 2012, the amount of coins held in addresses containing between 50 to 100 BTC are above my expectation and raises the possibility that a large number of these coins are lost. This conjecture is backed up by Bitcoin days destroyed evidence. There remain approximately 4 million coins that have never been spent, many of which are probably contained in the red section.

This finding correlates with mining estimates from ‘rutkdn’ who analyzed the blockchain and found that 1,919,950 bitcoins are stagnant on 38,399 addresses mined between 2009-2010.[12] Based on research from Sergio Lerner, roughly half of these are speculated to belong to Satoshi Nakamoto, the creator of Bitcoin, and the other half belong to miners who over the years: [13]

- Hard drive broke and was returned-to-manufacture but forgot to backup wallet
- Mined as a hobby on old equipment, hard drive now long forgotten and/or reformatted
- Sent dozens even hundreds of bitcoins to test it out with other hobbyists, then deleting them because they were “worthless” at the time

Altogether this represents 15.29% of all mined bitcoins as of April 14, 2014.

This is further visualized in another chart from John Ratcliff (below) which illustrates that more than half of all bitcoins mined have not been moved in over 6 months and 28% of the total have not been active in more than two years:[14][15]



Bitcoin Value Distribution Based on Age of Last Use Since January 18, 2014

All in all, what this means is that there is likely an upper bound of no more than 10 million people who have ever handled a digital key controlling bitcoin, and the actual figure is likely significantly less. In any given day there are between 60,000 – 70,000 on-chain transactions. According to the Bitcoin Rich List as of block 295,000, approximately 99.08% of all addresses contain less than 1 bitcoin.[16][17] Thus, despite the growth in hosted wallets, actual active bitcoin users – those who currently have more than 1 bitcoin and have sent a fraction of a bitcoin to another address in the past 6 months – may be as low as 500,000 individuals.

While an imperfect facsimile, Square, CloudFlare, Stripe and MakerBot each were founded in 2009 or 2010 yet their uptake and adoption relative to the amount of direct media attention and ecosystem investment, is significantly higher.[18] Similarly, M-PESA, a mobile payments systems which launched in 2007, currently carriers transactions worth 43% of Kenya's annual GDP and is used by tens of millions (67%) of adult residents daily.[19][20] Although the decentralized character of Bitcoin means that these corporate analogies are imperfect, there may be tangential explanations.

What are some reasons that led to this consolidation instead of dispersal? Based upon the chart provided by Levin, beginning in 2010 Bitcoin market participants increasingly liquidated their holdings to certain addresses, most likely hosted wallets and exchanges. Reflecting on historical events in Bitcoin there may be potential reasons for dips and consolidation of substantial bitcoin balances:

- February 6, 2010, Bitcoin Market opens becoming the first exchange which coincides with the beginning of consolidation
- July 18, 2010, Mt. Gox opens, ultimately reaching 80% of exchange marketshare at its peak two years later[21]

- July 18, 2010, the first GPU hash farm (run by ArtForz called the "AntFarm") finds its first block and later purportedly reaches 25% of network hashrate at its peak for several months[22]
- December 16, 2010, the first mining pool, Slush's pool finds its first block and reportedly reaches 10,000 Mhash/s the following month (~8% of global hashrate) by January 8, 2011
- July 2011 – December 2013, the ZeroAccess botnet spreads to between 1 – 2.2 million systems. During one phase reported in September 2012, the botnets theoretical collective hashing power reached 2,480 GHash/s generating up to 1,022 bitcoins per day (~14% of global hashrate)[23]
- January 30, 2013, Jeff Garzik received the first ASIC manufactured by Avalon which performed at 68,252.65 Mhash/s (earning up to 11 bitcoins per day)[24][25]
    - Note: for comparison a quadcore desktop CPU from Intel reaches approximately 10-11 MHash/s

Increased hashing asymmetries, have substantially raised the barriers to profitably enter this segment leading to potential centralization concerns.[26] Initially mining was a common gateway into the cryptocurrency economy.[27] While increases in upfront capital costs do not completely explain the relatively low adoption rate, it does explain some of the centralization seen in token distribution as visualized by address analytics.

Bitcoin: a peer-to-peer heat engine

While there will be volumes more written on the econometrics of Bitcoin's underlying incentive mechanisms, Danny Bradburry has done some important research on an issue that no one could have foreseen in 2007 – 2008, the years in which Satoshi Nakamoto, ostensibly designed the system: what are the actual energy and infrastructure costs for seingiorage?[28]

Ignoring for the moment the colorful anecdotes in Bradbury's research, we now know that there is a near-precise model that describes the cost of running and maintaining the network. The way the cost estimate is determined is through how Bitcoin acts as a decentralized waste heat creator that activates and deactivates heat generation based on market participation and pricing signals. What do the randomizations necessary for cryptography and the waste heat produced by computing devices have in common? One word: "exergy," a term of art describing the maximum useful work possible during a process that brings a system into equilibrium with a heat reservoir. Exergy is always destroyed in the seigniorage hashing process - for example - if a token's value increases to $1,000, this means that at most $1,000 worth of waste heat will be generated in its creation. This is largely in the form of actual electricity to heat conversion, but also throughout the ASIC manufacturing and logistical supply chain as well as new market participants coming online seeking rents arising from their production of this ledger unit.

Where that same token is valued by the market at $500, that means that *ceteris paribus*, it collectively costs the network $500 to operate per token generated (+/- several percent). This then means if the price were to go up to $1,000 again for an entire year, approximately $1.3 billion worth of operating costs (e.g., infrastructure capital expenditures) will subsequently be spent to "extract" tokens and process transactions at this higher price. This is known in advanced due to the monetary base expansion built into the code; this year the money supply on the Bitcoin network will expand by approximately 1,312,500 bitcoins or 11.1% of the total bitcoins ever created (i.e., scheduled inflation). As the market value of these tokens fluctuates, miners (seigniorage crafters) will turn off, on, dispose of or acquire machines depending on whether it is profitable to do so.

What this means is that if a bitcoin reaches $10,000 in value, then at least $13 billion worth of capital expenditure will be invested in extracting it.[29] Scaled up to $100,000 and the infrastructure costs alone would cost more than the entire market capitalization of several global payment processors (e.g., MasterCards current marketcap is $125.4 billion and spent $299 million on capital expenditures in 2009), yet likely without providing any immediate benefits to customers or merchants.[30][31] This is debatable and discussion over which, including proposals from core developers such as Peter Todd and Adam Back, will continue to be researched and published in the coming months.[32] While there are plans in the works to modify the Bitcoin core code to address these issues, as the code sits today, the provision of additional hashpower will not result in faster confirmation times or greater transactional capacity. Furthermore, at this scale centralization will likely become crystalized because miners incapable of breaking even at $100,000 a token will be purged from the marketplace. The only miners capable of participating at this level will likely be professionally run datacenters with peering agreements and increasingly capital intensive economies of scale.[33][34] At a stable $1 million a token, mining facilities would need to efficiently utilize and dissipate $150 million of exergy per hour limiting their geographic locations to a global handful capable of powering the internal infrastructure (e.g., next to multiple power plants dedicated solely to it).[35] This will change again in two years due to block reward halving but is used for illustrative purposes. In other words, non-marginal mining operations will and have become fully professionalized IT teams (CEX.io, Cloudhashing) that model their budget from earnings projections and an estimated revenue stream from seigniorage. Price volatility may cannibalize their accounting profit and ultimately can purge them as well (as described below).

Another related issue to this is the equivocation of hashrate with security; this is arguably a *non sequitur*. Hashrate is an arbitrary metric that fails to fully qualify the security of the network or the quality of network performance either of which is dependent on a number of other factors including the wide distribution of the blockchain.[36] To equate hashrate to security is akin to Soviet-era planners boasting about the amount of tonnage each car at a state factory produced to demonstrate these automobiles' performance. Though a mass-produced Yugo or Lada from the Eastern bloc might indeed move via a combustion engine, a more accurate gauge and metric of performance would be an F1 auto that is a unique product which is amenable to ongoing maintenance and upgrades. Since Bitcoin is supposedly a real-time gross settlement (RTGS) platform, a more accurate comparison would be with Visa, which processes on average 3000 times as many transactions each second than Bitcoin does currently.[37] Yet, as we shall see below, funds invested in the Bitcoin network are not being utilized to actually enhance its performance or its security.

Robert Sams has written about this recently noting that:[38]

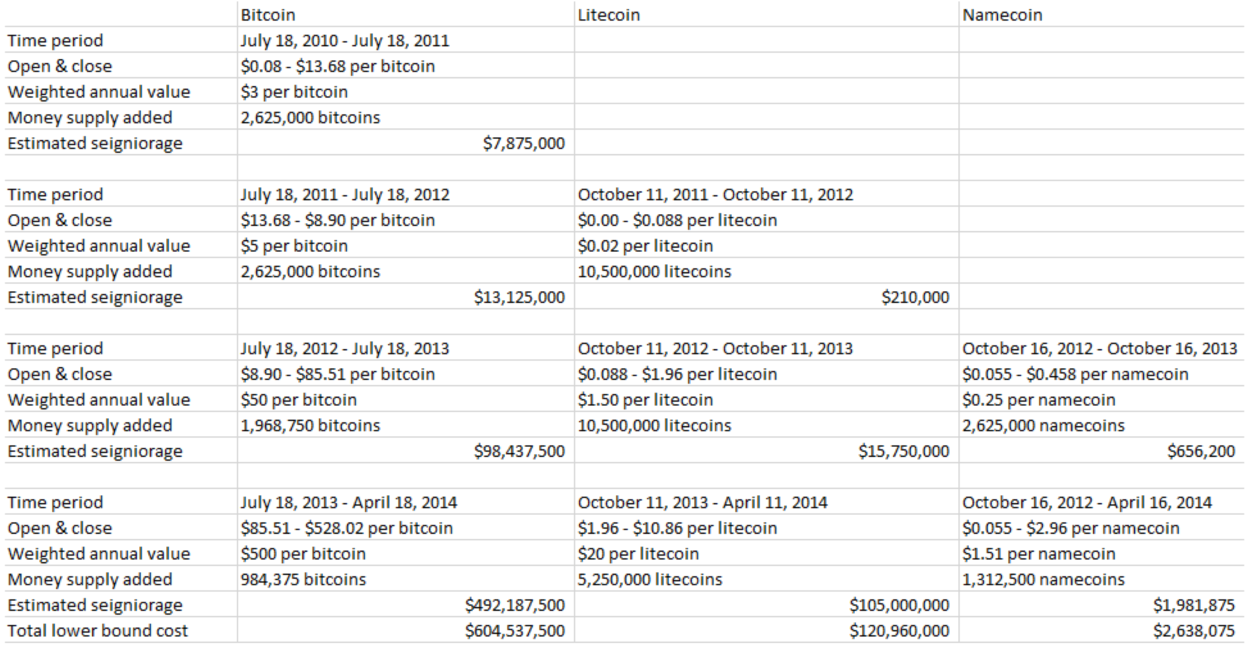
> Hash rate says nothing about security, it's the amount spent on hashing that matters. If there were a way of requiring miners to hash using an abacus, hash rate would be tiny but network just as secure if same amount of capital was spent employing dextrous human calculators.
>
> Efficiency of converting a scarce resource into hashes has no social benefits here. (Except that it correlates with tx verification, where efficiency is beneficial).
>
> You ultimately have two problems to solve: what tx fee maximises fee revenue for miners? Second, is that maximum sufficient to cover the required hashing costs for minimum security?

Because of how they are interconnected: additional hashrate may provide utility for transactions. However after 51% of the hashrate it is exergic deadweight relative to security.[39] Thus there are likely other more accurate metrics for measuring and qualifying the security of the network.

Estimated costs of building the infrastructure

Since the genesis block it has generally been accepted that there has been between $200 million and $1 billion worth of hardware sales related to building the current Bitcoin network. The lower limit is an estimate from Gil Luria at Wedbush Securities, yet the higher limit, as shown below, is the more accurate number.[40] In fact, the costs are perhaps even higher once botnet externalities are factored in.[41]

Figure 1: Lowerbound seigniorage estimate



	Bitcoin	Litecoin	Namecoin
Time period	July 18, 2010 - July 18, 2011		
Open & close	$0.08 - $13.68 per bitcoin		
Weighted annual value	$3 per bitcoin		
Money supply added	2,625,000 bitcoins		
Estimated seigniorage	$7,875,000		
Time period	July 18, 2011 - July 18, 2012	October 11, 2011 - October 11, 2012	
Open & close	$13.68 - $8.90 per bitcoin	$0.00 - $0.088 per litecoin	
Weighted annual value	$5 per bitcoin	$0.02 per litecoin	
Money supply added	2,625,000 bitcoins	10,500,000 litecoins	
Estimated seigniorage	$13,125,000	$210,000	
Time period	July 18, 2012 - July 18, 2013	October 11, 2012 - October 11, 2013	October 16, 2012 - October 16, 2013
Open & close	$8.90 - $85.51 per bitcoin	$0.088 - $1.96 per litecoin	$0.055 - $0.458 per namecoin
Weighted annual value	$50 per bitcoin	$1.50 per litecoin	$0.25 per namecoin
Money supply added	1,968,750 bitcoins	10,500,000 litecoins	2,625,000 namecoins
Estimated seigniorage	$98,437,500	$15,750,000	$656,200
Time period	July 18, 2013 - April 18, 2014	October 11, 2013 - April 11, 2014	October 16, 2012 - April 16, 2014
Open & close	$85.51 - $528.02 per bitcoin	$1.96 - $10.86 per litecoin	$0.055 - $2.96 per namecoin
Weighted annual value	$500 per bitcoin	$20 per litecoin	$1.51 per namecoin
Money supply added	984,375 bitcoins	5,250,000 litecoins	1,312,500 namecoins
Estimated seigniorage	$492,187,500	$105,000,000	$1,981,875
Total lower bound cost	$604,537,500	$120,960,000	$2,638,075

As noted in *Bitcoin Hurdles*, there is no such thing as “free” in bitcoin transactions.[42] Someone pays both in terms of inflation and in transaction costs: roughly every 10 minutes the money supply increases, diluting the shares of every holder, yet incentivizing users to process transactions. The two are fully integrated and Figure 1 (above) provides a lower bound estimate of this relationship.[43] The total lower bound cost is an approximation of the aggregate weighted annual value. Thus, all things being equal, $604,537,500 is the lower bound cost to extract and maintain the Bitcoin network since July 2011. Similarly, approximately $120,960,000 was spent on infrastructure for Litecoin seigniorage over the past 30 months and $2,638,075 for Namecoin seigniorage for the past 18 months.

This intersects with a common refrain in Bitcoin public forums during 2014, “$600 million has been irreversibly spent securing the Bitcoin network.”[44] This does not seem like a particularly positive data point to focus on as virtually all other industries that utilize capital machinery also undergo some form of irreversible capital depreciation. If this was a positive attribute, marketers at automobile companies would likely be using it in television advertisement, “nearly $1 billion has been irreversibly spent building an engine for the new Lexus ES350.” The quantity of the funds involved does not necessarily reflect the performance of the engine or the vehicle. Alternative consensus mechanisms such as proof-of-stake or the Ripple protocol purportedly provide roughly the same level of security and trustlessness yet at a fraction of the capital requirements.[45]

In an open market, prices serve as signals to market participants to either enter or exit a market. In the case of Bitcoin, the value of the token provides one quantitative signal to miners to either continue hashing or to stop. While there are exceptions to the rational economic actor (*homo economicus*) when it costs more to hash than miners receive, miners will each have to decide whether to continue or not. Because it is a competitive marketplace and because each mining operation has different economies of scale, marginal players may be purged from the seigniorage market due to their inability to compete when token valuations are lower than the amortization rate of their depreciating capital goods.[46]

There are at least three exceptions to this rule however:

- hobbyists and researchers
- wishful-thinkers
- botnet operators

Hobbyists and researchers have and will likely continue to operate at loses for a variety of motivations including to understand how all the interactions within the system are taking place.

Well-wishers include, notably an Austrian family that *Bloomberg* recently interviewed. Even though the family owned a power plant and also received subsidies from the government, because of the volatility in token prices which have dropped more than a half since their peak in late November, their mining pool was still operating at a net loss. One of the sons in the family acknowledged these market challenges, concluding that "[i]f you're mining at this stage, you're not doing it to make dollars, you're doing it because you believe it will go up."[47] In other words, they were hedging their losses in their income statement with future residuals from potential price appreciation.

Yet it would likely be cheaper for this family to simply shut the pool and the power plant off and simply purchase tokens instead, stepping aside as other mining pools with larger operating margins would continue seigniorage. This modeling limitation is typically measured via a discount function, which attempts to quantify the expectations and low time preferences of miners. For instance, even if Bob's operating costs were higher than the block rewards, he might mine today with the expectation that the price increases. As noted above, some miners do not necessarily want or need to sell today, Bob could store 50% of the bitcoin and effectively buys future network security on that price expectation creating temporary additional hashrate overhang.[48]

Botnets are the third and perhaps hardest to qualify or quantify due to their opaque nature yet fine-tuned *modus operandi*. In a sense, botnets are the most rational economic actors because they seek, at the expense of the machine owners, to achieve one sole purpose, mining tokens at the absolute minimum of cost to the beneficiary of these activities. And because both their electricity and capital costs are "free" (appropriated from their legitimate owners), they can and still do scale tens of thousands of highly inefficient hashing systems (desktop and laptop computers) to squeeze out *utils* for their operators and in this case, nonces for bitcoin.

Yet, as noted by James Wyke in SophosLabs research, there are unseen damages that botnets cause. In addition to destroying the lifetime cycles of the computers (wearing down the CPU, GPU, hard drive and memory) botnets also consumes bandwidth which, while marginal among a handful of computers, is very large when scaled to 100,000 or more. It also, in the words of Wyke's, "deprives hard-working legitimate Bitcoin miners from generating those coins and therefore receiving payment."[49] Furthermore, there is the cost of electricity which someone must pay for, and the increases in difficulty rating which requires "legitimate" miners to increase their investment in hardware in order to obtain the same return. That is to say, these botnets are artificially inflating the difficulty rating which in turn pushes out marginal, legitimate miners. Until these botnets are removed, they are effectively rent-seeking off the entire ecosystem and distorting the difficulty rating.

Yet even with the advent of ASICs, this is not an easy problem to solve. In November 2013, E-Sports Entertainment was fined $1 million USD after an investigation uncovered that an employee had inserted rogue code into an anti-cheating software program used by gamers in CounterStrike competitions.[50] The code would activate the GPUs at night, turning the host machines into a GPU farm that during its short duration, mined a total of 30 bitcoins. Again, while ASICs largely remove this ability for botnets to exist and compete with anything lower than a few million infected systems, the flip side is that massive centralization has taken place within the Bitcoin mining ecosystem, creating potential social engineering vulnerabilities.

While the ZeroAccess botnet mentioned above was declared defeated in mid-December 2013, Symantec published an estimate in October 2013 on these externalities of running the ZeroAccess botnet.[51] Based on 1.9 million infected machines, they projected it generated $2,165 per day mining bitcoins while using 3,458 MWh/day of energy (one infected computer consumes 1.82 kWh per day). For perspective, this is enough energy to power 111,000 homes each day.[52] This externality has not been factored into the seigniorage chart above. And it was not the only botnet as others such as Trojan.badminer and Ulfasoft from the TDSS rootkit could be used to generate tens of thousands of dollars each month in ill-gotten gains, which was not accounted for in Figure 1.[53] All told, according to research published by Huang *et. al.,* as of August 2013 they had identified more than 2,000 executables that connect to mining pools to mine bitcoins; 74% of which connected to public pools, the remainder connecting to private (dark) mining pools.[54] This same research found that another large botnet, DLoad.asia had amassed more than 100,000 computer drones between 2011 through 2012 and received at least 10,000 bitcoins during that time frame. Although ASICs have largely made even large botnets uncompetitive, malware operators still continue to use them, sometimes targeting altcoins with lower difficulty thresholds.[55][56]

As time goes on, other exploits will likely arise, including using power plant subsidies in China - now the location of several mining pools that not only have access to subsidized electricity but do not have to worry about many environmental externalities.[57]

While there are likely a variety of market distortions in part due to arbitraged electricity prices, botnets and a variety of uncertainty in legal frameworks, even relatively large capitalized companies in this mining space inadequately hedge risk. In November 2013, Alydian filed for Chapter 11 protection in bankruptcy court.[58] It was an ASIC-based hosted mining company ("outsourced mining"), one of the first in which customers simply buy shares of hashrate and the maintenance and management of the equipment occurred on site at Alydian's facility.[59] During the subsequent hearing, it was report that rapid increases in the global hashrate for Bitcoin in November 2011 resulted in the company's investment in mining hardware – planned in the summer of 2013 – not being sufficient to generate income in after a sharp increase in the network's hashing power in November later that year.

As a consequence, one of the considerations outlined above, the true costs of operating the network are almost certainly higher than the lowerbound estimate due to botnets which essentially steal and externalize resources costs, well-wishers who continue despite financial incentives to liquidate and hobbyists who may have ideological inclinations and see their mining as "donation" and "charity" to the community.[60]

Initial "killer apps"

Initially announced on April 24, 2012, by the summer of 2012, fully half of the transactions on the Bitcoin network were being used to transmit bets through a start-up on-chain gambling company called Satoshi Dice.[61] According to one statistical analysis, from between its April announcement through August 28, 2013, Satoshi Dice-related transactions accounted for 52.3% of all bitcoin transactions.[62] During this same time frame, transactions for Silk Road – an anonymous online marketplace which sold wares including narcotics and other banned substances exclusively with bitcoins – were estimated to make up 5-10% of the transaction volume of the Bitcoin network.[63] Between February 6, 2011 and July 23, 2013 approximately 1,229,465 transactions were completed on Silk Road which generated gross sales estimated at 9,519,664 bitcoins.[64] It is important to note that this is not to say every bitcoin mined was used on Silk Road, it is likely that coins spent were re-spent in Silk Road several times, generating an aggregate volume equal to this figure. Silk Road has since been closed and the alleged founder arrested by the FBI; Satoshi Dice has since been superseded by other off-chain competitors.[6566]

One of the reasons for relatively low user adoption for Bitcoin could be that despite the enormous amounts of publicity, most people do not gamble or use illicit drugs. Or in other words, if these are the "killer apps," why would those who do not gamble want to use this new network?

If the goal of cryptoprotocols is to provide frictionless mechanisms to foster real economic growth, then creating applications that provide genuine increases in productivity (total-factor productivity or TFP) to everyone including end-users that replace existing infrastructure in fully legal transactions, is likely an area for profitable business development (e.g., if gambling actually created real growth, then Las Vegas and Macau would replace New York City and Shanghai as economic centers for growth).[67] For comparison, the United States casino industry generates roughly $125 billion in revenue a year (or roughly 1% of GDP), yet most people do not gamble in part to the 'math-tax.'[68] Similarly, if the advertised apps for the Bitcoin network are online casinos, the potential user base will likely be limited to the same percentages of those who have been or currently participate in this segment of the entertainment industry.

Information security is hard

In legal terms, bitcoins are most closely related to possessory property, such as personal chattels or bearer instruments: to "own" a ledger balance is to possess knowledge of the corresponding private key. While the network itself is cryptographically secure, the edges of the network are still vulnerable to many of the same exploits that centralized financial institutions have been hedging against for decades. One question that Bitcoin adopters therefore frequently ask is: what are the edge-case statistics for losing possession to this key?

Tabulating publicly reported bitcoins that were lost, stolen, seized, scammed and accidentally destroyed between August 9, 2010 and November 28, 2013 comes to approximately 803,285 bitcoins.[69] A large bulk of this (171,955 bitcoins) comes from funds seized by the FBI from Silk Road in October 2013.

Between the end of November 2013 through March 2014, more than 150,000 bitcoins are known to have been stolen, destroyed, scammed, lost and "burned" bringing the total publicly known amount to 966,531 bitcoins that are no longer with their "legitimate" or "rightful" bearer.[70][71] Legitimate meaning, in this context, the person whom the law of a particular jurisdiction would be most likely to recognize as their legal owner, and from whom these bitcoins would be capable of being "stolen" in such a way that criminal sanctions would arise in relation to the theft.

Yet from the networks point of view, it does not matter what is stolen.[72] There is no protocol distinction between ownership and possession. Stealing is a legal term – not a physical phenomenon – thus the point over whether it is rightfully transferred or not is the subject for legal scholars to debate. The bitcoins still exist. However, legitimate bearer issues are important in so much as they create uncertainty about the safety of attaching assets to the blockchain.

Furthermore, it should be noted that the concern here is not that bitcoins have necessarily been lost, since from a technical standpoint that does not make much of a difference. The concern is the uncertainty. The concern is that the market does not know what happened to or will happen to those stagnant tokens. If the market knew, for a fact, that all of Satoshi Nakamoto's bitcoins or Mt. Gox's bitcoins were gone and lost forever, the market could incorporate that knowledge into how it values the economic basis for the remaining bitcoins.[73] But as of this writing, this is uncertain. Further research should be done to reorganize lost coins into a group that increases uncertainty and a group that decreases uncertainty. It should also be noted that it is difficult to distinguish between bitcoins which may have also been stolen from thieves by still other thieves during this tabulation.

Other considerations while real, may not have yet been aggregated or publicly disclosed:

- Coins stolen from mining pools (operator scalping/skimming)
- Unclaimed or unused promotions and dust tips on reddit and Twitter
- Coins stolen from insecure brainwallets (such as Naval Ravikant's "Hello World")[74]
- Dust on mining pools, exchanges and wallets
- Intentional spam for taint analysis (1Sochi and 1Enjoy in mid-February 2014)
- Money or undisclosed bitcoins stolen off numerous exchanges in which only fiat value is disclosed (e.g. GBL platform, on which $4.1 million in user money was stolen in November 2013)[75]
- Ransomeware copycats (CryptoLocker 2.0, CryptoDefense)[76]
- Accidental destruction arising from transfer to "temporary addresses" (i.e., many exchanges will issue new deposit addresses for each user, but by sending tokens to an identical address even minutes later could result in permanent purgatory or coin 'destruction.' All addresses are meant

to be single-use however due to "user confusion" some users repeat spending to single addresses)

- Marginal cases of mining and forgetting keys or throwing away a laptop (e.g., Stefan Thomas, James Howell).[77] Hal Finney remembered to back-up, others have not.[78]
- Jaded spouses[79]
- OTC and "hidden" order book[80]

Pre-eminent among these unknown numbers is Mt. Gox, an exchange that filed for bankruptcy on February 28, 2014. In its initial filings it noted customers may have lost 750,000 bitcoins and Mt. Gox itself lost another 100,000 bitcoins.[81] Subsequently on March 20, 2014, Mt. Gox announced that it had found 200,000 bitcoins in a wallet the company no longer used.[82] While it is still unclear what happened, many commentators have likened its operation to a stealth fractional reserve bank, which lent funds they did not have, effectively trading while insolvent without disclosing this fact to any party involved.

By 2013, it was a generally accepted that approximately 1 million bitcoins had been lost, stolen, seized, scammed or destroyed in some manner. Therefore, to answer the question of what the edge-case statistics are for the aggregate of private key loss, tabulations provided by these empirical example validate the notion that at least 1 million bitcoins were no longer with the property owner in some fashion. Adding Mt. Gox to this amount brings the figure to approximately 1,650,000 bitcoins which represents 13.7% of all mined bitcoins. Thus if all Mt. Gox coins are recovered, then the lower bound is 10%, if less are recovered then closer to 15% altogether.

Including the 15.29% of mining rewards which are stagnant or lost forever and the 0.86% of near-dust that resides on over 32 million addresses and most may never be used, at least 30% of all mined bitcoins are either lost, stolen, seized, destroyed, scammed, "dust" or forgotten.

While the non-collection of mining rewards will likely fall to zero as the industry consolidates and professionalizes, there are still on-going cases of fraud and abuse on exchanges. During the month of March 2014, CoinEx, an exchange got hacked; in this case the customers were refunded. Also in March, another exchange Coinmarket.io, stopped processing withdrawals but continued accepting deposits leading to accusations that it was stealing customer funds.[83] The following month, Cryptorush.io had internal mismanagement issues which culminated in a purported "hack" leading to a suspension of trading on and withdrawals from thee exchange.[84] . And on April 2, 2014, Danny Brewster the CEO of Neo & Bee, a Cyprus-based exchange allegedly absconded with up to several thousand bitcoins in investor funds.[85] One study published in 2013 found that from 2010-2013, 18 out of 40 Bitcoin exchanges closed, often wiping customer balances with them. And revisiting the list of exchanges used in the study would include 5-6 more exchanges that have since closed.

Thus despite a maturing industry, there are still a number of vulnerabilities, some of which can be mitigated and removed by the following methods:

- Trezor, a hardware wallet that must be activated (similar to an RSA token or Google authenticator)
- Proof-of-reserves, such as that offered by Bitfoo[86]

- Insurance from a wallet and vault provider, Xapo[87]
- Hierarchical Deterministic Multi-signature (HDM) and oracle-based wallets such as Cryptocorp[88]
- "On-chain wallet" from Blockchain.info[89]
- Armory, an advanced desktop-based wallet[90]
- Paper wallets[91]
- Multisignature wallets[92]

Looking forward: expanded functionality brings extended risks

There are benefits and drawbacks to each of these; over time mitigating edge-case vulnerabilities will still potentially be an issue. For instance, when smart contract platforms arise the stakes may potentially be higher still.

For example, Alice goes to bed. During the night, Bob from Hack Island, breaks into her laptop and email account, stealing her digital keys that control her bitcoins and most importantly the smart contract "deed" to her home. During the night, this contract is sold and resold a dozen times on a decentralized exchange. Alice wakes up, unable to open her home because the door is synched via wifi to a cryptoledger. What does she do? Today she would go to the police or public court, explain that even though there is a perfectly unabused contract, signed in a cryptographic manner, the property has been robbed and the contract should be ignored. As a consequence a new lock and title are issued and installed and a new digital "deed" is created.

What if the new owner of Alice's home is a non-governmental organization (NGO) or a non-profit organization? What if several days, weeks or months pass before the original, the owner realizes the deed or title to their boat or summer home has been resold and sold again and last owner is an orphanage or church? Preston Byrne, a cryptocurrency lawyer and securities lawyer in London, thinks that on account of problems such as these, the most likely future is hybridized - where decentralized computing would be paired with centralized key issuance and user registries. He adds: "it is entirely plausible to say that many of Bitcoin's descendants could be less free and more centralised than the Bitcoin of today, perhaps even state-run."[93]

Competition does not disappear in an open market

One of the memes propagating on Twitter, reddit and Bitcoin Talk is the coming death of alts or alternative coins. It has been historically true that more than half of all proof-of-work-based alts never live past their second "halvingday" – and the new "Blockchain 2.0" solution seems to provide technical incentives for why alt designers may be interested in working within one existing system instead of building entirely new protocols which compete with Bitcoin directly.[94]

However, there are at least two economic reasons for why making and deploying alts will continue into the foreseeable future:

1) Scarce labor. The pool of engineers capable of building a blockchain is small but growing. If you have the ability to do so, then it also stands to reason that you would like to be compensated for the work you provide. Until the recent announcement of Austin Hill's "Blockchain 2.0" company, despite the several dozen contributors to the main bitcoind repository over the past five years, there were only four people directly funded to provide new code. What this means is that because there is no financial incentive to contribute to Bitcoin, there may be an incentive to

profit on making an altcoin or altplatform. Unless you create a company that can hire each and every person capable of learning about building these platforms, there will always be competition and an incentive to make an alt which provides its developer with financial remuneration.

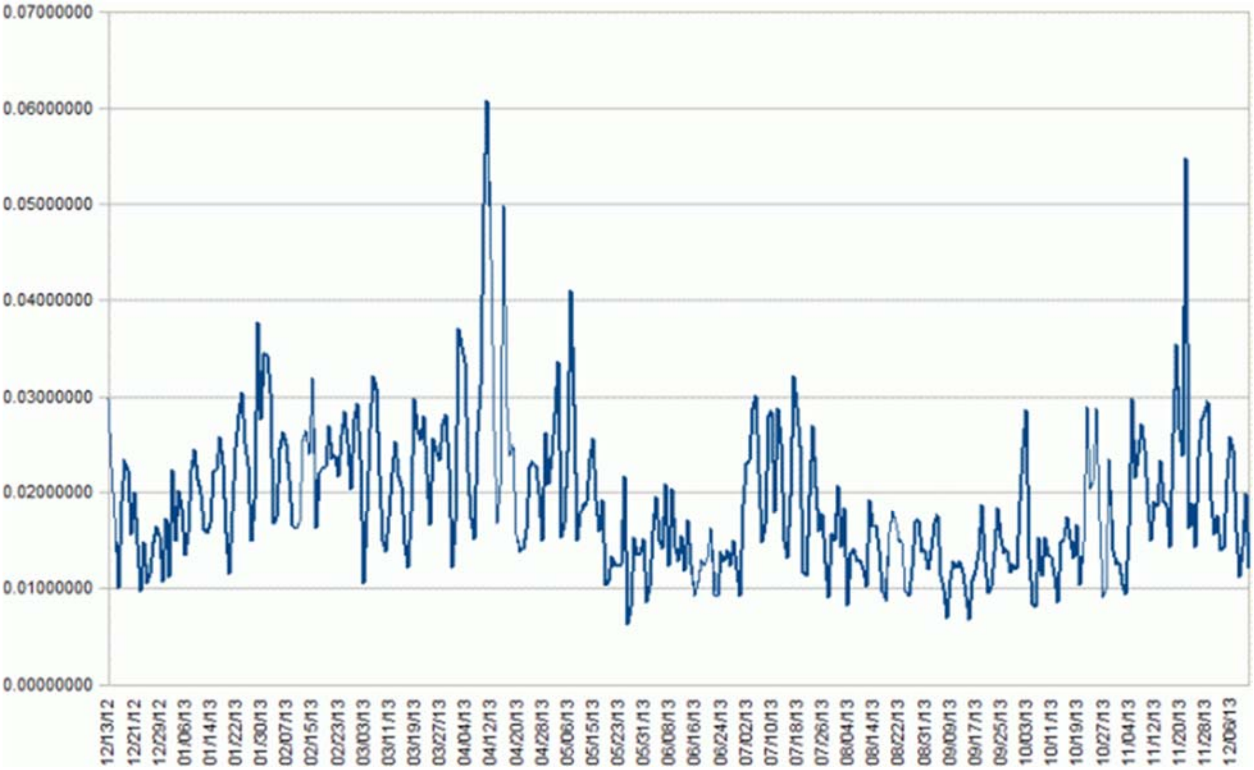
2) ASICs. ASICs are a depreciating capital good that only have a short time frame, a very small window of opportunity (roughly 6 months) to profitably hash nonces. Once they lose their competitive edge, they must be offloaded and replaced with something more powerful. ASIC owners therefore have an incentive to either sell these to a different party willing to take on the risk of never recovering their capital expenditure, or the owner can turn the ASIC and point it towards a more profitable altcoin or alt platform. Because alt tokens are typically open-sourced, the barrier to entry in terms of creating a simple clone is relatively low, especially with turnkey providers like Coingen or Razorcoin. Thus there is a built-in incentive to eke out the last *util* of capital stock which means a continued cycle of concocting new alts.

Just as holding press conferences to talk down price inflation has historically proven to be a futile task, no amount of 'jawboning' will remove these economic incentives. Although the new sidechains proposal will likely bring mindshare (and market share) back to the Bitcoin platform, unless this company (or others like it) can continually hire an increasingly growing developer pool and simultaneously buy all deprecated ASICs, then alts will continue.

Another relevant example is Diners Club. Diners Club was founded in 1950 and was the first charge card company. It laid the foundation, both with spearheading acceptance and in dealing with legal challenges of this segment. However within a decade it faced competition from American Express and later Visa and MasterCard, all of whom had to recreate some forms of physical infrastructure. Yet despite this competition the charge card segment did not spiral into dereliction, but instead flourished. In fact, nearly five decades after it was founded, Diners Club was acquired by one of its competitors, Discover. And despite technological similarities all of these competitors continued to grow and expand globally. Thus, in a competitive marketplace, it is unlikely that altcoins will either completely die or lead to failure of cryptocurrencies as an experiment in peer-to-peer payments. As shown below, there are arguably larger macro issues that have not been highlighted.

Waiting to get rich

As noted above, with the exception of illicit activities, the on-chain transactional volume of Bitcoin has been relatively muted. Jason Kuznicki has attempted to describe the lack of growth in on-chain transactions in graphical form:[95]



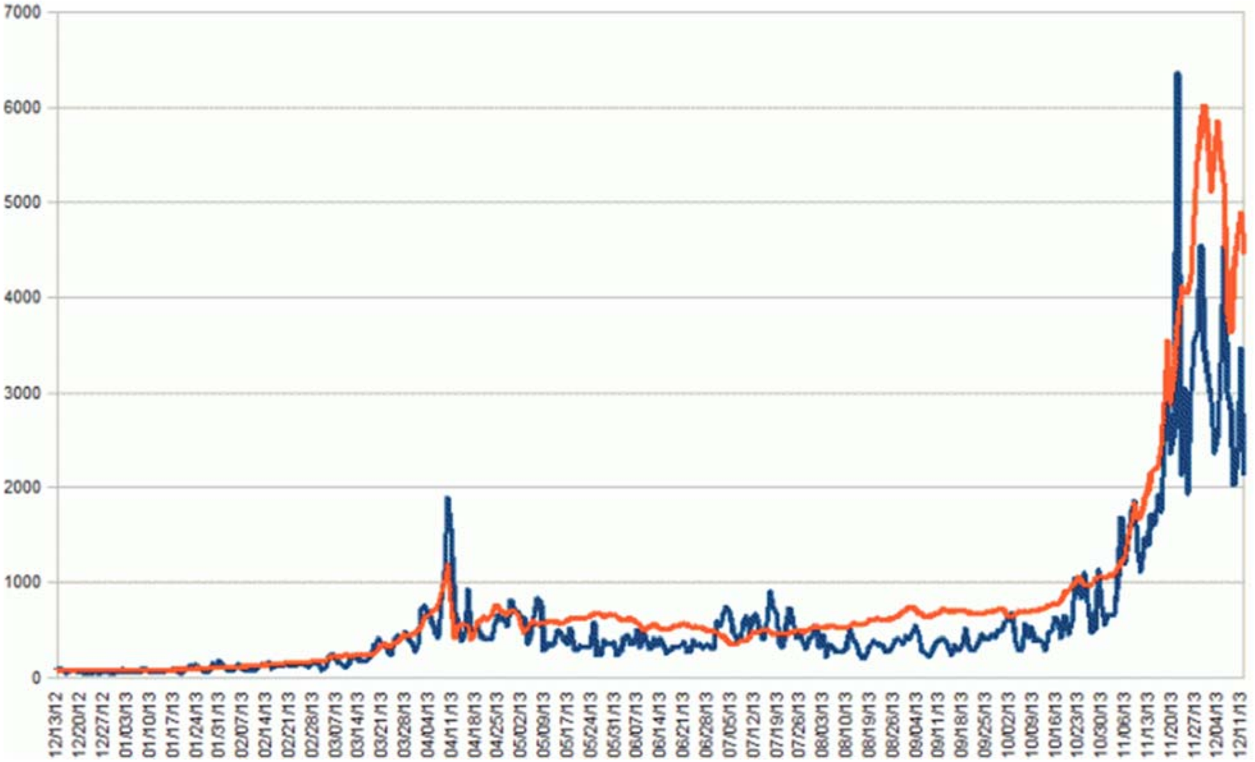
His chart, above, reflects the daily total transaction value of the bitcoin economy, denominated in U.S. dollars, divided by the total market capitalization of the bitcoin economy on that day, denominated in U.S. dollars. Between December 2012 and December 2013, he points out, the velocity of bitcoins remained within a very narrow band.[96] The notable two largest peaks are in April 2013 during enormous global media attention of the platform creating a temporary bubble and at the end of November 2013 when Bitcoin Black Friday (BBF) was held. BBF was the busiest ecommerce day of the year for the network, which achieved 1.5 transactions per second (compared with the average of 0.7 transactions per second and its theoretical maximum of 7 transactions per second).[97]

He notes that:

> The key here is that nothing seems to be happening all that dramatically in bitcoin's velocity of money over time. It's not circulating more rapidly over time, which is what one should expect if it were taking off as a currency, and if more and more transactions were of the form of people passing bitcoins around for stuff. Instead, most transactions (that is, most that don't go dollar-to-bitcoin-and-then-stop) are likely to be money-to-bitcoin-to-stuff, after which the merchant reverts to the dollar as soon as possible. If the bitcoin economy were becoming independent, we might expect a takeoff in the velocity of money, but we're definitely not seeing it yet.

One counter-argument could be made that there is a chicken-and-egg problem that without merchant support, there is no place to spend the tokens: or that in order to provide long-term value which in turn incentivizes new entrepreneurial entrants, savings (capital accumulation) creates reserve demand for a currency. Thus as services such as BitPagos, BitPay and Coinbase continue to on-board merchants, perhaps this trend could change in the future, but then it also may not.

Yet Kuznicki concludes with the following comparison, the blue line is the average value of all bitcoin transactions for the day, in dollars. The orange line is the dollar-denominated price of one bitcoin multiplied by five:



In his view this is evidence that the average person buying bitcoin is simply speculating, or in his words:

> The mode bitcoin is probably mined, disbursed, and never goes anywhere thereafter. The mode transaction is someone buying an arbitrarily chosen amount of bitcoin and then sitting on it forever. Consumers using bitcoin to buy stuff (other than dollars) appear to be few and far between. Bitcoins circulating without immediate reconversion to the dollar are likely very few. And all of this has been true for at least a year.

As noted in *Bitcoin Hurdles*, this is related to game theory, which was described by Koen Swinkels:[98]

> Bitcoin won't succeed unless there are a lot of Bitcoin companies building the Bitcoin infrastructure / Bitcoin economy. So there seems to be a classic public good / positive externality problem here: People are better off free riding on the efforts of others, but if everybody did that there would be nothing to free ride on.

Conclusions

Bitcoin provides at least two novel properties that are considered its competitive advantage: the creation of a trustless infrastructure that can handle bilateral exchange without the use of a trusted third party, all while preventing the double-spending of a ledger unit. However, as described with numerous data points, despite these advantages information security is empirically hard on the edges, with roughly 30% of all bitcoins having been lost, stolen, seized, destroyed or in some manner expropriated from their legal owner. Half of this total number, 15% of all tokens were lost, stolen, destroyed or scammed via exchanges or hosted wallets which are centralized off-chain silos that customers rely on to move between fiat values. While the coins are still technically still on the blockchain, knowing some of these risks for potential losses, because the necessary technical skills to operate on-chain solutions has been prohibitively high or time consuming, new customers conducting due diligence still continue to use edge-based centralized solutions which are typically easier to use and in some cases, are insured. As a consequence, a significant portion of actual utility of the network still relies on the edges in trusted silos. In addition, the perceived complexity is arguably still the largest barrier to entry. Other barriers to entry may include the lack of broad base merchant support and the relative volatility in price levels.   Because of these barriers to entry, comparing the adoption rate with conversion rates used in advertising – where barriers to entry often merely consist of directing your cart planned routes in mature ecosystems – is a topic for further refinement and study.[99]

Furthermore, due to the costs of upfront capital expenditures for ASICs, it is difficult to say what solutions will incentivize the re-on ramping of the mining process by more than a few circle of professionals including malware authors. Simultaneously there are historically very few profitable exits for volunteer work or organizations. If the development of Linux is an indication, someone else will likely capitalize off Bob's volunteer efforts for adding extensibility features to the code. If this is the case in Bitcoin, one continual challenge will be monetarily incentivizing scarce talent like Bob to provide utility in the form of coding and debugging to the main codebase. Failing that Bob will likely be motivated to build competing, profitable platforms of his own instead. And because no two histories are alike, Bitcoin adopters have no specific blue print to build their ecosystem to or from. As a consequence, some liken the current experiment as a five year condensed version of the past century in banking involving scams, booms, bubbles, fractional reserve schemes and outright theft. Providing incentives to overcome these challenges may result in new data illustrating growth in on-chain activity including transactional volume or renewed activity by old dormant addresses.

Acknowledgements

I would like to thank Dave Babbitt, Preston Byrne, Hudson Cashdan, Joseph Chow, Petri Kajander, Taariq Lewis, Jonathan Levin, Andrew Miller, Pieter Nooren, John Ratcliff, Robert Sams, Koen Swinkels and Andy Toshi for their feedback and constructive criticism.

Endnotes

[1] A large portion of this paper is based off a guest presentation I gave on April 28, 2014 at the Symbolic Systems course at Stanford (slides) (video). I can be reached at: tswanson@gmail.com

[2] Is Bitcoin Over the Hill? by Danny Bradbury

[3] John Wanamaker, was a merchant and one of the first pioneers in advertising and marketing. William Lever is the namesake of the modern brand line.

[4] Cryptocurrency may not be an accurate term for describing what bitcoins are. See Bitcoin: a Money-like Informational Commodity by Jan Bergstra and Peter Weijland

[5] Chart from Bring Out Your Dead .... Bitcoins that is by John Ratcliff

[6] Andy Toshi noted that, "Semantically an address is a payment identifier, so if you ever see an address used twice that indicates some confusion on the part of the user. (Alternately it may indicate a public "donation" address from a user who does not care to distinguish between multiple payments, and who also does not care about privacy.) In the future the payment protocol should hide addresses entirely and we can mostly forget about this confusion. So comments like "multiple addresses are often owned by one person" seems to me to represent a semantic confusion. The reason that address counts do not correspond to user counts is simply that addresses identify payments, not users. Similarly there is no distinction between "throwaway addresses" and any other address. All addresses are single-use."

[7] I would like to thank Andy Toshi for clarifying this, as there is semantic conflation between addresses and UTXO.

[8] A Major Coinbase Milestone: 1 Million Consumer Wallets from Coinbase

[9] Coinbase began 2013 with 13,000 wallets and on February 27, 2014 announced it had reached 1 million. In contrast, Blockchain.info had roughly 13,000 wallets as of August 2013 and reached 1 million in January 2014. Thus 14 months versus 17 months. On April 14, 2014, Blockchain.info reached 1.5 million wallets, which are on-chain, yet it is unclear how many are active or have any bitcoins in them (similar uncertainties surround Coinbase wallets). Furthermore, Blockchain.info announced an implementation of CoinJoin (SharedCoin) on November 18, 2013 which coincided with a large increase in wallet creation. Though, it is unclear if wallet creation is instead linked to the increased popularity of Bitcoin in China, the height of which occurred in late November and early December.

[10] One reviewer noted that, "Blockchain's wallets are just as centralized as any other. The blockchain is not structured to host wallets."

[11] A history of Bitcoin in one chart by Jonathan Levin

[12] There are 38,399 addresses with a balance of exactly 50 BTCs. Most are dormant since 2009. I estimate 30-40% of all coins are gone. by rutkdn

[13] Satoshi 's Fortune: a more accurate figure by Sergio Lerner

[14] Chart from Bring Out Your Dead .... Bitcoins that is by John Ratcliff

[15] One reason for this is that the large miners cannot necessarily immediately sell coins in bulk without dramatically depressing the price of bitcoin; the market is sometimes too thin for them to sell their positions.

[16] Bitcoin Distribution by Address at Block 295,000 from Bitcoin Rich List

[17] One reviewer noted that "the claim that 98.08% of all addresses contain less than one Bitcoin is an extreme understatement. In fact it is impossible for more than 21 million distinct addresses to correspond to UTXOs containing 1 bitcoin, but there are 10^48 addresses. So it will always be the case that at least (100 - 10^-38)% of addresses contain less than one bitcoin."

[18] Subpoenas and testifying in front of various government committees raised the public's awareness of Bitcoin, yet conversion rates are still quite low. In contrast, these four companies have not been subpoenaed or received the same amount of publicity, but have expanded both marketshare and user base significantly. This may due to the "hype cycle," see Is Bitcoin Over the Hill? by Danny Bradbury

[19] From oil painter to the C-suite from *Financial Times* and M-Pesa helps world's poorest go to the bank using mobile phones from *The Christian Science Monitor*

[20] Insight: African tech startups aim to power growing economies from *Reuters*

[21] Original announcement thread: New Bitcoin Exchange (mtgox.com)

[22] How ArtForz changed the history of Bitcoin mining by Tim Swanson

[23] The ZeroAccess Botnet – Mining and Fraud for Massive Financial Gain by James Wyke and Microsoft: ZeroAccess botnet has been abandoned from Threatpost

[24] Once upon a time in China, a package shipped by Jeff Garzik, The First Bitcoin ASICs are Hashing Away! from *The Bitcoin Trader,* AVALON ASIC has delivered first RIG (68GH/s Confirmed) 2nd out proof from Bitcoin Talk and Engineering the Bitcoin Gold Rush: An Interview with Yifu Guo, Creator of the First Purpose-Built Miner from *Motherboard*

[25] The economics of gravitating towards specialized hardware and in this case ASICs is described in Bitcoin and The Age of Bespoke Silicon by Michael Taylor

[26] One reviewer noted an imperfect similarity between primary dealers and open market operations with ASICs manufacturers (assuming they mine too), likening them to the new central bank. "This is because they get the hardware before others and thus reap the largest benefits. Especially, since the useful production window of a hardware is around 6 months or so, thus every day counts. Similarly, primary bond dealers receive funds first and therefore can spend the funds first."

[27] There are multiple competing technical terms to describe bitcoin, see Bitcoin: a Money-like Informational Commodity by Jan Bergstra and Peter Weijland

[28] Satoshi stated several times that he wrote the code first beginning sometime in mid-2007 and then later wrote the whitepaper to describe it, see the last comment on November 9th, Re: Bitcoin P2P e-cash paper. See also, What is the Carbon Footprint of a Bitcoin? from *CoinDesk*

[29] This depends strongly on how investors expect the price to behave in the future and this in turn will determine the ratio of capital expenditure to operating expenditure. It should also be noted that there are only 2 years left in which 1.3 million bitcoins will be created. It will halve again in 2016.

[30] The comparison with MasterCard is not entirely apple's to apple's because it is just processing transactions and not acting as a type of seigniorage entity. There is a lot more that goes into a Visa transaction than their overt energy costs. There are also additional layers in bitcoin but much less. Again, in Mastercard case, they only get transaction cost and energy expended by all the support layers, see How Merchant Processing Works from IPPAY. Furthermore, MasterCard spent $299 million on their capital expenditures in 2013.

[31] As ASICs increase the hash/watt efficiencies, they may run into the limits of Koomey's law.

[32] E77 – The Adam Back Interview from *Let's Talk Bitcoin* and Re: [Bitcoin-development] Tree-chains preliminary summary by Peter Todd

[33] [ANN] High-speed Bitcoin Relay Network by Matt Corallo and The Future of Bitcoin: Corporate Mines and Network Peering? from *Data Center Knowledge*

[34] One reviewer noted that "The real mining is done by ASICs, searching for hashes. The blockchain management is done by normal CPU´s, they verify the new blocks, calculate which hash-patterns the miners have to to search for, and communicate with the Bitcoin network. The blockchain management likely needs good bandwidth and good connectivity, but the communication between blockchain management and the mining hardware should take something like 100 bytes every 10 minutes, a case could be argued that it could work great over protocols like Datex-P or old GSM-Data or perhaps even Acoustic coupler´s. Thus in practice it could be one server in a well-connected datacenter e.g. in Europe or the US, and a place with cheap energy for the miners with at least IP connectivity, it does not need to be broadband. The requirements for the blockchain management might change, but the requirements for the communication between blockchain management and mining should remain stable, independent of the amount of transactions on the bitcoin network."

[35] In doing so this would lead to numerous social engineering issues including regulatory oversight.

[36] Feathercoin had a major problem in the spring of 2013, many large mining pools abandoned it (almost all at once) after the block rewards halved ("halvingday") and as a result the difficulty rating remained very high. During the subsequent month very few blocks were able to be processed because the remaining pools did not have the necessary hashrate to cycle through them, reducing the network to a relative crawl. This hashrate overhang ultimately was solved with a hardfork in the code. A similar decrease, though not nearly as severe, took place with the Bitcoin network in the fall of 2012. Following "halvingday" on November 28, the network remained stagnant. It was not until the new ASIC miners were turned on (first from Avalon) that the hashrate began its upward ascent once more. See Section 2.3 in CryptoNote v 2.0 by Nicolas van Saberhagen (likely a pseudonym)

[37] The Bitcoin network, on average, processes roughly 0.7 transaction per second over the past year versus 2,000 per second with Visa.

[38] Robert Sams has written about a number of these issues on Cryptonomics, the quote comes from personal correspondence, April 18, 2014

[39] One reviewer does not see decentralization as binary. In this instance, once 51% of the hashrate is secured by honest miners, the remainder of the hashrate – for security purposes – is deadweight.

[40] Following the Money: Trends in Bitcoin Venture Capital Investment by Garrick Hileman. In an email exchange with Hileman he noted that the $200 million figure comes from Wedbush.

[41] This figure could increase due to numerous undisclosed hardware purchases by private parties including enterprises and investors in this space

[42] Bitcoin Hurdles: the Public Goods Costs of Securing a Decentralized Seigniorage Network which Incentivizes Alternatives and Centralization by Tim Swanson

[43] Data for Figure 1 came from: CoinDesk BPI, BitInfoCharts – Litecoin, BitInfoCharts – Namecoin. Note that Namecoin prices generally track Bitcoin at a 0.005 ratio.

[44] One of many instances include this comment on reddit.

[45] This comment received a lot of criticism, primarily along the lines of how a PoS allegedly cannot provide consensus and Ripple can, but requires some trust and only in a distributed fashion. These issues will likely continue being discussed in future papers, suffice to say that if these systems are vulnerable there should be an economic incentive for them to be hacked. See Proof-of-stake, Ripple protocol

[46] Technically speaking, it is like that their (variable) electricity costs that matter significantly more because hardware costs are fixed (e.g., electricity typically costs about 98% of the total cost of mining). The amortized cost of the hardware usually only enters the calculation before the miner buys the system.

[47] Bitcoin Miner Taps Dad's Power Plant in Virtual-Money Hunt: Tech from *Bloomberg*

[48] One reviewer noted that, "There may also be an element of the sunk costs fallacy applying – irrational behavior arising from a psychological aversion to realizing that the amounts they had invested in their mining hardware are now worthless, the shutting down of which would constitute realizing the loss."

[49] The ZeroAccess Botnet – Mining and Fraud for Massive Financial Gain by James Wyke

[50] Gaming Company Fined $1M for Turning Customers Into Secret Bitcoin Army from *Wired*

[51] Symantec takes on one of largest botnets in history from *c|net*

[52] Fred Trotter, estimates that since January 2009, the mining process of Bitcoin has consumed 150,000 megawatt hours of electricity, which is equivalent to a year's worth of electricity for about 14,000 average U.S. homes. See Malignant computation from *O'Reilly* and Bitcoin Miner Taps Dad's Power Plant in Virtual-Money Hunt: Tech from *Bloomberg*

[53] GPU Roaring? You May Be Infected With a Bitcoin Trojan Says Symantec from *Daily Tech*, World's most dangerous botnet mines Bitcoins from *The Inquirer*, Security researchers kill Kelihos again after Bitcoin crime spree from *ArsTechnica*, Cybercriminals Unleash Bitcoin-Mining Malware from TrendMicro, More users, more attacks: Kaspersky Lab stats show a surge in Bitcoin cybercrime from Kaspersky, Bitcoin Botnet Mining from Symantec, IAmA a malware coder and botnet operator, AMA from reddit and Have there been reports of botnets mining Bitcoin / crypto-currencies? from StackExchange

[54] Botcoin: Monetizing Stolen Cycles by Huang *et. al.* Another paper from the same team discusses the differences between "light" and "dark" mining pools, Poster: Botcoin – Bitcoin-Mining by Botnets

[55] Microsoft Destroys Bitcoin Mining Botnet Sefnit from *CoinDesk*

[56] FPGAs and ASICs are credited for pushing out small botnet operations which still require a certain amount of working capital to maintain which could not be covered with increasingly less competitive hashrate from CPUs nodes. See Bitcoin & Gresham's Law - the economic inevitability of Collapse by Philipp Güring & Ian Grigg and A Botnet herder mining Bitcoin from Zooko Wilcox-O'Hearn

[57] Personal correspondence with two mining startups in China.

[58] CoinLab's Alydian files for bankruptcy and reveals debt of over $3.6m from *CoinDesk*

[59] A Non-Outsourceable Puzzle to Prevent Hosted Mining by Andrew Miller

[60] The Dogecoin defense force is one such group.

[61] SatoshiDICE.com - The World's Most Popular Bitcoin Game by Erik Voorhees. On May 4, 2012 Stephen Gornick calculated that of the 42,152 total transaction on the blockchain, 21,076 transactions were wagers related to Satoshi Dice. This volume doubled within four days, as Gornick posted an update that 94,706 total transactions on the blockchain, 47,353 were wagers.

[62] Re: Satoshi Dice -- Statistical Analysis from Bitcoin Talk

[63] Prior to emptying its wallet (the first time), on its then-summer 2012 height, Silk Road's public address (1DkyBEKt5S2GDtv7aQw6rQepAvnsRyHoYM) contained 5% of all mined bitcoins at that point. See A Fistful of Bitcoins: Characterizing Payments Among Men with No Names by Meiklejohn *et al*.

[64] Sealed Complaint 13 MAG 2328: United States of America v. Ross William Ulbricht from the Federal Bureau of Investigation

[65] Ross William Ulbricht is the alleged creator and owner of Silk Road, see Silk Road, Shut Down in Fall, Had Digital Outpost in Pennsylvania from *The New York Times*. Erik Voorhees is the founder of Satoshi Dice, he sold the company a year after its creation and the company is currently under investigation from the SEC. See Bitcoin company acquisitions begin: Gambling site SatoshiDice sells for $11.5m (126,315 BTC) from *CoinDesk* and Gambling Website's Bitcoin-Denominated Stock Draws SEC Inquiry from *Bloomberg*

[66] A detailed analysis of transactional volume can be found in A Fistful of Bitcoins: Characterizing Payments Among Men with No Names by Meiklejohn *et al*. See also, The Completely Insane Saga of CoinBet.cc by Neil Sardesai

[67] Total-factor productivity

[68] Casino Industry Accounts For Significant Slice Of U.S. Economy: Study from *The Huffington Post*

[69] List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses from Bitcoin Talk. Note: on April 12, 2014 I contacted the creator of the list (dree12 by email) and have verified all but the Allinvain theft. I then contacted Allinvain on April 14, 2014 and the user said "I'm afraid there is nothing new. No coins have been recovered and the thief was not found. I've essentially given up."

[70] The user dree12 recently updated the previous list but as of this writing has not added the following: 5,800 PicoStocks; 96,000 Sheepmarketplace; 4,474 Silk Road 2; 335 Pony virus; 896 Flexcoin; 1,454 Vircurex; 950 Cryptorush; 1,295 BIPS; 484 Bitcash.cz; 7,500 James Howell's laptop; 2,130 Proof-of-burn (Counterparty); 41,928 CryptoLocker ransomeware.

[71] A number of reviewers suggested using "rightful" owner instead of "legitimate" for this paper.

[72] One reviewer provided a thought experiment of stolen coins. What if these coins have actually gone back into circulation and are being used actively in the criminal network and beyond, "this in a quantity theory of money sense or Metcalfe's law sense means that the network is more valuable. But it certainly detracts legitimacy that has to be earned in the eyes of people that enjoy well defined property rights or at least some concept of rightful ownership. Indeed play out the thought experiment that Coinbase was looted and those coins are now in the hands of some criminals that walk to the exchange and sell the coins. Even assuming that no one finds out about the heist for many hours, this would damage the network forever."

[73] One reviewer noted that, "Tomorrow Satoshi Nakamoto could decide to start moving his bitcoins around. He could do that a year from now. Or ten years from now. And, it's highly likely, that Satoshi probably has control over those keys. He was a thoughtful and careful person when it came to cryptography. I would say it's quite likely he still controls those keys. What he plans to do with them, is unknown. While it's interesting to note how many bitcoins may or may not be lost or gone, other than the uncertainty of it, it doesn't really matter economically. It has been argued that the entire world-wide economy could operate on a single bitcoin, such is the power of mathematics and numbers with a whole lot of decimal places."

[74] Talking Bitcoin With the Winklevosses, Naval Ravikant, and BalajiSrinivasan from *TechCrunch*

[75] $4.1m goes missing as Chinese bitcoin trading platform GBL vanishes from *CoinDesk*

[76] CryptoDefense, the CryptoLocker Imitator, Makes Over $34,000 in One Month from *Symantec*

[77] In order to reclaim James Howell's laptop and hard drive from the landfill this would take real world digging and "mining." See Missing: hard drive containing Bitcoins worth £4m in Newport landfill site from *The Guardian* and Digital Gold Rush: The Bitcoin Boom and Its Many Risks from *Der Spiegel*

[78] Nakamoto's Neighbor: My Hunt For Bitcoin's Creator Led To A Paralyzed Crypto Genius from *Forbes*

[79] Stories on forums over the years include spouses and significant others who have taken computers out of spite and anger, never returning them. Some hard drives on these purportedly include hundreds of bitcoins each.

[80] While many exchanges now have created purported "dark pool" or "dark liquidity" services (such as Prime from Trade Hill, prior to its closure), it is unknown how large these may be and likely that they are not using the term correctly. Other intermediary platforms may trade between these "dark pools" as well, including TruCoin. The pools exist to protect an institutions trading strategy from other participants and typically the sell side comes from large mining pools and merchant processors. In reality these are likely, hidden or reserve orders: implemented by exchanges and other marketplaces with the intent to allow traders to place larger orders discretely, in an attempt to avoid moving the market up or down.

[81] Mt. Gox files for bankruptcy, hit with lawsuit from *Reuters*

[82] Mt. Gox Finds 200,000 Missing Bitcoin from *The Wall Street Journal*

[83] For discussion on Coinmarket.io see dozens of threads in the late 100s and early 200s: CoinMarket.io | New, self-moderated support and news thread.

[84] Scam exchange cryptorush implodes with epic drama (support staff breaks ranks) from reddit

[85] Cyprus police issues arrest warrant for bitcoin entrepreneur from *Cyprus Mail*

[86] Bitfoo is the international name for Bifubao. See With Bifubao's Wallet, Users Can Prove Funds via Cryptography from *CoinDesk*

[87] Xapo Raises $20 Million for 'Ultra-Secure' Bitcoin Storage from *CoinDesk*

[88] Securing wallets by integrating a third-party Oracle from CryptoCorp

[89] Roger Ver, founder of Blockchain.info claims that the wallet is an "on-blockchain" solution yet it is still centralized. See Roger Ver on Blockchain's Past, Present and Future from *CoinDesk*

[90] Armory features

[91] The usage of paper wallets raises an important question: if Bitcoin is supposed to be a new form of electronic cash, is not the usage of paper wallets (or notes) just a recreation of the old monetary order?

[92] Even though m-of-n transactions has been supported since the acceptance of BIP 11 in 2011 and BIP 16 the following year, implementations of multisig has been slow going until recently due to lack of support from wallet software. This will likely change, yet as of this writing, no address on the Bitcoin Top 500 Rich List uses on-chain multisig.

[93] Personal correspondence, April 19, 2014. "The legal system is not entirely ill-equipped for cryptoledgers - particularly in relation to crime, where the law is fairly well-established," he says. "Blockchains pose more practical, rather than conceptual, problems. In terms of protecting and putting other parties on notice of property rights, new rules and transfer formalities would need to be established, with something like two-factor or three-factor authentication (or multisig) required for a valid transfer of certain types of crypto-titles. On the basis that some fraudulent transfers might still get through, however, the extent to which the market might tolerate wholly decentralised ledgers is an open question. I can't see the market - large or small - committing much by way of funds to a decentralised autonomous organization (DAO) which doesn't have a well-insured human corporate backdoor. Re-introducing some trust would, I suspect, be a price many would happily pay for the benefit of added accountability."

[94] Blockchain 2.0 – Let a Thousand Chains Blossom from *Let's Talk Bitcoin*

[95] These Three Graphs Prove That Bitcoin Is a Speculative Bubble by Jason Kuznicki

[96] One reviewer noted that "Velocity analysis is really important. For something that purports to be a currency, it is the key metric of success with respect to its role as a medium-of-exchange. There is likely a correlation between the fx rate and tx volume due to speculative demand. However it is uncertain that the price chart of fx and USD tx volume proves that. In the future, a researcher could equally tell the story that the fx rate is being driven by increasing tx demand. Without a way to distinguish block tx due to fx settlements and block tx due to trade in real goods (and of course estimating tx due to change, same-person wallet transfers, etc), these series are likely ambiguous."

[97] BitPay alone processed 6,926 bitcoin-based transactions on November 29th last year up from 99 transactions on the same day the year before, see BitPay Drives Explosive Growth in Bitcoin Commerce from *BusinessWire*

[98] Why start or invest in Bitcoin companies? Why not free ride Instead? by Koen Swinkels. This topic also been discussed by others: Talking Bitcoin With the Winklevosses, Naval Ravikant, and BalajiSrinivasan from *TechCrunch* and Why would you invest in a Bitcoin-related company instead of Bitcoins? by Adam Draper

[99] One reviewer noted that, "The conversion rates and metrics exist for many other industries and markets. But comparing them with Bitcoin would not necessarily be relevant at this stage because of the much higher barriers to entry (friction of access) in participating on the Bitcoin network."