Bitcoin Hurdles: the Public Goods Costs of Securing a Decentralized Seigniorage Network which Incentivizes Alternatives and Centralization

By Tim Swanson[1]

Revised: April 9, 2014

Abstract

Bitcoin has provided a creative way to solve several long-standing problems in computer science yet despite its innovations, there are still fundamental technical and governance hurdles that limit its growth. This includes the financial incentives for operating a centralized mining pool, the centralization of infrastructure without the benefits of centralization, the lack of financial incentives for working as a developer and the various public goods issues surrounding a communal effort beholden to lobbying by special interest groups.

Background

A public good is a good that is non-rivalrous and non-excludable in that users are not excluded from its use yet simultaneously such usage does not reduce the availability of said good. Traditional examples include air, light houses and street lighting.

Bitcoin is a decentralized cryptographically controlled ledger database system released via an MIT license in January 2009.[2] When spelled with an uppercase "B" Bitcoin refers to a peer-to-peer network, open-source software, decentralized accounting ledger, software development platform, computing infrastructure, transaction platform and financial services marketplace.[3] When spelled with a lowercase "b" bitcoin it refers to a quantity of cryptocurrency itself. A cryptocurrency is a virtual token (e.g., a bitcoin, a litecoin) having at least one moneyness attribute, such as serving as a medium of exchange. It is transported and tracked on an encrypted, decentralized ledger called a cryptoledger.[4]

According to a whitepaper released in November 2008, the original author of the protocol was trying to resolve the issue of creating a trustless peer-to-peer payment system that could not be abused by outside 3rd parties such as financial institutions.[5] Or in other words, while there had been many previous attempts at creating a bilateral cryptographic electronic cash system over the past twenty years, they all were unable to remove a central clearing house and thus

were vulnerable to double-spending attempts by a trusted 3rd party. In contrast, the Bitcoin system utilized novel approach by combining existing technologies to create the Bitcoin network, most of which were at least a decade old.

According to Gwern Branwen, the key components necessary to build this system were:[6]

2001: SHA-256 finalized

1999-present: Byzantine fault tolerance (PBFT etc.)

1999-present: P2P networks (excluding early networks like Usenet or FidoNet; MojoNation & BitTorrent, Napster, Gnutella, eDonkey, Freenet, etc.)

1998: Wei Dai, B-money

1998: Nick Szabo, Bit Gold

1997: HashCash

1992-1993: Proof-of-work for spam

1991: cryptographic timestamps

1980: public key cryptography

1979: Hash tree

While there are other pieces, one component that should also be mentioned which will later be used as an illustration of the nebulous governance surrounding the protocol is the Elliptic Curve Digital Signature Algorithm (ECDSA) and is the public-private key signature technique used by the Bitcoin network.

As noted above, while the underlying mathematics and cryptographic concepts took decades to develop and mature, the technical parts and mechanisms of the ledger (or blockchain) are greater than the sum of the ledger's parts. Yet bitcoins (the cryptocurrency) do not actually exist.[7] Rather, there are only records of bitcoin transactions through a ledger, called a blockchain. And a bitcoin transaction (*tx*) consists of three parts:

an input with a record of the previous address that sent the bitcoins;

an amount; and

an output address of the intended recipient.

These transactions are then placed into a block and each completed block is placed into a perpetually growing chain of transactions —hence the term, block chain. In order to move or transfer these bitcoins to a different address, a user needs to have access to a private encryption key that corresponds directly to a public encryption key.[8] This technique is called public-key encryption and this particular method, Elliptic Curve Digital Signature Algorithm

(ECDSA), has been used by a number of institutions including financial enterprises for over a decade.[9][10] Thus in practice, in order to move a token from one address to another, a user is required to input a private-key that corresponds with the public-key.

Economics does not have a category of "property," as it is the study of human actors and scarce resources.[11] Property is a legally recognized right, a relation between actors, with respect to control rights over given contestable, rivalrous resources. And with public-private key encryption, individuals can control a specific integer value on a specific address within the blockchain. This "dry" code effectively removes middlemen and valueless transaction costs all while preserving the integrity of the ledger. In less metaphysical terms, if the protocol is a cryptocurrency's "law," and possession is "ownership," possession of a private key corresponding to set of transaction (*tx*) outputs is what constitutes possession.[12] All crypto assets are essentially bearer assets. To own it is to possess the key. The shift from bearer, to registered, to dematerialized, and back to bearer assets is like civilization going full circle, as the institution of property evolved from legal right (possession of property) to the registered form (technical ability to control) that predominates in developed countries today.

To verify these transactions and movements along the ledger, a network infrastructure is necessary to provide payment processing. This network is composed of decentralized computer systems called "miners." As noted above, a mining machine processes all bitcoin transactions (ledger movements) by building a blockchain tree (called a "parent") and it is consequently rewarded for performing this action through seigniorage. Seigniorage is the value of new money created less the cost of creating it.[13]

These blockchain trees are simultaneously built and elongated by each machine based on previously known validated trees, an ever growing blockchain. During this building process, a mining machine performs a "proof-of-work" or rather, a series of increasingly difficult, yet benign, math problems tied to cryptographic hashes of a Merkle tree, which is meant to prevent network abuse.[14] That is to say, just as e-commerce sites use CAPTCHA to prevent automated spamming, in order to participate in the Bitcoin network, a mining machine must continually prove that it is not just working, but working on (hashing) and validating the consensus-based blockchain.[15][16] At the time of this writing the computational power of the network is 200 petaflops, roughly 800 times the collective power of the top 500 supercomputers on the globe.[17]

To prevent forging or double-spending by a rogue mining system, these systems are continually communicating with each other over the internet and whichever machine has the longest tree is considered the valid one through pre-defined "consensus." That is to say, all mining machines have or will obtain (through peer-to-peer communication) a copy of the longest chain and any other shorter chain is ignored as invalid and thus discarded (such a block is called an "orphan").[18] If a majority of computing power is controlled by an honest system, the honest chain will grow faster and outpace any competing chains. To modify a past block, an attacker (rogue miner) would have to redo the previous proof-of-work of that block as well as all the blocks after it and then surpass the work of the honest nodes (this is called a 51% attack or 51%

problem).[19] Each 10 minutes (on average) these machines process all global transactions – the integer movements along the ledger – and are rewarded for their work with a token called a bitcoin.[20] The first transaction in each block is called the "coinbase" transaction and it is in this transaction that the awarded tokens are algorithmically distributed to miners.[21]

When Bitcoin was first released as software in 2009, miners were collectively rewarded 50 tokens every ten minutes; each of these tokens can further be subdivided and split into 10^8 sub-tokens.[22] Every 210,000 blocks (roughly every four years) this amount is split in half; thus today miners are collectively rewarded 25 tokens and in 2016-2017 the amount will be 12.5 tokens. This token was supposed to incentivize individuals and companies as a way to participate directly in the ecosystem. And after several years as a hobbyist experiment, the exchange value of bitcoin rose organically against an asset class: fiat currency.

Current situation

While the transportation mechanism still exists in a decentralized form, the processing is done in an increasingly centralized form. But before delving into these infrastructure and logistical issues, there are several unseen, hidden costs that should be explored.

Transaction Cost	Precious Metals	Fiat Currencies	Bitcoin
Storage	0.15% to 1% per year	Subsidized by FRB*	*Free and 100% reserve*
Transportation	Expensive	Inconvenient	*Free & Easy*
Security	Physical	Institutional	*Cryptographic*
Fiduciary media	Inevitable	Inherent	*Impossible*
Recordkeeping	Manual	Manual	*Automatic*
Counterfeiting	Impossible	Inevitable	*Impossible*
Issuance	Mining	Politics	*Algorithm*
Payment clearing	Expensive	Centralized	*Cheap & Distributed*
Scarcity	High	Arbitrary	*Fixed - 21 million btc*
Authentication	Expensive assay	Trust counterparty	*Built-in*

** fractional reserve banking*

In the chart above created by Pierre Rochard, showing the transaction cost advantages a cryptocurrency such as Bitcoin purportedly has over fiat and precious metals, there should probably be an asterisk next to "Built-in" because while it is true, authentication is built-into the protocol, securing signatures is becoming one of the most expensive part of Bitcoin due to hacking and due to resource constraints: to perform authentication oneself, one must have a computer downloading and storing the entire blockchain and confirming the transactions – there is an entire subindustry of wallet and security providers now – many of whom have raised multimillionaire dollar investments.[23][24]

The blockchain is over 14 gigabytes yet with relatively little usage. Besides computational cost of creating proof-of-work transaction evidence (which is already being addressed by altcoins and alternative platforms through proof-of-stake and Ripple), ledger size is another creeping

issue and adding new data types such as contract storage through the existing framework, as discussed later, could conceivably make it even more costly (though this itself does not mean it will not be included or implemented in Bitcoin or other systems). Yet it should be noted that the first issue is being tackled through a system originally detailed in the Bitcoin whitepaper, called Simplified Payment Verification (SPV) and other projects like Greg Maxwell's proposed CoinWitness compression method may be implemented later on, reducing the costs of the second issue.[25]

There should also be another asterisk next to Counterfeiting Precious Metals. Because of similar densities and therefore weight, gold-coated tungsten bars are a common way to defeat this.[26]

In addition, another asterisk should be placed next to Transportation, because it is not free. As Robert Heinlein might note, there is no such thing as a free lunch.[27] For example, on-chain Bitcoin transfers may be more expensive than traditional credit card transfers, not cheaper. The actual costs of bitcoin transfers masked by price appreciation and token dilution in the form of scheduled monetary inflation. Each day, approximately 3600 bitcoins are added to the network, all of which go to those running the network (the miners). While the volume of transaction varies day-by-day, at 60,000 transactions a day, based on current prices of $600, bitcoin miners are receiving $35 per transaction they process.[28] This price fluctuates and it should also be noted that the marginal costs of adding transactions is almost zero. This will be discussed at length later.

Based on calculations provided by Dave Carlson, founder of an ASIC mining pool called Megabigpower, he estimates that at their current hashrate of 10 terahashes per second the pool mines roughly 1 bitcoin per day.[29] In doing so the systems consume 10 kW of electricity. Thus Carlson's firm uses one watt per GH/second. Because this equipment runs all day, it collectively consumes 240 kW·h, which according to IEA conversions amounts to roughly 312 pounds of carbon dioxide per coin. Other mining pools may have different electrical rates due to varying geographic locations. And while some pools have begun taking advantage of geographical arbitrage (moving to cooler climates and relatively cheap energy sources), the sole generation of power for Carlson's pool is through a hydroelectric dam. For comparison, the United States Treasury department alone consumes 335,520,255 kW·h of energy each year.[30] Thus, ignoring the rest of the financial and credit systems, the energy used to power this one department could power the entire Bitcoin network for 388 days at the current difficulty rating. Yet this is not an apples-to-apples comparison because the Bitcoin network processes a mere 60,000 transactions per day and the "market cap" of all mined bitcoins is roughly $7 billion at the time of this writing; both marginal in comparison to the transaction volume and value processed by most financial institutions in the United States today.

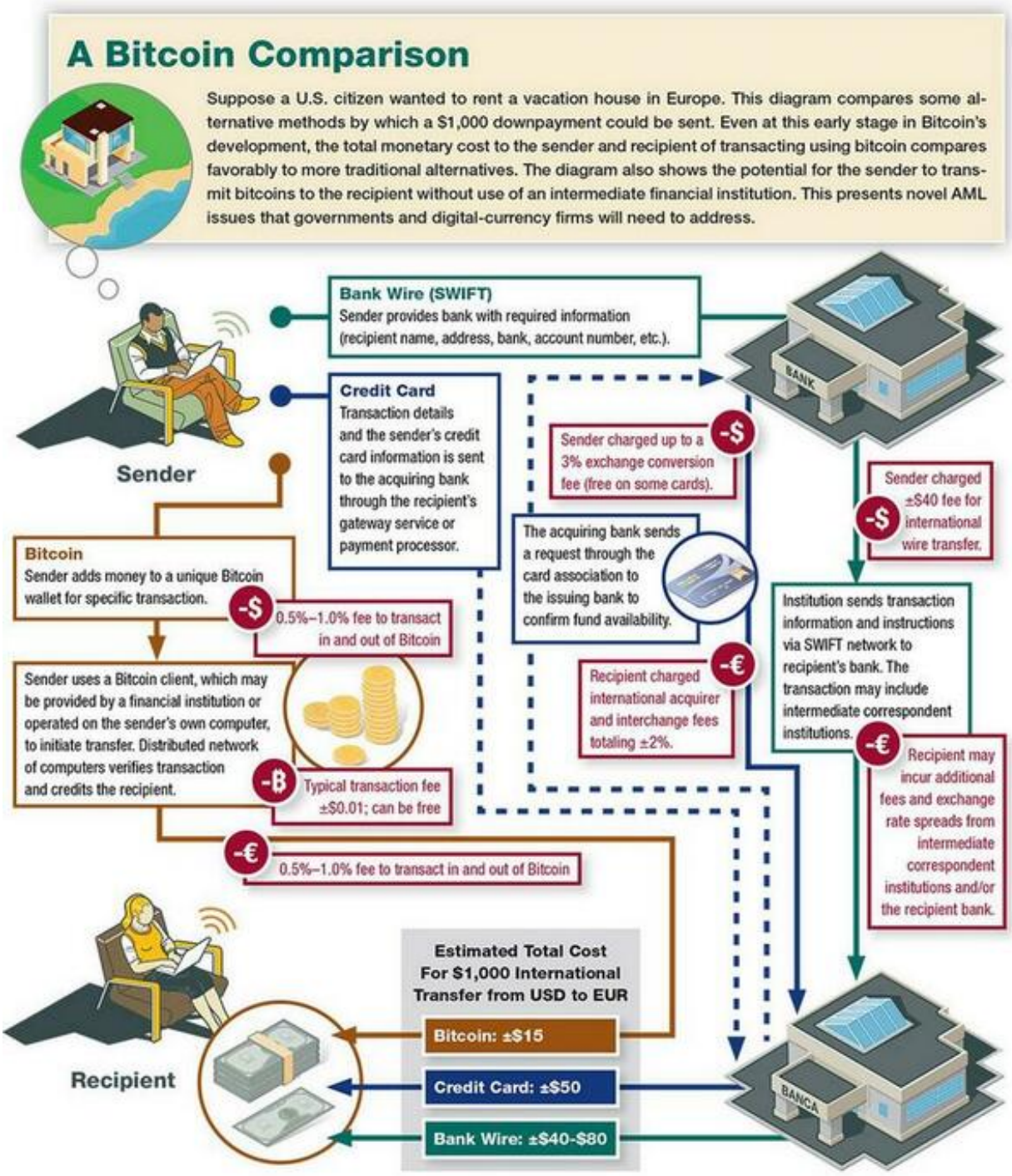
Despite the deadweight loss involved in securing the network – the arguable waste of electricity spent in the proof-of-work method – Bitcoin seigniorage is likely still cheaper than fiat seigniorage.[31] For instance, in 2010 the United States federal government spent $614,400,000

producing new currency notes just for that year alone (this includes the paper and printing) — a 50% cost increase in two years due to inflation.[32] The footprint of 3 billion euro notes in circulation during 2003 was equivalent to 460,000 60W bulbs switched on for a year. USD notes are comprised of 75% cotton and 25% linen.[33] 10,308,370 lbs of cotton were used in 2009 to circulate new USD notes alone (the old ones are removed and destroyed).[34] This also does not take into account the carbon used by machines that sew, harvest, spin, transport the cotton. And it also ignores all of the metal coins in circulation that originated in mines, were extracted, transported, smelted and stored — a supply chain that requires carbon consumption. One also needs to factor in the amount of counterfeiting that consumes carbon to forge banknotes that takes place globally. Or the cost of maintaining a financial and banking industry, with at minimum, hundreds of thousands of branches around the world that utilize valuable real estate to house those institutions, employ millions of people at great cost, require transportation of each of those people to and from their homes.

With that said, strictly speaking however, the comparison above is not entirely valid either, that the cost of Bitcoin seigniorage is lower than that of fiat.[35] The United States Treasury spends less producing a note than the face value, whereas the cost of creating a new bitcoin will equal its exchange value on average.[36] The United States government may have spent more in *absolute* terms than miners spent on electricity, but then the outstanding value of fiat is much greater than the market cap of Bitcoin. The cost as a percent of value in this case is what matters.

More precisely, seigniorage is value of new supply less cost. On the usual definition, there is no bitcoin seigniorage at the margin, the value of the new supply is burned up in hashing. Relevant to the discussion later in this paper, while it could be stated that seigniorage exists in the form of price appreciation, but this is extending the definition here as the concept is usually applied to money that acts as a unit of account and is a (theoretical) liability of the issuer, neither of which apply to Bitcoin. The actual comparison is the total cost of producing a cryptocurrency plus running the payments network, which is lower than the United States Treasury's cost of creating and replacing paper plus bank and credit card transaction fees, in percentage terms.[37]

Comparison against incumbents

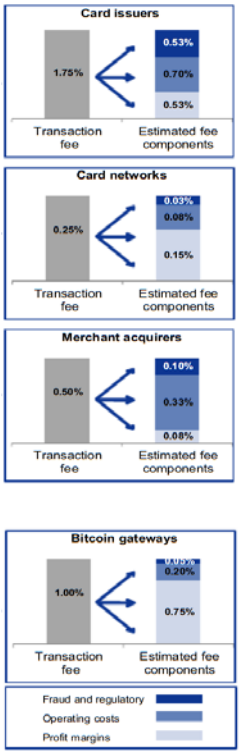


The above flowchart is another illustration that intends to show the purported transactional costs of Bitcoin.[38] While the timing aspects tilt in the favor of Bitcoin, the estimated costs do not include the mining costs, the dilution of bitcoin. This is important as later the discussion

over block rewards and halving as well as block sizes could become the linchpin to the success of this decentralized system.[39]

Underbanked and remittances

As will be described in later sections, because current decentralized systems cannot beat incumbent credit card processors on speed and confirmations, Bitcoin adopters are encouraged to go where Visa is not. For instance, Paypal is not offered in 60 countries yet there are many writers and bloggers in those same countries, hence WordPress adopted Bitcoin two years ago to provide services to the underbanked.[40]



One additional area that applies to the residents of these countries was recently detailed in a Goldman Sachs report: by using the Bitcoin network today, retail merchants, online merchants and remittance consumer could find $210 billion of savings.[41] Though, to be clear, unlike a recently released UBS report, the Goldman Sachs report does not take into account the actual transaction costs of using the network (i.e., 1% fee).[42] In fact, the discrepancy between the two (UBS cites a 4% average transaction fee) hinges on what to include in the calculation: the Goldman Sachs report does not mention the block rewards and money supply aspect in terms of share dilution or the fact that there are monetary costs of maintaining the infrastructure; whereas the UBS takes the miners revenue and divides by the number of transactions.[43]

In terms of remittances, in 2012 Western Union generated $4.6 billion in transaction fees and had a net profit margin of 16%.[44] A recent report from the World Bank found that the 232 million international migrants working abroad remitted an estimated $550 billion in 2013 – the top three countries for incoming remittances reached $71 billion in India, $60 billion in China and $26 billion for the Philippines.[45][46] Fees charged by various levels of middlemen providers, exchangers and compliance offices collectively add another $74 billion from this process, with no value added. For example, African migrants could save $4 billion USD by simply reducing current remittance fees of 12.4% to 5%.[47] Globally the average fee on remittances is 9% and many banks charge an additional "lifting" fee that adds another 5% to remit it into local currency.

While Bitcoin could shine in this one particular segment, as block rewards are halved and transaction fees by miners are floated, these costs to end users could in fact grow starting as early as 2016.

Potential annual net savings with Bitcoin based on 2013 volumes

2013 Market Size ($bn)	Retail	E-commerce	Remittances
Dollar volume by market	10,383	609	549
Prevailing average pricing	2.5%	2.9%	8.9%
Bitcoin pricing	1.0%	1.0%	1.0%
Prevailing transaction fees	259.6	17.8	48.9
Bitcoin transaction fees	103.8	6.1	5.5
Potential savings with Bitcoin ($ bn)	155.7	11.8	43.4

Source: Goldman Sachs Global Investment Research.

Disadvantages of Bitcoin versus M-PESA and Visa

Since the creation of the genesis block in January 2009, while Bitcoin's network of intentional 10 minute confirmation times may be faster than moving gold or processing a bank wire which can take days or weeks, it is several orders in magnitude 'slower' than current payment systems such as Visa which while averaging 2,000 transactions per second, is capable of processing 10,000 transactions per second and even 20,000 during surges.[48] It should be noted, that this 10 minute block interval (approximately) is not currently a problem today as while the capacity is less, the usage is low as well (0.7 transactions per second), so it is not as if the network itself is slowing transactions down.

This is also not necessarily a design flaw, but rather a known hardcoded limit set from day one.[49] Block sizes can be increased relatively easily, by merely replacing a couple lines of code a core developer could increase the block size from the current 1 MB to 10 MB or even 100 GB.[50] At 1 MB the network is limited to 7 transactions per second, forcing any high-frequency trading (HFT) to the edges, into off-chain solutions such as centralized exchanges using their own infrastructure and databases. While efficient and effective, these are trusted party and when you trust a 3rd party, you are exposing yourself to the malfeasance of that 3rd party.[51]

The downside to the increased block size approach is a resource issue. In order for a decentralized system to scale these transaction sizes on a global level, centralization of resources will likely be required. That is to say, in order to increase the network speed by a factor of 100x, a mining system would need to be able to download and process 100 MB of data every second, storing and filling hard drives very quickly and saturating bandwidth. Thus in a twist, while Bitcoin has succeeded in providing a proof-of-concept experiment of what decentralized, trustless bilateral exchanges can look like, in order for them to compete against incumbents, it will likely become increasingly centralized. In fact, another issue with proposed larger block sizes is that unless the miners invest in more effective network equipment, there is an increased frequency of *orphaned* blocks; this then adds a barrier to entry and thereby reduces the pool of miners to well-capitalized professionals.[52][53] And while developers such as Peter Todd have designed alternative solutions involving the integration of off-chain decentralized systems capable of processing at these higher throughputs, some of the Bitcoin core development team is moving towards using a two-way pegged method combining merged mining and atomic transactions as described in a new project by Adam Back and Austin Hill.[54][55]

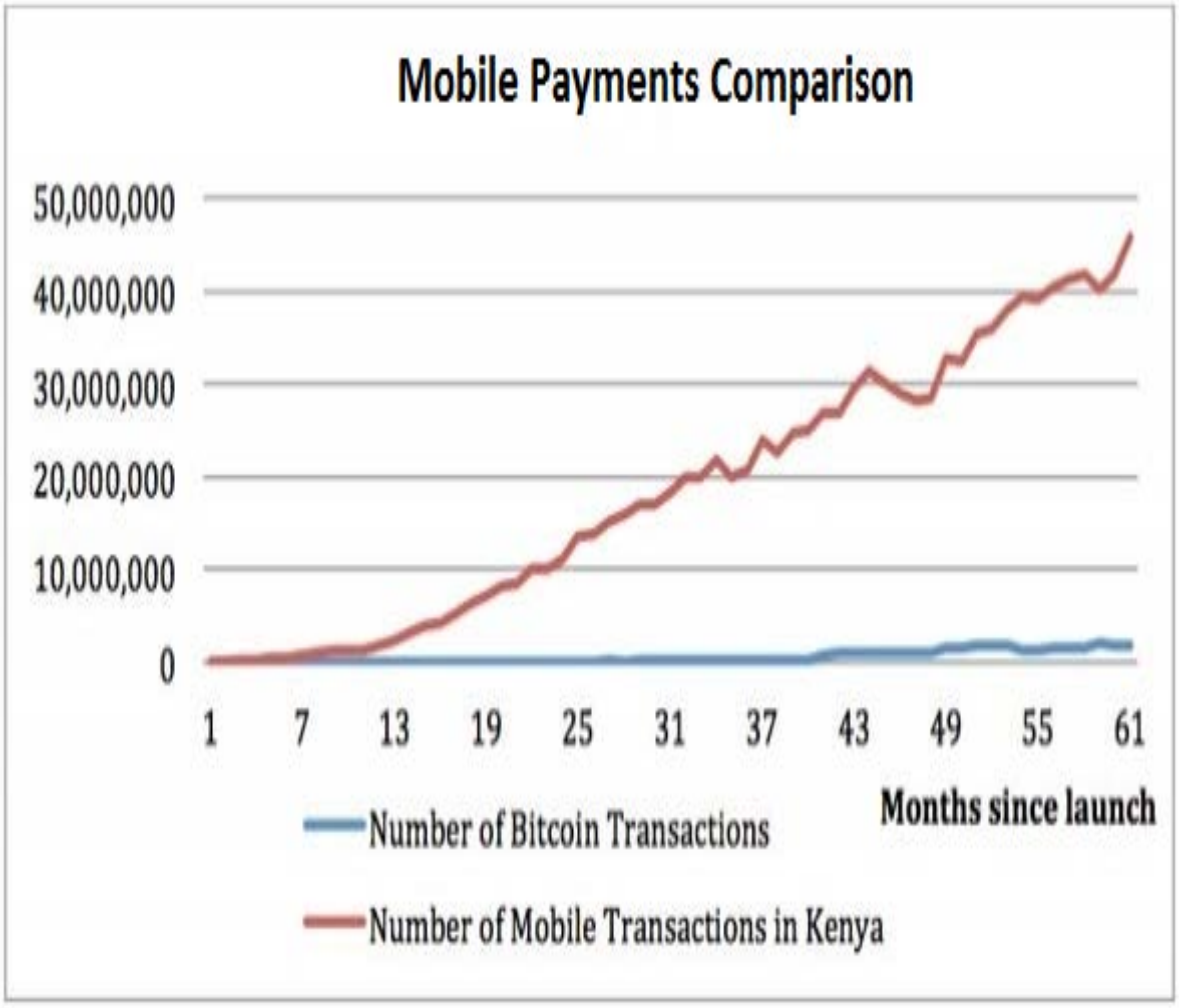
These solutions, which would work (increasing the block size) but in order to do so would require more processing power, bandwidth and disk space. Which requires more than a laptop, more than a USB ASIC. It requires professionally managed datacenters, which leads to centralization, thus in order to compete with a real time gross settlement system (RTGS), such as Visa, you probably have to build a Visa-like facility.[56][57]

It should also be noted that the majority of the network does not currently process at the maximum speed. While there is no minimum, the maximum default block size was increased

from 300,000 to 350,000 in the 0.8.6 release to see which pools simply utilized the default settings or if pool operators manually recoded to include block sizes of 1 MB (roughly 3.3 transactions per second).[58] In practice, the majority of blocks propagated are less than 250 KB.[59] And while still young, for comparison, on Bitcoin Black Friday in 2013, the busiest e-commerce day for Bitcoin, the network processed at a peak 1.5 transactions per second.

M-PESA

The most successful mobile payment system currently is M-PESA, operated by Safaricom and Vodacom and serving 30 million users in East Africa (Kenya and Tanzania), the Middle East and India.[60] It is a mobile-phone based money transfer and microfinancing platform; last summer, Kipochi integrated a lightweight Bitcoin wallet with M-PESA which enables Kenyans to bypass costly remittance fees charged by middlemen such as MoneyGram and Western Union.[61] While some may ignore the possibilities of mobile banking, preferring desktops or even physical visits to bank branches, 43% of Kenya's GDP is spent through mobile phones.[62] In fact, according to a recent *Reuters* report, "M-Pesa has enabled 67 percent of Kenyan adults to access banking. Its transactions total about $1 billion per month."[63][64] There are roughly 253 million unique mobile phone subscribers in Africa (many have two SIM cards) and an estimated 70% of the population on the continent are underbanked or have no access to a bank.[65] Therefore cryptocurrencies and trustless asset management tools built on cryptoledgers that interface with mobile phones will enable and empower an entirely new demographic and consumer base to emerge from subsistence. In fact, according to a 2009 report from Financial Access Initiative, half of the world is unbanked which leads to new opportunities for entrepreneurs.[66]



The above line graph was designed by David Evans, a law professor at the University of Chicago, who recently published a payment platform comparison between M-PESA (in red) and Bitcoin (in blue).[67]

As Evans points out in his article, M-PESA was first introduced in Kenya in mid-2007 whereas Bitcoin was launched in January 2009. Yet as I mentioned above in chapter 6, M-PESA is so widely used in Kenya that roughly 43% of its annual GDP is handled through this mobile payment system, the same obviously has not occurred with Bitcoin yet (perhaps it could with other systems such as NXT or Ripple).[68][69]

It should be noted that the direct comparison is not entirely apples-to-apples either as the Bitcoin transactions in this chart only include on-chain transactions.[70] Coinbase and Circle use off-chain wallets which permit users to buy, sell and trade bitcoins (including micropayments) instantly that would otherwise take tens of minutes to confirm via an on-block chain implementation. An off-blockchain solution also allows users to trade below the dust limit (roughly 5460 satoshis) which is an artificial limit implemented by the developers several years ago to prevent spam from propagating the network (e.g., a malicious user could send out

millions of 1 satoshi, each of which needs to be added to a block, thus taking up time and resources).[71] BTC-e takes this off-chain approach a step further by allowing users to build bots that interact with its API, enabling high-frequency trading. None of this is possible on-chain and thus these types of transactions are not represented in the image above.

But Evans is right to bring this criticism up and it is an issue that has motivated other developers to build several 'next generation' platforms. For example, as noted above regarding the difference between Bitcoin and Visa, other platforms such as Ripple have a purposefully more robust payments system, in the case of Ripple its current setup, while security conscious, can handle 100 transactions per second but it is designed to handle at least 1,000 transactions per second as well.

Again, this may not be an issue in developed countries, where users have easy-access to Bitcoin wallets (both web and mobile based). And because of the relatively large fees, cross-border remittances has purportedly been one of the 'killer' apps for Bitcoin and will remain so into the future.[72] In fact, despite the fact that it takes 10 minutes for one confirmation, it is still quicker than other existing remittance processes such as ACH which can take three days to clear.[73]

But as an RTGS, where transactions clear near instantaneously, it cannot compete at the same level as credit cards or M-PESA.[74] This is an issue that potential entrepreneurs should keep in mind. In fact, while there are certain days that $50-$100 million worth of bitcoins are processed along the network that is about as much as MasterCard and Visa process in a few minutes.[75] For comparison, in 2013, MasterCard and Visa processed a combined $7.4 trillion in purchases. Together with American Express and Discover, these four companies generated $61.3 billion in revenue during the same period. While credit card companies like Visa can make the verification of payments even offline (they download the blacklist on terminals) and M-PESA is quick and easy via SMS, the slower confirmations are a challenge for Bitcoin as it makes its way into the mobile payments space.

Yet while users in developing countries have more incentives but are limited due to few smartphones, unreliable internet connection and reliance on shared devices. There are roughly 253 million unique mobile phone subscribers in Africa (many have two SIM cards) and an estimated 70% of the population on the continent are underbanked or have no access to a bank thus one competitive advantage cryptocurrencies such as Bitcoin do have is the global reach is numerically larger than Visa (which is discussed later).

None of the benefits of centralization yet with all of the costly overhead of decentralization

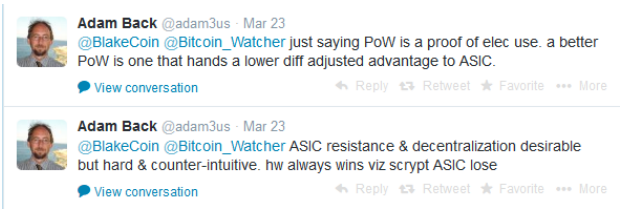
While there are advantages to using decentralized systems, in any non-centralized system constraints exist and are described in the CAP theorem, which is to say that no distributed system can simultaneously guarantee:

- Consistency (all nodes see the same data at the same time)

- Availability (a guarantee that every request receives a response about whether it was successful or failed)
- Partition tolerance (the system continues to operate despite arbitrary message loss or failure of part of the system)[76]

The Bitcoin network is not immune to these resource constraints either.

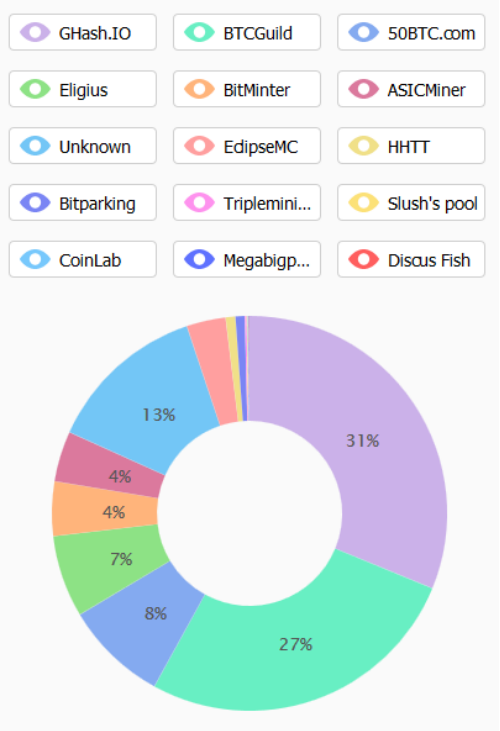
As the years have passed, the deadweight loss of (over)securing the network via a perpetual proof-of-work arms race has moved from the original CPU mining method described in the 2008 whitepaper. That is to say, as the system was original envisioned, each CPU core was considered one vote on the network – a type of virtual democratization that intersected with the physical world. However, by late 2010, users had figured out how to take advantage of the parallelization computational horsepower of their GPUs, to increase the hashrate of the mining algorithm (SHA256d), and therefore increase their chances at finding a block and thus being rewarded with block rewards. While there was a purported "gentleman's agreement" by early adopters to refrain from using this, this amounted to an illustration of game theory, a type of prisoner's dilemma in which users (or miners) are better off not cooperating but by seeking the most powerful equipment to not process transactions but to increase their statistical odds of finding a block.[77]



Consequently, as multiple CPU cores were sidelined by GPUs, GPUs were likewise sidelined by FPGAs, which while relatively similar in terms of hashrate, were several times more efficient in terms of electrical consumption. That is to say, while it is still possible to mine (or hash) with CPUs or GPUs, due to how the protocol difficulty rating scales linearly with hashrate, unless the tokens appreciate, most users of non-FPGAs were spending more on electricity than they were generating from block rewards (i.e., unprofitable mining). All three of these options were later nullified as competitive, profitable options with the release of ASICs – computers specifically designed to do one sole task: hash SHA256d. These ASIC systems similarly have led to several orders in magnitude for both performance and in terms of electrical consumption (i.e., the most efficient hashes per watt).

In fact, during March 22 – 23, 2014, Adam Back the creator of Hashcash which is the proof-of-work anti-spam hashing system used in Bitcoin, posted several comments (above) on Twitter related to the issue of ASIC performance, noting this inexorable drive towards efficiency.[78]

Yet this make-work arms race has unintentionally led to the centralization of the mining network. In 2009, while early adopters used computers such as laptops that were capable of mining blocks by themselves (retroactively called "solo mining") as the CPU race first from multiple cores and then with botnets began to form, collective mining pools formed in which users would pool their resources together. While the odds of one person with a simple laptop of finding a block were low, pooled with others, the odds of success were much higher (just like lottery pools). Pool operators have multiple ways of rewarding participants, typically the most common technique is just a pay per share or pay per performance (i.e., the more valid hashed shares your system sends to the pool, the higher your share of block rewards are).[79] In return for running the pool, mining pool operators extract a 1%-5% fee which is used for maintenance (e.g., protection against DDOS). Eventually these became professionalized and run by teams of IT administrators. The first mining pool, Bitcoin Pooled Mining (operated by "slush"), began public operations on November 27, 2010.[8081] Within two months its collective hashrate hit 10,000 megahashes per second.[82] For comparison, an Intel quadcore desktop CPU performs at 10 megahashes per second.[83] As of this writing the collective Bitcoin network hashrate is approximately 45 petahashes per second, virtually all of which is comprised of ASIC hashing systems.



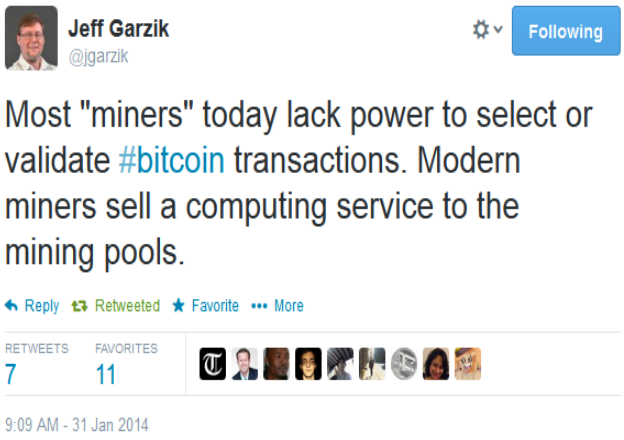
Mining Pools as of March 25, 2014

While the size, composition and pool operators have changed over the past 5 years, the current composition and distribution of hashrate looks like the following diagram to the right which some have likened to a Red Queen's race (i.e., everyone is running faster, or hashing faster, yet staying in the same place).[84]

Bitcoin core developer Jeff Garzik has pointed out the ironic nature of this phenomenon on several occasions. Recently he noted:[85]

If the intended goal of a cryptocurrency such as Bitcoin was to move away from centralization, the opposite has occurred and in fact, just as the US is divided into 12 Federal Reserve districts, perhaps in the future there may only be a dozen ASIC datacenters capable of providing competitive hashrate (as illustrated).[86] Since anonymity and decentralization will be removed, these known facilities and professionals may then also become susceptible to the same vulnerabilities and abuse that traditional systems have been.

Earlier this year he made a similar observation, making the statement in the image below.



Today, mining Bitcoin *profitably* currently requires a significant capital investment in single-use ASIC hardware. While a user could use a cloud-based hashing service such as Ghash.io or ASICMiner, as noted by Garzik, most mining systems currently lack power to select or validate bitcoin transactions themselves; you are merely selling a computing service (hashing) to the mining pools.[87][88] Another lower-cost option that some hobbyists have utilized is purchasing a small USB ASIC miner (e.g., Bi•Fury); however, the problem is that you would need to rely on whatever token amount you generate to appreciate in value in order to pay for the electricity you expend in mining (i.e., if you generate 0.1 BTC that is worth $80 but it cost you $85 in electricity to generate, then you would need to wait for the bitcoin to appreciate; otherwise you are at a net loss).[89] Large miners face similar issues, hence the periodic downtimes of ASIC servers (i.e., mining only when it is profitable to do so).

One solution to the deadweight loss issue is through further use of merged mining such as Namecoin. That is to say, while Namecoin was created in 2010 as a modified version of Bitcoin, in 2011 the mining of namecoins (after block 19,200) was effectively merged with Bitcoin through a software update (e.g., pools had to use a new software release). By using a similar

process with altcoins that use incorporate new features (like longer namespaces for metadata and characters) this could provide further incentives for ASIC miners to continue mining even after block rewards for Bitcoin are reduced in the future. While details are sparse, merged mining and sidechains is integral to a new project that is currently being developed by the team noted above led by Adam Back and Austin Hill.[90]

In addition, one of the known limitations in ASIC datacenters are Ethernet and outside internet connectivity. Optimizing not only the hardware but software to enable maximum block throughput is necessary for profitably mining. Taken to the next level, in November 2013, an opt-in high-speed Bitcoin Relay Network was setup to allow mining pools to peer with one another, allowing them to propagate and broadcast blocks in the fastest manner possible in the event that the public Bitcoin network encountered issues.[91] While private peering agreements between pools have existed over the years due to these increasingly non-marginal efficiencies made possible via faster propagation, pursuing these goals – professional mining facilities with network peering – will likely remove anonymity and potentially lead towards further centralization.[92][93]

The importance of reducing propagation delays was also highlighted by Sompolinksy and Zohar:[94]

> Attempting to increase either the block creation rate of the block size may increase the throughput, but both options also adversely affect the protocol to some extent, a fact that has been noted by Decker and Wattenhofer as well.[95] Since the process of block creation is effectively random, it is possible for two blocks to be created simultaneously in the network by two different nodes, each one as a possible addition to the same sub-chain. These two blocks can be consistent with the history, but are mutually conflicting. The Bitcoin protocol ensures that eventually only one of the generated blocks will be accepted by the network. Discarding a block amounts to wasting effort, and this waste is only avoided if blocks are propagated quickly enough through the network so that additional blocks are built on top of them. Any increase in the block size implies that blocks take longer to propagate through the network, and thus many wasted blocks will be built in parallel. In a similar manner, increasing the rate of block creation implies blocks are created more often, and frequently before previous blocks have propagated through the network.

Homo economicus

In many economic theories, humans are assumed to be rational, self-interested actors, continuously pursuing ways to maximize their utility and profit from their resources. Because of the hashrate arms race, ASICs are a depreciating capital good. That is to say, there is a short time frame, a narrow window in which their capital good can provide profitable hashrate before their hashrate is negated and marginalized by ever more powerful systems. In any market, prices serve as signals to competitors. The higher the profit margins, the more likely

competitors will join a market thus reducing the margins, or in this case, the seigniorage spread. While some miners may keep the tokens they generate and spend fiat out of pocket to operate the facilities, many operators sell their tokens for fiat.

Consequently, once the window of hashrate opportunity closes, once the difficulty rate of the algorithms and the network crosses the threshold into an operating loss, miners will turn off their machines. Or, in many cases, because their ASICs are one-use and lacks utility beyond the hashing subindustry, this provides incentive to create altcoins to mine. In fact, because the resale value of the equipment diminishes over time as well (for the same hashrate competitiveness) owners either must offload the equipment quickly or turn to a profitable alt (or create an alt). While there are hundreds of altcoins at the time of this writing, most of them are almost identical copies of the Bitcoin code, repackaged with different marketing (e.g., BBQcoin).

Mining pools also have incentives to do two other activities: 1) create a distributed denial of service (DDOS) against competitors and 2) "selfish mine."[96] DDOS attacks against competitors are frequent and are increasingly made easier by the centralized nature of mining pools. That is to say, aside from P2Pool, all the largest mining pools have a known series of central servers with IP addresses. A malicious agent can send spam traffic to prevent those servers from communicating with pool hashers, thereby preventing that pool from effectively mining. If that takes place, then other mining pools benefit as it increase their odds of finding block and therefore block rewards. While protecting against a DDOS is a constant cat-and-mouse game, it is not relegated to mining pools as token-fiat exchanges such as BTC-e, Huobi and the late Mt. Gox also were under relatively continuous attacks.[97] These attacks are done with the motivation of psychological warfare, that is to say, if a large exchange goes offline, it has the effect of "spooking" the market and participants globally may sell their tokens, momentarily depressing the price. These hackers will use this time to purchase the tokens and then terminate the DDOS, allowing the exchange to come back online, which in turn restores consumer confidence and thereby typically raising the price of the tokens. One other method that has been done in the past with frequency is the following: Bob the attacker will deposit Bitcoins or fiat onto an exchange. They will sell bitcoins and immediately after DDOS the network. As the network is attacked, confidence in the exchange falters and users sell their tokens, pushing the price levels down. At some defined point, Bob stops the DDOS and then immediately purchases tokens at the lower price. Or in other words, incentivized market manipulation.[98]

While these types of attacks were unforeseen in 2008 and 2009, by 2012 it was possible for pool operators to utilize their vast hashing power to also disrupt other alts. For example, in January 2012, Luke-Jr., the owner and operator of Eligius, a mining pool, publicly noted that he unilaterally utilized the mining pools resources to conduct a 51% attack against the alt Coiledcoin (attempting to 'merge mine') which had been released.[99] Security for proof-of-work-based tokens is contingent on more than half of the nodes being honest, that is to say, if

any individual, organization or entity is capable of collectively hashing more than 50% of the network hashrate, they can continuously double-spend ledger entries and deny the rest of the network transactions from being processed – thus effectively killing the network. Yet it should be noted that individuals have their own time preferences, so it may be difficult to generalize the motivation for each mining pool operator.

Selfish mining

Another problem that has arisen over the past 5 years is a form of "cheating" called selfish mining that is probably best described by Vitalik Buterin.[100] In short, the more hashrate Bob controls, the higher the chance your system(s) have at finding a block before other competitors do. That is to say, even if Bob has less than 50%, but more than 25% of the network, it is in Bob's economic interest as a pool operator to pursue the following scenario:

> A hasher in the pool finds a block (x), but you do not announce it to the rest of the network, instead your hashers continue mining till they find another block (y) and you still do not release it until someone in your pool find block (z) and then you announce the discovery of them near simultaneously to the rest of the network. While risky, what happens is that this effectively negates all other hashers and miners who are still working on the first block. Several of the largest pools are suspected of frequently doing this, frequently yet it is in the self-interest of the pools to maximize their assets and hashrate.

Microtransactions

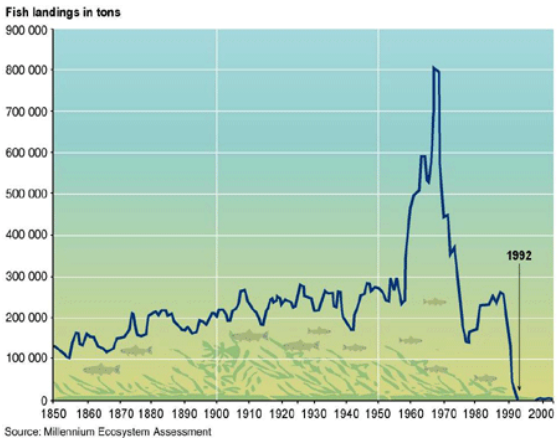
While unstated in the original whitepaper, one of the secondary goals of creating this decentralized payment system was to effectively enable microtransactions, a feat that is considered nearly impossible in current system due to transaction costs (e.g., minimum fees) which price out certain market participants.[101] That is to say, while the money supply of this system effectively creates 21 million bitcoins, these tokens are divisible to the 10 millionth decimal place (0.00000001). This final digit space is called a satoshi. While it is possible on paper to do this, in practice what happened is that several users began to fill the network with "spam," creating tens of thousands of 1 satoshi transactions and causing a type of denial of service on the network. As a consequence two solutions were created. The first is a threshold referred to as the "dust limit" was encoded by which a minimum amount of bitcoin was required to be used in order for a transaction to be processed, this limit is currently set at 5460 satoshis. The other solution was to enact a transaction fee per transaction. Thus the Bitcoin network does charge a small nominal fee for some transactions, although most are processed without any fee. A transaction drawing bitcoins from multiple addresses and larger than 1,000 bytes may be assessed 0.0002 bitcoin as a fee.[102] When it was instituted, it was initially thought that the higher a fee a user includes, the more incentive the miners have to include the transaction in a block to propagate it to the rest of the network.

Gavin Andresen is currently the lead Bitcoin core developer and he set a fixed fee amount which due to the fiat price appreciation actually now costs significantly higher than it was intended.[103][104] In his own words:[105]

> [–] **gavinandresen** 18 points 3 months ago
>
> Payments of less than 5-thousand-something satoshis are still considered dust, so this does NOT open up the market for micro-transactions.
>
> Plain-old transactions might never be affordable for transactions worth less than a cup of coffee, and in the next year or two you should expect low-value transactions to get forced off the blockchain because transaction fees are likely to rise.
>
> I have no idea what will happen in the long run; there might be micro-transaction systems that use Bitcoin as the "settlement currency", or technology and innovation might make transmitted-all-across-the-world Bitcoin transactions inexpensive enough for micro-transactions. We'll see!

Developers are aware of this issue and consequently plan to allow fees to float, that is to say, miners will be able to charge based on supply and demand, what the market will bear for inclusion in the block (a scarce resource).[106] And as block rewards halve each year, miners will likely charge higher transaction fees to make up for the loss of income originally provided via seigniorage.[107]

Thus this specific issue again, illustrates the difference between a theoretical public good and how it is treated in practice. The purported abuse of it via spamming and the arbitrary threshold limit setup thereafter is reflected in the collapse of the Atlantic cod stocks off the East Coast of Newfoundland in 1992 or in other environmental collapses in the former Soviet Union in which rivalrous goods (scarce resources such as land) were treated as unlimited by the public at large and thus resource cannibalization and pollution took place.[108]



Financial incentives for developers

Despite the fact that the code is open-sourced and has been available for five years, notwithstanding members of the intelligence community, there are likely only a few hundred civilian software engineers in the world capable of independently building or reconstructing a decentralized cryptographic ledger similar to Bitcoin.[109] This is because the underlying systems are difficult to not only conceptualize but also code in a cogent manner. As such, those capable of creating and shipping productive code in this space have an incentive to charge market prices for their scarce labor.

Because of how the Bitcoin protocol exists, without a monolithic corporate or organizational sponsor, with the responsibility to reward code contributions, there is no financial incentive to be a core developer. That is to say, because there is no financial reward for contributing code

on a regular basis as one might do at a job, those capable of building onto and improving the feature set of Bitcoin have an incentive to work on other projects. Historically there is more money to be gained (and in less time) building and speculating on an alt coin or alt platform.

Currently there are only ~3.1 people who are funded and specifically paid by their organization to work solely on the Bitcoin protocol: Gavin Andresen and Wladimir van der Laan whom are both funded by the Bitcoin Foundation, Jeff Garzik at BitPay and 10% of Mike Hearn (just the hands and mind) who spent a portion of his time at Google working on Bitcoin-related efforts.[110] Hearn has actually voiced his concerns regarding this phenomenon – the dearth of funding despite the hundreds of millions of dollars in value being extracted by portions of the ecosystem.[111] This is best labeled as the "tragedy of the crypto commons." That is to say, while visible growth has traditionally come from the volunteer work of dedicated engineers and hobbyists, there is a free-rider issue due to how the protocol actually is developed (e.g., outside firms who utilize the code but do not contribute back).[112][113] One interim solution to this is bounties, assurance contracts, and dominant assurance contracts that can help fund fixes and travel budgets (so the volunteer developers can attend workshops in other countries) or even as milestone-based contractors.[114][115]

Two markets and non-sustainability

When economists analyze for public goods problems, they first try to eliminate the individual incentives. And because this segment is still relatively young, individual incentives are still being discovered. Provided that they cannot be discovered, below are several public goods problems that currently exist.

Despite the fact that the Bitcoin protocol intersects with both game theory and public goods issues, there is very little academic literature on this topic – in fact, almost none that is currently published in an English-language academic journal.[116]

One expert who has begun discussing these issues however is Jonathan Levin, a post-graduate student at Oxford and co-founder of Coinometrics.[117] In his view:

> There are two markets and it is not likely that we will get an equilibrium in the private goods market which does not lead to welfare loss in the public goods market. Hashrate is a public good, it is non-scarce and non-rivalrous that everyone benefits from. No one is excluded from trading – it cannot exclude. In addition there is a private goods game, the inclusion of transactions. Because their limited block size, only so much data can be included. This transaction cost is masked through seigniorage, through block rewards. Current transactions costs are not borne on users all of whom free ride. The private good has to fund the public good, it has to create a revenue stream of paying tax fee to be included in a block. Thus there are two markets, which is not currently efficient as the actual transaction cost. The private good market game has to provide adequate incentives for miners to provide the optimal amount of hashing power.[118]

Levin raises several pertinent issues facing any public good. In Bitcoin's case, participants in the network (Bitcoin users) essentially treat it as if it is non-scarce, but it fundamentally is not due to the limited resource (block size). One reflection of its scarce nature is that people do pay for it in the form of the inflation tax (if it were truly scarce one would expect it to be free, like air). The problem is that the vast majority of the costs of a transaction are not paid by the person doing the transaction but spread across onto all holders of bitcoin in the form of share dilution (e.g., schedule inflation). In addition, another way of looking at its scarce nature is in comparison to alt coins: for many alt coins the network simply does not reward those who secure it well enough so that the supply of computing power is insufficient to meet demand. This recently was a problem that faced Auroracoin, which underwent a 51% attack on the weekend of March 29, 2014.[119] That is not currently the case with Bitcoin, but that could change.

Thus the incentive to provide this public good (hashing), via a private method (seigniorage via the coinbase), lessens with block reward halving. Yet as noted by Levin, access to the hashrate via the network is treated as a public good as defined in the beginning (non-scarce and non-rivalrous). However, the inclusion of the transaction is necessarily a private good due to the block size scarcity (1 MB) whose provision was originally incentivized via seigniorage but will later turn towards transaction fees.[120] And as noted in the previous section, the current transaction fees do not cover the costs of maintaining the network, thus they will eventually be floated and determined by miners. And consequently, there is a continual trade-off between block size (which can also be increased but with the requirement of increased mining centralization), network propagation speed, infrastructure centralization and resource costs.

The actual network costs are likely higher, certainly not free and are masked by price appreciation and token dilution. Yet arguably, once block rewards continue to diminish over the coming 6 years (reaching 6.25 BTC in approximately the year 2020), and transaction fees raise to market levels, there is a possibility that the costs of a transaction will equal to or cost more than a credit card transaction in some countries. Simultaneously, the on-chain network will be decentralized, yet the entire infrastructure on the edges, those with on-ramping utility such as Coinbase, BitPay and Circle will be centralized – yet the on-chain network will not benefit from such centralization with faster confirmation times for reasons described in the next section.

Reducing and removing block rewards

Nicolas Houy recently published a paper that looked at this transaction fee and mining issue in terms of a Nash equilibrium.[121]

According to Houy's calculations, the transaction fees amount to only 0.4% of the miner rewards, block rewards represent the other 99.6%. While the transaction fees are probably more than 0.4% of the mining rewards (by an order of magnitude) because miners have more of an incentive to strictly hash for nonce values, the shorter the block size they can propagate

to peers, the better, because it allows their mining network and resources to instead focus on block rewards which offer much higher return-on-investment.[122][123][124] Or in other words, the larger the transaction block size, the more time is needed to broadcast it which incentivizes propagating the shortest block sizes possible.[125] Thus, because there is currently little incentive to actually process transactions, all miners would be better off individually if they did not process any. Yet if this was done the network would lose its utility as a payments platform and demand for bitcoins would likely decrease creating a drop in price levels and cutting into their break-even point.

Or in other words, miners are currently providing a public good in a charitable manner because of the overall utility it creates for the network which in some ways is similar to the incentives for not conducting a 51% attack on your own cryptoledger network (i.e., self-defeating, destroying your investment). All things being equal, according to Houy's calculations, if you were to remove block rewards, to compensate the transaction fee would need to be at least 12 times larger (0.0012 BTC or roughly $0.76 at current market prices). This empirical data set is known and has made some observers, including Gavin Anderesen in the past, to hypothesize as to why miners include transactions at all, is it merely out of altruism?[126] For comparison, the average network and processing expense per Visa transaction ($414 million / 77.6 billion transactions) is $0.0053.[127]

Robert Sams, a former hedge fund manager and founder of Kryptonomics has written on this issue, an issue he dubs a tragedy of the *transaction verification* commons.[128] In his analysis, miners do have an incentive to include transactions because of the fees, and while block size is a factor in terms of network propagation, it is not clear whether the costs of large blocks is purely a private cost to the miner with the big block or a cost borne by the network as a whole in terms of more orphan blocks.[129] The issue, as Vitalik Buterin and Sams have discussed, is that Bob, the miner, collects the fees on the transaction of Bob's (winning) block, but the costs of processing those transaction is incurred by the entire network, as every node must verify every transaction (tx). So in Sams' model it is a private and social cost problem. Thus according to him, there needs to be an internal mechanism to calculate the "optimal" fee in a Piquovian sense:

> The essence of the problem is this. In Bitcoin, tx fees are effectively set by what tx miners choose to include in their blocks. The creator of a tx can pay any fee he chooses, but miners are free to ignore a tx, so a payer who pays a relatively large fee is more likely to have a faster-than-average confirmation time. On the surface, this looks like a market mechanism. But it isn't. The miner gets the tx fees of every tx included in a block that the miner solves. But every node on the network pays the costs of verifying a transaction; tx must be verified before relaying and building on top of a solved block. Therefore, a miner will include any tx with a fee in excess of his computational costs of verifying it (and reassembling the Merkel tree of his block), not the network's computational costs of verifying it.

> A single, very large block containing many transactions with many inputs/outputs can bog down the network. To deal with this, the Bitcoin protocol imposes a 1MB upper limit on the size of a block. This isn't a great solution. Not only does it put an upper limit on the number of tx Bitcoin can process per unit of time, it does nothing to rationalise tx fees to tx verification costs.

While both Sams and Buterin have a potential solution to this, via a Pigou tax, it is likely the case that at least one party (miners who include few if any transactions) is free-riding off the value-chain provided by those who do provide such utility.[130][131] Whether this is sustainable in the long-run or whether or not free-floating fees will fix it entirely is the topic for other papers in the coming years.[132]

This is not to say that others looking at this issue come to the same conclusions. While, Kroll *et. al.,* surmised that under the current rules, transaction fees will not play a long-term role in the economics of the network, they do think that these rules will likely be changed:[133]

> The only way to preserve the system's health will be to change the rules, most likely either by maintaining mining rewards at a level higher than originally envisioned, or making transaction fees mandatory. Different groups benefit from each solution (for example, raising the mining reward modifies the money supply, which is anathema to much of the Bitcoin community, but mandatory transaction fees can be seen as slowing adoption of the technology by merchants).

As noted throughout this paper, the core developers plan to float the fees at some point in the future, to offset the diminishing block rewards. This would then be a fulfillment of the prediction by Kroll *et. al.*

Mike Hearn, a Bitcoin core developer, recently noted that developers have observed similar behavior based on the motivations described in this section:[134]

> What we have seen is keeping the network decentralized has been very hard. Mining is obviously very centralized which is not really healthy. And it's been very difficult to try and fight that trend. A lot of miners they don't seem to really care about decentralization, they only after the financial rewards. So that is a challenge. And one thing we see as a result of that is some very large mining pools that don't include very many transactions in their blocks so they're actually reducing the overall capacity of the network by doing that. And they're doing this usually we think to try and increase their earnings very slightly because the core system is not scaling well enough for that.

Yet there may be at least four reasons why large mining pools such as GHash.io continually broadcasts large block sizes: [135]

> 1) They do not want to have more than 40% of hashrate because it leads to public backlash as seen in mid-January 2014 – they issued a press release on January 9th to assuage fears.[136]

2) GHash.io does not merely hash and broadcast nonce-only blocks for similar public relations issues as well (i.e., the headlines accusing and shaming them of "free-riding" would be poor public relations).

3) By adding to the utility of the network by including transactions, their cache of bitcoins could appreciate in value.

4) If GHash.io rejected blocks (irrespective as to whether or not the blocks included any transactions) they would also have to worry about public perception. Failure to include transactions which remain in memory pools for some time could impact the performance and utility of the network.

Thus it may be too broad to paint each miner with having the same motives or incentives. There might not be a generalized econometric model as individuals have their own time preferences with respect to pursuing mining.[137][138] Public shaming may motivate some and not others. Price appreciation likewise. Therefore it may be premature to include the commons when not all private costs (and benefits) have been accounted for.

Furthermore, in its first year of operation, virtually all of the blocks generated on the Bitcoin network were essentially empty because very few users existed at the time. Upon seeing that this system could lead to free-riders, why not create a minimum block size going forward? While it would be trivial to change the code to do this, it would likely have a number of unintended consequences. For example, if 200 KB became the minimum block size, that would price out any miner incapable of generating profitable hashrate at that expected boundary which could lead to fewer participants and more centralization.

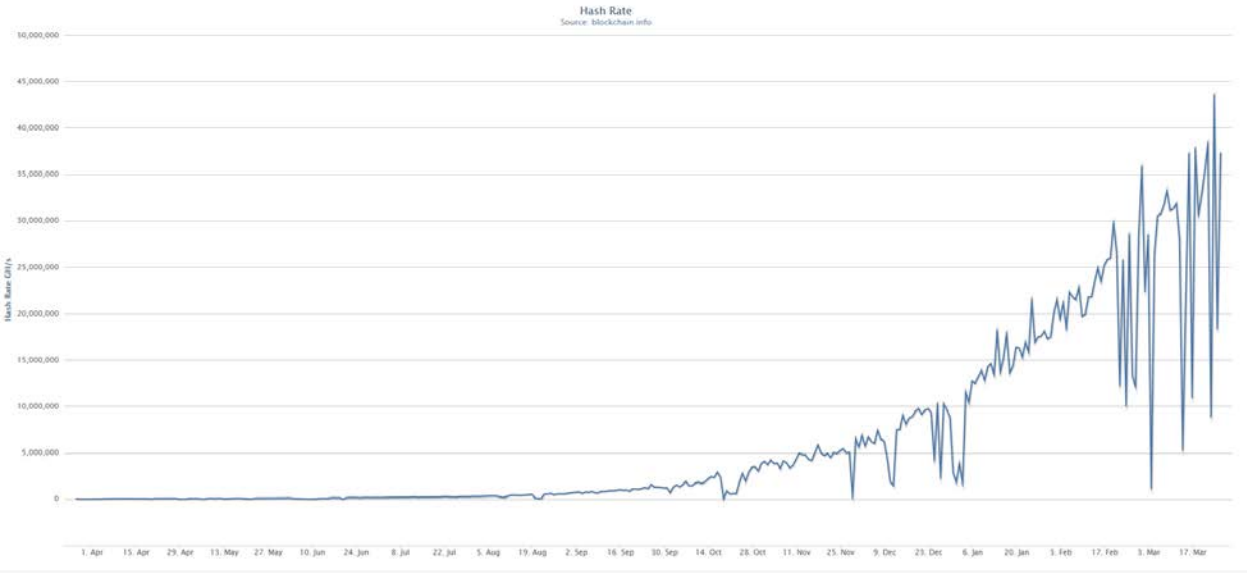
Securing information

Since the genesis block 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 is likely the more accurate figure as there are numerous undisclosed hardware purchases by private parties including enterprises and investors in this space.[139]

As noted above, a proof-of-work based system is a continuous arms race with numerous financial incentives to out-hash your competitors for block rewards (and not necessarily transaction fees as some of those are left in memory pools). In addition, these funds went to semiconductor designers, not software developers or the actual ecosystem itself. In fact, a significant cost that is difficult to estimate is the electrical fees needed to sustain this money supply network, nearly all of which went to electricity oligopolies and none of which went back into creating additional utility on the Bitcoin network.

While it is possible for a core developer to create a hardfork that includes a different security system, such as proof-of-stake (POS) which requires virtually no hardware infrastructure yet is arguably just as secure, a type of "regulatory capture" exists as miners have a financial

incentive not to switch to a fork that does not repay their capital investment thus the *status quo* will remain. Yet despite these investments, the network operates at roughly the same performance as it did five years ago, with 10 minute confirmation times. This is intentionally hard coded but as noted above, to increase the size would effectively lead to a variety of consequences (such as centralizeation). And while speculative, if a payment processing company such as Visa spent between $200 million and $1 billion on hardware and yet their overall network performance had not improved, the CTO would arguably be under pressure to resign.[140] However there is no such accountability in Bitcoin because it is a public good. There may still be attempted solutions however, as Adam Back and Austin Hill have proposed a method for capitalizing off this underutilized capacity via merged mining with sidechains in an upcoming venture involving several other core developers.[141]



Above is an image from Blockchain.info which illustrates the total hashrate of the Bitcoin network between two dates:[142]

- April 1, 2013: 51,925 GH/s
- March 25, 2014: 37,582,751 GH/s

This is a 723x increase in hashrate, yet roughly with the same network performance. The dips and hashrate volatility: this is evidence of miners acting rationally with incentives and switching off to lower difficulty next period or temporarily pointing their miners towards a more profitable altcoin. This can be problematic, as Kroll *et. al.* noted, "miners are amortizing sunk costs related to capital expenditure for equipment" and miners may, "therefore overinvest in mining to offset their fixed costs, investing up to their marginal costs per unit time."[143] Thus anytime they are not profitably hashing *something* is an additional delay towards the repayment of loans or outside investments which paid for the fixed capital. Such drops also create security risks for the overall network as rogue mining pools could take advantage of the sudden drop to attempt a relatively cheaper 51% attack.[144]

This income stream issue is an ongoing concern in the mining industry as bitcoin price levels peaked at over $1000 in November and early December 2013, bringing in a large number of new entrants and consolidating existing independent miners into more professionalized entities looking to scale operations. Yet volatility has impacted the strategic planning of many mining operations. For instance, during the spring of 2014, several ecosystem events including the bankruptcy of Mt. Gox, a large online exchange and new regulations enacted by the People's Bank of China, reduced confidence and fiat liquidity into and out of the bitcoin exchange system. As a consequence, price levels since there peak in November, have declined to below $500 at the time of this writing.[145] This in turn has squeezed out marginal mining pools, who are unable to operate in a cost effective manner due to having invested into capital stock based on expected bitcoin price levels that have since deteriorated. As a consequence, some miners have sold their equipment and others have turned their equipment to hash other, more profitable alts. As Colin Lusk, an early bitcoin miner and adopter explained to *Bloomberg*:[146]

> While he once mined only bitcoins, Lusk now uses five of his eight machines to produce Litecoins and other virtual currencies. Created in 2011, Litecoin is similar in design to bitcoin yet requires less computing power. A $3,500 computer can produce $25 worth of Litecoins a day for $3 in electricity, while producing $20 worth of bitcoins would cost $17, Lusk said.

These prices will likely continue to fluctuate due to the underlying variables (e.g., electrical costs, hardware costs, management costs, real-estate costs, market supply and demand for bitcoin and other alts).

Is Bitcoin a private company?

One argument that has surfaced over the past year is that Bitcoin is itself the first type of decentralized autonomous organization (DAO), that all of the users technically must submit a digital key which counts as some kind of voting mechanism, shareholders (miners) receive direct compensation for their work (seigniorage) – and there is no administrative overhead per se.[147][148] Yet, since development and direction of the Bitcoin protocol itself is not handled by direct "votes" it is not technically a company.[149][150]

But voting and separate personality does not a company make. Just like the cargo cult on Vanuatu in the South Pacific dressed up and marched like soldiers even going as far as reconstructing non-flying airplane models, with the belief that Western air cargo planes would return with wartime goods, implementing "voting" into a cryptoprotocol and assuming this will create a company is a fairly superficial understanding of a corporation.[151] Because of how some aspects of development has come under the purview of the Bitcoin Foundation, the current Bitcoin ecosystem is a blend between "shareholder" and "stakeholder"

system.[152] This has potentially destabilizing issues in the long-term: fiduciary responsibility boundaries are fuzzy due in part to how it is funded (sponsorships) and how the organization wants to be perceived from the outside. Furthermore, like any initiative there is the possibility that the network could be abandoned by users; a company cannot function without shareholder input. This is not to say that there should not be a foundation (or many foundations) or even that a foundation could not receive money from outside sources or that users will abandon the project and network – rather, that because there is no direct voting process by bitcoin holders (like in a real corporation), the decision making process of the actual direction of the protocol itself is not an example of a DAO or a traditional company.

Because there are no clear decision makers, no clear responsibilities or duties, no governance or accountability determined by private keys, a change in the protocol, such as adding a feature for the inclusion of smart contracts, ends up becoming a lobbying effort by competing special interest groups, each vying for *cui bono*.[153]

Bitcoin as a public good

Since the Bitcoin protocol is not privately owned by any institution, individual or organization, does that mean it is a public good?

As described by Jonathan Levin in the above section, there are two markets – private seigniorage (and transaction fees) that provide a public service, the hashrate. Currently block rewards subsidizes this public service as transaction fees do not cover the cost of maintaining the hashrate. Yet there is a scarce resource, block size, that ultimately the debate as to whether or not this is sustainable in the long-run cannot be determined *a priori* but will likely be highlighed when the halvings of the next block rewards take place – from 25 BTC to 12.5 BTC around 2016 and then again in roughly every four years.

While the analogy is imperfect, a public highway and the Bitcoin protocol share traits. You have toll roads (miners to pay for transactions), adopt-a-highway volunteers (developers), speed bumps (dust limits). Yet no one owns the protocol so all decision making becomes a matter of public policy debates (i.e., debates on github over what to include and what not to include). Additional value and utility is created on the edges that require investment, yet historically there is an incentive not to build services and products onto the ecosystem because speculating on bitcoin appreciation is less risky than developing services. That is to say, buying and burying bitcoins around the globe instead of building part of the ecosystem has been a lucrative investment strategy because Bitcoin-related startups, like any start-up space, statistically is prone to have the same amount of failures – 3 out of 4 start-ups do not succeed.[154]

As a consequence, due to these incentives there has been a discussion over the past year regarding free-riding. A free-rider refers to someone who benefits from resources, goods, or services without paying for the cost of the benefit. While there is a debate as to whether or not this is an actual problem, Koen Swinkels, an early Bitcoin adopter and technology writer has written about the conundrum this phenomenon creates:

> 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.[155]

Coupled with the lack of incentive to work as a core developer, this situation can be summarized as a socialiazation of labor yet privatization of their gains. Yet simultaneously, holding bitcoins itself helps to develop and market the product (because it increases price which attracts others into the market and pushes price towards where it would be if it were to be used as common medium of exchange).[156] And while this model has been used to develop other open-source software projects, there have been other successful commercializations of open-source products. For instance, SugarCRM, MySQL, MongoDB and Jira all succeeded in the market arguably due to the sponsorship of a dedicated company with clear governance involving the delegation of responsibilities and incorporation of community code contributions.

"Bitcoin neutrality"

Beginning in the mid-2000s there was a debate within the technology and policy making communities over whether or not ISP providers could charge prioritization or additional usage fees for accessing content over the internet. Proponents and advocates of "net neutrality" claimed that all network traffic, irrespective of size, origin or content should be treated the same and delivered in a non-discriminatory fashion. Opponents counter-arguments while based in the economics of scarcity (e.g., a finite amount of bandwidth exists), were often likened to astroturfing because many of the ISPs pushing against "net neutrality" policies were regional monopolies partaking in rent-seeking behavior.

This same type of argument as to what type of transaction should be allowed to be included on the blockchain and how much it should cost to include it, has resurfaced over the past year. Does one-size (1 MB block) or one fixed price (0.0001 BTC) fit all? Can the blockchain operate as a subsidized data buffet, a type of "all-you-can-use" for one fixed price? Is there a limit to "unlimited" transactions for this price and are transaction really "free"?

The answer to these is that, if there are scarce, rivalrous goods, then economic laws of supply and demand apply to them. Because there is a scarce resource, a fixed block size, then there is a fixed supply that cannot satiate an unlimited demand. Thus just as FedEx has multiple product lines for priority mail and content delivery networks (CDN) similarly have multiple service options for providing digital content over the internet – which itself is a cornucopia of publicly and privately owned networks – allowing miners to charge what the market will bear for transaction fees will likely illustrate the actual costs of running a globally decentralized network.

'Get off my lawn, get out of my blockchain'

During the week spanning roughly March 18 - March 24, 2014, there was a large vocal debate between two Bitcoin core developers and members and developers of the Counterparty platform. Counterparty is one of the new "2.0" next-generation platforms. It is a peer-to-peer financial platform uses the Bitcoin blockchain as a method for enabling users to create user-defined assets such as custom tokens or even a contract for difference.

The background in a nutshell was that on October 24, 2013, lead Bitcoin developer Gavin Andresen announced that in an upcoming release of the protocol a new function called OP_RETURN would be included, which is a prunable output (meaning it can be removed if and when a SPV client is released). In his words:

> Pull request #2738 lets developers associate up to 80 bytes of arbitrary data with their transactions by adding an extra "immediately prune-able" zero-valued output.
>
> Why 80 bytes? Because we imagine that most uses will be to hash some larger data (perhaps a contract of some sort) and then embed the hash plus maybe a little bit of metadata into the output. But it is not large enough to do something silly like embed images or tweets.
>
> Why allow any bytes at all? Because we can't stop people from adding one or more ordinary-looking-but-unspendable outputs to their transactions to embed arbitrary data in the blockchain.

While there were ways to insert metadata permanently into the blockchain, much of the community considered this OP_RETURN announcement to be some kind of feature to enable the blockchain to be used as some kind of data store.[157] With this understanding, Counterparty developers similarly built a future version of their platform around this 80 byte space, allowing Counterparty users to send data to this space instead of using multisignature transactions (which is what Counterparty and Mastercoin platforms currently do).

After several months of testing, this feature (or non-feature to some) was released in the 0.9 bitcoind client in mid-March 2014. However, unbeknownst to Counterparty developers, the 80 byte size was reduced to 40 bytes in the final version. And 40 bytes is not large enough to include the necessary amount of data between the Counterparty database and Bitcoin's. As a consequence, several Counterparty developers, not knowing the standard operating procedures for debating these feature inclusions, used a popular web forum called Bitcoin Talk and over the course of a week, more than 40 threads of forum pages were devoted to arguments between two Bitcoin core developers and the Counterparty community.

The discussion involved many topics including what a financial transaction is as well as how Bitcoin Improvement Proposals (BIP) are used to expand the functionality of the protocol. Below are several quotes from Bitcoin developers:[158]

- "It's called a free ride."

- "Too many people were getting the impression that OP_RETURN was a feature, meant to be used."
- "Not acting like bitcoin is your personal property."
- "Every full node has consented to download and store financial transactions."
- "The community agrees and the protocol is updated."
- "All data storage attempts, even the OP_RETURN stuff, are technically abuses the protocol was never intended for."

While there are pages of comments on other venues including notably reddit and *CoinDesk* related to this issue, the last quote in particular is of germane interest.[159]

As noted in the original post by Gavin Andresen, the impression that most of the community had was that this OP_RETURN was an actual feature.[160] Yet as seen in the quotes above, other developers noted that OP_RETURN was not intended to be used as a general data store function and that it was to be used solely for encrypted keys (specifically ECDSA). Furthermore, just as cookies and JavaScript added functionality to the web in a permissionless manner, many people – developers included – believed that you can contribute to the ecosystem in a permissionless manner – that due to its decentralized public nature, anyone can add functionality to the protocol.

One frequently cited examples is AJAX, a framework built from JavaScript which itself was built on top of TCP/IP. The various developers of AJAX tools (most notably Gmail) did not need to call up the inventors of TCP/IP and ask for permission to create this tool. Similarly, neither did Henry Ford need to call up Karl Benz (who was still very alive) and ask for permission to build on and improve upon the idea of an automobile. Likewise, the Bitcoin community typically prides itself on having created a permissionless financial system. Yet the actual reality is that if anyone could change and modify the code located on github, you would likely have a tragedy of the commons – in which both malicious code and beneficial code was being uploaded and added to the protocol and wallets. Speculatively, there would only be chaos if everyone changed the same code and only that code could be uploaded by all users. Instead there is trusted code (put out by the developers) that everybody voluntarily agrees to use (because everybody else does too via consensus which is a requirement to all be part of same network), and anybody else could create alternative codebases but getting users to switch to that code is prohibitively difficult because you would need to overcome network effects.[161] Or in other words, usage of the code and hashrate is permissionless, yet modifying the code (to provide for transaction inclusions) requires permission. In addition, "permission" required for features that involve protocol change is really the permission of 51% of the network. And while these developers may have significant influence over what version of the code miners accept, ultimately it is the miners that decide.[162]

As a consequence, what has emerged is a small, devoted and committed group of volunteers, who have created a process called the Bitcoin Improvement Proposal (BIP) system in which individuals and organizations that want to change or modify the protocol, to submit a proposal (typically a whitepaper) outlining the technical limitations or functionality that would be added

to the protocol through this new proposal. Notable BIPs include #11 which was accepted and integrated m-of-n standard transactions, #13 which integrated pay-to-script hashing (P2SH) and most recently #70, a standardized payment protocol.[163]

While there is a debate as to the existence of gatekeepers, they exist and based on the forum debates, several of the developers were unswayed by the points raised by either Counterparty as a platform or the usage of 80 bytes as a data store.

Again, while this issue is still simmering in both camps, one understated issue going forward will likely needed to be addressed to prevent similar problems from occurring in the future is a formal outline of the steps needed to be taken to dialogue with the core developers (both on and off github) as well as how BIP works – and this standard operating procedure would likely need to be translated into other languages such as Mandarin. For instance, while Counterparty developers all communicate in English fluently, what if another team in China had developed a similar platform using a similar technique yet were unable to debate the merits of their project due to the language barrier? Such restrictions, which exist around all APIs (which is what the Bitcoin protocol may become) could push added value and utility away from Bitcoin, which as a nascent up-start arguably has more upside with the inclusion of 80 bytes than downsides.[164]

How to contact mining pools?

During this debate between Counterpary and Bitcoin developers, another issue was unintentionally highlighted: the centralization of pools.

For instance, below is an actual quote from a Bitcoin developer regarding how the process of convincing a consensus of miners about new transaction types and features of an updated protocol:

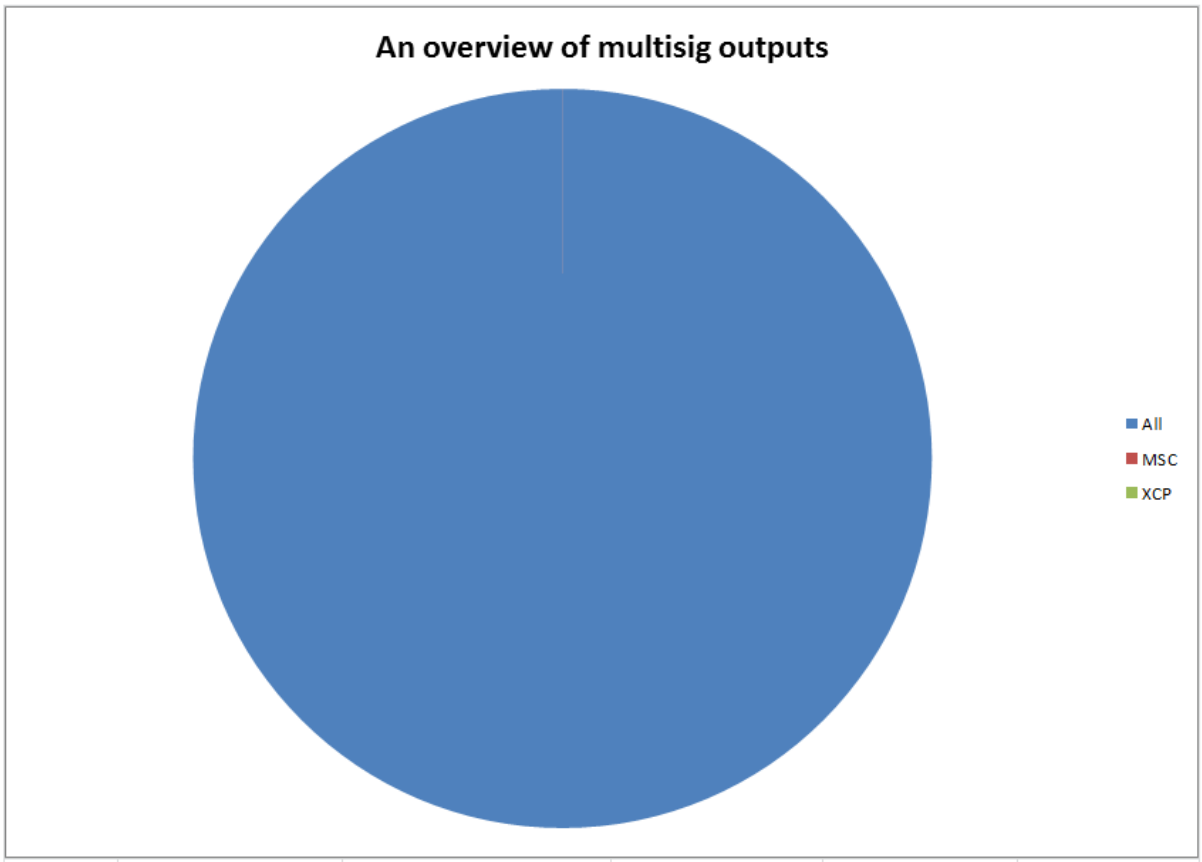
> "Then contact more than a couple of pools. This statement sounds like you wish to force miners to include your transactions; surely you didn't mean it that way?"[165]

This is potentially problematic for several reasons. The first is logistical, even if a new developer could contact a mining pool, how do you contact "unknown" mining pools which represent significant hashrates?[166] Furthermore, one of the original intents and incentives for running Bitcoin mining nodes was that it provided a near anonymous way to secure a trustless payments network – if you know who the miners are, what does that say about the safety and scalability of decentralized proof-of-work systems?[167]

However, if this is the process that will be followed in the future, perhaps there is a way to kill two birds with one stone: a company could hire several core developers and work with mining pools to integrate new features such as merged mining or the ideas discussed by Adam Back in December 2013 or more recently in March 2014 presented by Peter Todd regarding off-chain trees.[168]

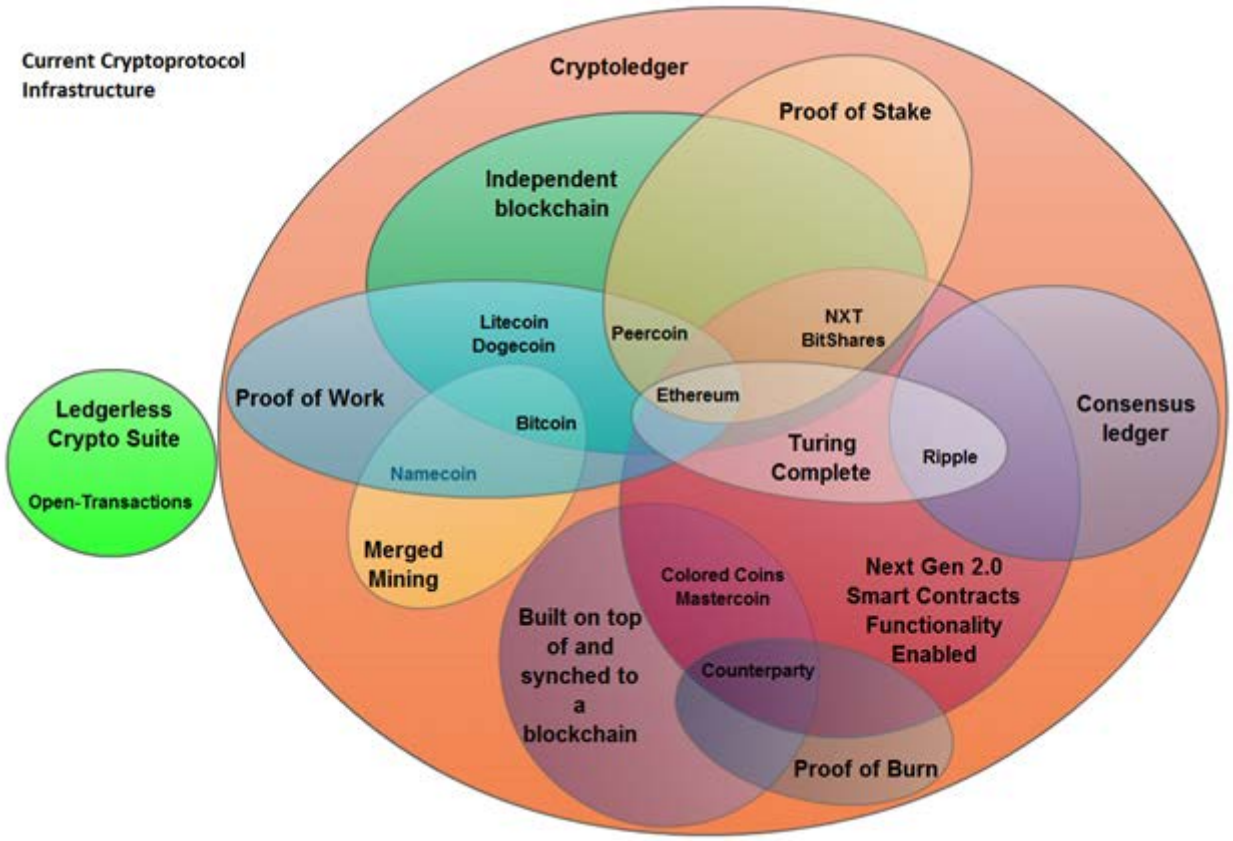
Multisignature transaction bloat

One of the common complaints that some Bitcoin adopters have towards the 2.0 platforms that reside on top of the Bitcoin blockchain, such as Mastercoin, Colored Coins and Counterparty is that in order to interface with Bitcoin, these protocols effectively clutter up the blockchain with "bloat." For instance, in order to make a transaction with Mastercoin, a small amount (roughly 0.0001 BTC) is used to represent a particular asset defined by the Master protocol and only visible to users using a Mastercoin-enabled wallet (which are also open-source). Mastercoin uses the multisig output to accomplish this task (effectively linking Bitcoin's database with Mastercoin's) and as a result, one argument is that these types of transactions will bloat up the blockchain, filling scarce blocks with bloat. Yet as shown in the image below, created on March 24, 2014, the stark reality is that all but 0.000146% of multisig outputs are unrelated to either Mastercoin or Counterparty:[169]



	Multisig transactions	Unspent multisig outputs	Spent multisig outputs	Multisig outputs	Comparison
All				35.508.561	100,00000000%
MSC	2.983	1.025	1.966	2.991	0,00842332%
XCP	2.193	2.201	0	2.201	0,00619851%

Next generation



Can 2.0 fix some other shortcomings?

There are several reasons for why developers have been motivated to create 2.0 platforms including:

> 1) Bitcoin's protocol does not have certain functionality (e.g., smart contracts, user definable assets);
>
> 2) Outside developers which have the ability to build such functionality choose not to do so without financial compensation of which little exists;
>
> 3) *Ad hoc* governance issues require interaction with certain stakeholders and incumbents who are in their position not necessarily through merit but sometimes because of the Peter Principle (i.e., gatekeepers until they choose not to be).

Looking at the above Euler diagram, there are roughly 30 developers and founders working on these 8 projects.[170] How could these same individuals be funded if they tried to work adding extensibility features to the Bitcoin protocol? Perhaps via an assurance contract, through some kind of Kickstarter project in which certain milestones and deadlines are publicly listed.[171]

Another way, and one in which several projects have opted to go, is through a type of crowdfunded "IPO" vis-à-vis bitcoins. Two such examples are the following:

- Mastercoin: on July 31, 2013 an Exodus address was setup for Mastercoin to which individuals would send Bitcoins to in exchange for mastercoins (MSC).[172] Only a limited number of MSC were created during the subsequent month of August and they are only visible to users that use a specially designed wallet that can distinguish them from the rest of the blockchain. After 30-days they raised 4,700 BTC; and 563,162 MSC were created.[173]
- Counterparty used a different strategy through the use of "proof-of-burn" – sending bitcoins to a provably unspendable public address (a terminator address with no corresponding private key). The first and only "burn" took place beginning on January 2, 2014 and lasted for thirty days – now all of the XCP that will ever exist have been created (2.64 million XCP). During that time, 2,130 BTC were effectively destroyed amounting to roughly $2 million in then-market prices (the immediate repercussion was that all other holders of bitcoin saw a net gain in value by roughly 0.01%).[174] Proof-of-burn does not in and of itself raise funds. Rather it incentivizes developers to create utility within the network with the expectation that token appreciation follows.

While this is not an endorsement of this particular fundraising effort, it does show you at least one innovative method for raising development funds. In addition, Ripple Labs the sponsor of Ripple, which is another of the "2.0" platforms noted in the diagram, went a different route and has received $6.5 million in funding from both venture capital and angel investors over the past two years.

Technical reasons to use a different platform

Bitcoin core developers are correct in stating that the original intent of the blockchain was not as a general data store as laid out in the whitepaper. Yet there are many uses that a modified or rebuilt cryptoledger can provide. The following is a list of 84 uses compiled by Antonis Polemitis from Ledra Capital:[175]

Alternate Uses for a Cryptoledger

I. Financial Instruments, Records and Models

1. Currency
2. Private equities
3. Public equities
4. Bonds
5. Derivatives (futures, forwards, swaps, options and more complex variations)
6. Voting rights associated with any of the above
7. Commodities
8. Spending records
9. Trading records
10. Mortgage / loan records
11. Servicing records
12. Crowd-funding
13. Micro-finance
14. Micro-charity

II. Public Records

15. Land titles
16. Vehicle registries
17. Business license
18. Business incorporation / dissolution records
19. Business ownership records
20. Regulatory records
21. Criminal records
22. Passports
23. Birth certificates
24. Death certificates
25. Voter IDs
26. Voting
27. Health / Safety Inspections
28. Building permits
29. Gun permits
30. Forensic evidence
31. Court records
32. Voting records
33. Non-profit records
34. Government/non-profit accounting/transparency

III. Private Records

35. Contracts
36. Signatures
37. Wills
38. Trusts
39. Escrows
40. GPS trails (personal)

IV. Other Semi-Public Records

41. Degree
42. Certifications
43. Learning Outcomes
44. Grades
45. HR records (salary, performance reviews, accomplishment)
46. Medical records
47. Accounting records
48. Business transaction records
49. Genome data
50. GPS trails (institutional)
51. Delivery records
52. Arbitration

V. Physical Asset Keys

53. Home / apartment keys
54. Vacation home / timeshare keys
55. Hotel room keys
56. Car keys
57. Rental car keys
58. Leased cars keys
59. Locker keys
60. Safety deposit box keys
61. Package delivery (split key between delivery firm and receiver)
62. Betting records
63. Fantasy sports records (!)

VI. Intangibles (?)

64. Coupons
65. Vouchers
66. Reservations (restaurants, hotels, queues, etc)
67. Movie tickets
68. Patents
69. Copyrights
70. Trademarks
71. Software licenses
72. Videogame licenses
73. Music/movie/book licenses (DRM)
74. Domain names
75. Online identities
76. Proof of authorship / Proof of prior art

VI. Other

77. Documentary records (photos, audio, video)
78. Data records (sports scores, temperature, etc)
79. Sim Cards
80. GPS network identity
81. Gun unlock codes
82. Weapons unlock codes
83. Nuclear launch codes (!)
84. Spam control (micro-payments for posting)

Several other potential use cases that have received notable coverage over the past quarter are:

- Real estate title tracking which has many additional benefits in developing countries
- Back office automation to track and verify trades without a need to worry about bloating as the cryptoledger would be internal
- HMOs and health providers can share medical records in an m-of-n manner, multisignature transactions could prevent and mitigate abuse
- Crowdequity and content rewards through programs like JoinMyIPO and LTBCoin[176]

The perfect is the enemy of the good

Even if the developers of these 2.0 protocols built the best, must user-friendly, technically robust system, people and most importantly consumers, may still not use it.

For instance, according to Stephen Pair, CTO of BitPay:

> While there are several ambitious projects currently being developed to remove the perceived 'ugliness' in the current protocol, I see this endeavor as Betamax versus VHS. VHS won out in the format war despite lower fidelity and it is possible that the new innovations which arise from the '2.0' projects will be adopted and integrated back into Bitcoin. In the past, I've worked on several software projects that required a team to simultaneously solve 10 to 12 hard problems, without which the underlying functionality could not be capitalized off on. Thus, unless these teams make substantial progress on all fronts, they may be taking on too many things at one time. In our perspective, "the perfect is the enemy of the good," that is to say, HTTP is not as elegant as a lot of other projects that were being developed at the same time, but it is now widely used because it worked good enough – and because the other competing teams suffered from trying to make the most elegant, perfect solutions.[177]

Other notable examples include BeOS, an operating system with a number of then-advanced features such as a 64-bit journaling filing system (JFS) and support for pervasive multithreading. Yet despite its technical superiority, a lack of network effect (user adoption) relegated it to a hobbyist niche. Similarly, Gentoo Linux enables users to compile the source code locally and optimize the codebase to the specific computer. Despite the subsequent speed improvements that such optimization provide, it still remains a small niche in overall marketshare; or as some users quipped: "I want an OS, not a hobby." Itanium is a chip design from Intel in which was intended to shake-up the RISC processor market place yet due to poor silicon performance and compiler issues, became a very expensive project that will likely be terminated.

As a consequence, consumers may just care for simplicity and "smart fine print." For instance, while early adopters may care about token allotment in a payment system, later mainstream adopters may not (i.e., do you know or care how Visa's transfer mechanism works, or do you just use it?).[178] Similarly, it may be the case that in order for an open-source project to succeed in the marketplace, it needs a formal sponsor. For example, while Fedora and Ubuntu are considered the top Linux distributions, in point of fact, Android is the largest Linux-based system and is used in more than two-thirds of all smart phones globally.[179] Similarly, while there are a variety of BSD-based systems (e.g., NetBSD, OpenBSD, FreeBSD), Mac OS X is largely considered the most widespread distribution of BSD.

Can on-chain decentralized systems compete against Visa in the developed world?

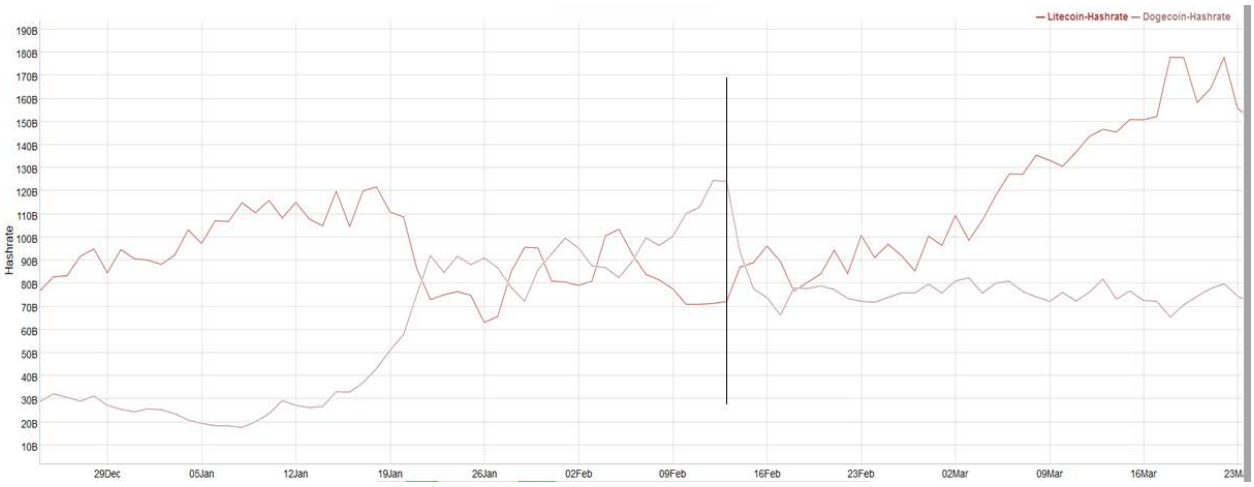
At the moment, no. Only the Ripple protocol (which uses a distributed infrastructure) can potentially match the performance needed of a real-time gross settlement (RTGS) platform such as Visa. Another potential is a proof-of-stake system that uses faster block times than any currently known public system. In February 2014, Sergio Lerner (creator of QixCoin) proposed a theoretical FastCoin5, with "block intervals is 5 seconds and transaction confirmation (for a reversal probability of 0.1%) is below 25 seconds."[180] His implementation is being developed into the NimbleCoin platform.[181] For comparison:

- GeistGeld had **15 second** blocks (but many orphans)[182][183]
- Litecoin has **2.5 minutes** blocks (max 28 tx per second)
- Dogecoin has **1 minute** blocks (max 70 tx per second)
- NXT (proof-of-stake) has **1 minute** blocks, 255 transactions per minute (~4 tx/s)
- Ripple has **5-10 second** ledger closings, and 100-1000 tx per second

For balance, Coinbase, Circle, Bitstamp are effective and efficient but centralized and off-chain, yet in the long run consumers may be okay with that.

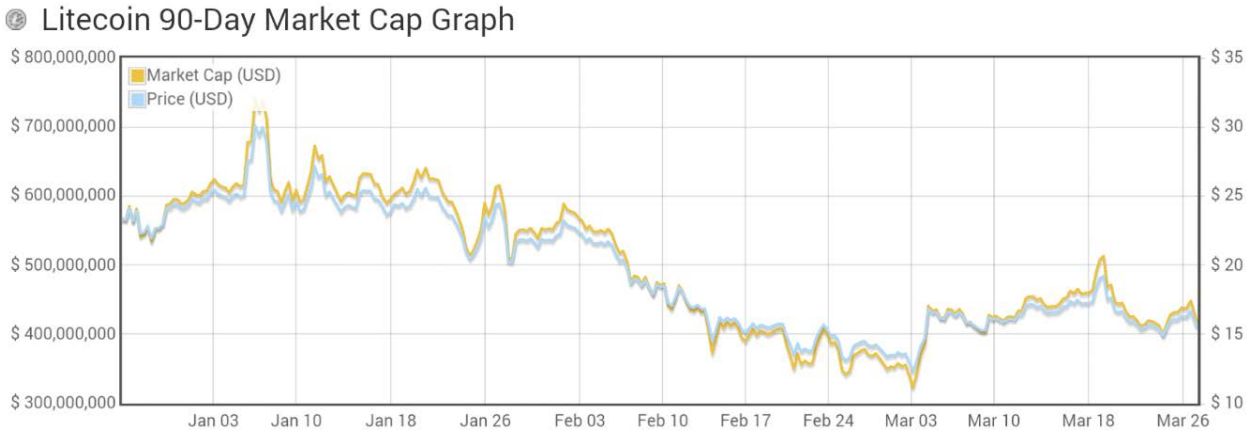
Incentives illustrated

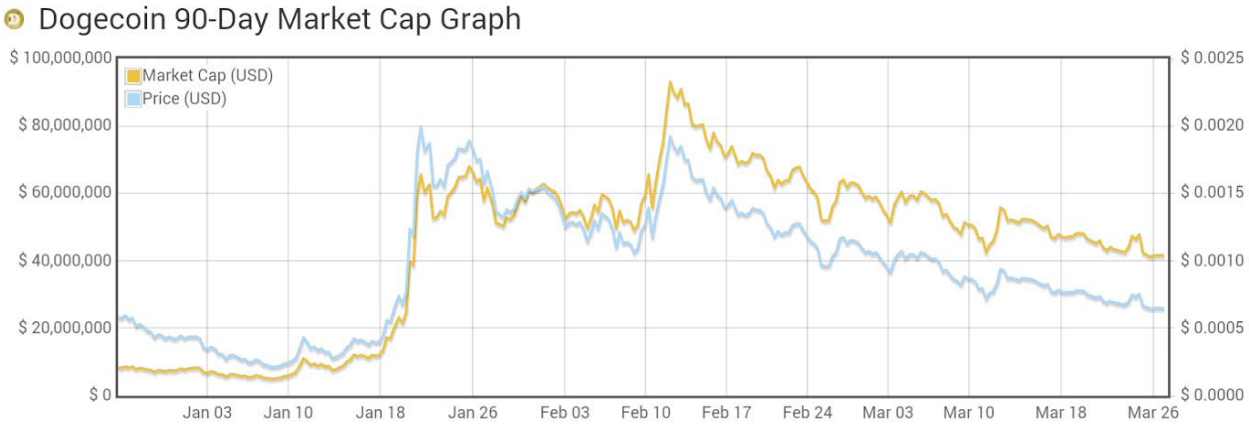
Below is a 90-day chart showing the network hashrate of Litecoin versus Dogecoin.



The black line shows the exact date in which block rewards for Dogecoin were halved (February 14, 2014). Because block rewards were lowered, *ceteris paribus*, hashrate moved back to trend line. Because both of these tokens utilize the Scrypt-based proof-of-work (as opposed to the SHA256d used in Bitcoin), one trend is that many independent miners are pointing their hashing equipment at "middle men" – that is to say, a central pool that will hash a Scrypt-based token that provides the most profit during that day. Popular pools include MiddleCoin, CleverMining, HashCows, WafflePool, Hashbros.

Below are the price levels during the same period of time:





In the second chart, the peak price for Dogecoin coincided with the block reward halving. While nothing is certain in the future, *ceteris paribus*, there are fewer incentives for miners to continue hashing Doge when there are more profitable alternatives. This could change if an ecosystem built up around Doge, creating additional demand for the token and thus causing price appreciation which in turn leads economic actors to continue mining Doge.

Because of the drop in hashrate, Dogecoin is now more vulnerable to a 51% attack which is an issue recently highlighted by Charlie Lee, creator of Litecoin. In April 2014 he proposed to the Dogecoin community, to merge mine the two tokens together much like Namecoin does with Bitcoin.[184] This would allow the two Scrypt-based coins to reinforce and strengthen one another with what would essentially be commonly shared hashrate, which as shown above, is susceptible as block rewards halve.

Hashrate does not determine prices

In a competitive marketplace, the economic profit (which includes the opportunity costs of pursuing certain actions) of a good or service typically tend towards zero.[185] That is to say while firms may still have accounting profit, the additional margins in the long run are reduced due to competitive pressure.

Bitcoin and other cryptocurrencies are subject to similar constraints. Prices provide signals to market participants to either stop or continue an economic activity. As mining pools become more professionalized, managers will track both the accounting profit and even economic profit to account for the opportunity costs foregone in the use of ASICs with bitcoin. While they could rely on token appreciation to boost their long-term solvency, due to competitive pressure mining pools typically must continually sell bitcoins in order to pay for expenses. There are real financial costs to providing new coins, namely electricity and rent (e.g., the operating costs and upkeep of physical plant) – hence the trend towards setting up mining facilities in regions that typically have colder climates and cheaper electricity (e.g., near dams) as extracting the heat produced from mining is a real economic cost.

Thus the two main variables are, the difficulty of hashing a SHA256d and the price per hash. If the price per hash decreases through technological improvements, this may incentivize mining, whereas in contrast, a higher difficulty rating yet with the same financial rewards lowers the profitably per hash and thus disincentivizes the activity.[186] And price, as in any market, is related to the supply and demand of the ledger entry.

Opportunities for legal professionals

Pamela Morgan, is a Chicago-based smart contract attorney with EmpoweredLaw. In her view, the technology can be used to decentralize parts of the legal system and create more efficient processes. For example, smart contracts cannot be nullified due to technical limitations or legal gymnastics. For firms using a crypto ledger for internal applications, such as record-keeping, voting, and employee rewards programs, bloat is unlikely to be a major impediment to implementation and maintenance. Other applications for the blockchain technology include providing a method for elections (corporate, civic) which enables greater transparency, nearly instant results, and unforgeability. Currently, Morgan is using the blockchain to register documents and be able to prove the existence of the documents at a later date. She uses proof of existence, but there are other similar services available. The service protects the confidentiality of the document, while providing a public timestamped record of its existence.[187] Uses include proving the existence of a Last Will and Testament. In her words, “Documents need to be secured and protected so that they can be delivered to another party (judge/heir/executor) when they are needed. One issue is ensuring document integrity - that the document presented today hasn't been altered - that it's the exact same document. PDF version of a document uploaded to the blockchain can provide that proof. For around $3. It is so inexpensive, why wouldn’t you do it?"[188]

Opportunities for middle offices

Preston Byrne is a London-based securitization attorney who sees at least two high-value industrial uses for cryptoledgers: 1) by governments, and 2) by banks and large corporates. As to the first Byrne points to MuniBit, a proposal of the Startup Cities Institute, which would involve the generation of coins by one public input address, and their "destruction" through depositing them in one output address, mirroring (respectively) the entry point for all receipts, including foreign aid and taxes, and expenditures, including salaries.[189] Such a ledger would be mineable only by government but visible to the entire world, with individuals and government departments being issued with keypairs in respect of the funds they have lawful authority to access. Since all interdepartmental transactions could be fully traced such a system might, if implemented, mitigate and prevent leakage of funds in state institutions of developing countries.

Another potential application, according to Byrne, is within large corporates or banks.[190] One example he provides is their use as an automated accounts reconciliation system to be used in conjunction with more traditional, “trusted” ledgers and reliable external data sources, with the proprietary cryptoledger sitting alongside as a kind of automated gatekeeper. Each financial contract would have two keypairs, one for the trader and one representing the counterparty (which would in fact be held by a computer operated by the bank, the relevant exchange, or the two in conjunction); the cryptoledger would independently verify booked and settled trades, preventing traders from issuing instructions which are non-existent or exceed their limits (a bank's equivalent of a double-spend). Tokens representing in-the-money or out-of-the-money positions would move within and beyond a trader's control based on real-time input from objective external data points. Byrne says it is entirely possible for such a system to prevent traders from issuing instructions which exceed their trading limits and endanger the institutions which employ them, pointing to examples from the recent past where traders who had a high degree of familiarity with internal compliance systems were able to "game the books" as they knew their firms' accountants would not discover the fraud for one or two weeks after it had been committed.

One such application, Subledger, could be used as the API connecting such a cryptoledger with a traditional ledger system.[191] Banks could inexpensively reduce their exposure and increase their awareness of sudden or unexpected liabilities on their balance sheets, and furthermore, the cryptoledger would be impossible to forge. In Byrne’s view, such a setup would have prevented or mitigated fraud and manipulation from well-known cases of fraudulent trading such as that of Jérôme Kerviel, Nick Leeson and Kweku Adoboli, and could even be used to provide real-time data on interbank lending which would prevent future LIBOR manipulation.

Conclusions

Sometimes good is good enough. New beginners and even experts alike may be perfectly satisfied and demand no more than a Yamaha piano instead of a Steinway (or for taxis, a Yaris

instead of a Lexus). Thus Bitcoin may ultimately satisfy the market place because some perceive it as good enough.

- All but four of the Bitcoin core developers are volunteers in some capacity yet the entire ecosystem depends on them not to introduce a new bug or problem that has the ramifications effecting several billion dollars' worth of assets. Thus it is understandable that these developers are conservative in adding new features, consequently there may be a business opportunity to provide employment to multiple developers to produce infrastructure services to the entire ecosystem (not limited simply to one particular token).
- Based on the evidence provided above, Bitcoin has massive structural incentive issues that it is as of yet totally unclear it (or anything else, for that matter) can overcome.[192] The incentives that are being overlooked in discussions regarding challenges within the ecosystem include a lack of financial incentives for attracting scarce talent to work on the core protocol. Similarly, because ASICs are a depreciating capital good, rational economic actors will utilize their resources in a profitable manner, including using an ASIC for non-bitcoin related mining after the profitable hashing window of opportunity disappears.
- Two of the underutilized capabilities that could be used to incentivize continued participation once block rewards lessen are merged mining and atomic transactions. However incentives are skewed to create an entirely new altchain to perform a new function entirely when in fact tying the two technologies together may provide new functionality to the ecosystem for experimentation.
- Special interest groups may exert pressure to include (or not include) certain features and lobbying and politicking will likely increase due to a "public goods" issue described in various dimensions.
- "Jawboning" is a term originating from the Kennedy and Johnson administrations. At the time, certain policy makers believed they could "talk down" the effects of monetary inflation by giving speeches and announcements (e.g., "Whip Inflation" by Ford and Carter). Yet inflation is not a cartoon character. Similarly, attempts to "jawbone" the cryptocurrency marketplace regarding altcoins will not work.[193] There is an economic incentive for miners to continue creating altcoins – jawboning will work no better than central planners could talk down inflation in Zimbabwe during 2008. If you cannot ban the behavior or provide greater incentives to do other behaviors, the forks will continue.[194] Furthermore, Bitcoin will not fail simply because scarce resources (e.g., human capital) are attracted to other projects. This would be akin to saying the Linux community should rally behind one and only one Linux distribution. Distros have come and gone, in fact, Slackware was created in 1993 and is the oldest remaining distro, yet as noted above, despite the competitive forces and consumers using many different distributions (of which Slackware is just one), Linux itself is now a widely used tool on smartphones and tablets. The idea was bigger than the first-mover (or second, or third).
- Any technological innovations that improves the performance of decentralized networks (e.g., better switching equipment, faster processors) will likely increase the performance of centralized competitors as well – and rogue attackers too. Thus relying on a

hardware or infrastructure break through to reduce overhead is probably a net gain for every party.[195]

- Despite all the shortcoming discussed in this paper, Bitcoin (the protocol) will still likely flourish in the near term due to network effects, mind-share and edge-based ecosystem. Furthermore, some of the governance challenges noted above will also be an issue for nearly all of the 2.0 platforms. While this is not an endorsement of their service, Ripple Labs is likely one of the better positioned in that it is the custodian of a protocol creating a known chain-of-command and is only able to extract value from the network from XRP which provides an incentive to manage and create value to the network in the most efficient manner. In addition, a proof-of-stake (POS) system is along with the Ripple protocol, the most likely candidate for intranet-based ledgers based on currently known public models as of this writing.
- Edge providers such as CoinBase, BitPay and trading platforms like Kraken provide new functionality beyond simple exchanges, creating new utility to the ecosystem and could conceivably act as clearing houses if absorbed into existing financial institutions. In the long-run the average user may not care about their centralized nature.
- These tools, like any database, are agnostic and open-source creating new use-cases and enabling new parties irrespective of ideology to utilize them. That is to say, decision makers at institutions will use the code that brings new utility to their organizations and dispense of the code that is unneeded. Thus, five years from now there will likely be thousands of cryptoledgers used internally and externally as the technology moves beyond a niche payment experiment (as noted by the 84 use cases and growing).
- 2.0 platforms following the same governance structure as Bitcoin will likely have the same governance hurdles. Similarly, alternative coins based on proof-of-work could have similar challenges as the seigniorage incentives are removed.

It is impossible to predict the future or to know *a priori* what the market will eventually adopt. And perhaps the concerns raised in this paper are not show stoppers but mere bumps in the road. Time will tell whether or not currently encoded incentive structures motivate certain actions over others.

Acknowledgements

I would like to thank the following people for providing feedback, constructive criticism and anecdotes: Kevin Barnett, Isaac Bergman, Gwern Branwen, Preston Byrne, Joseph Chow, Petri Kajander, Andrew Lapp, Sergio Lerner, Taariq Lewis, Adam Marsh, Andrew Miller, Pamela Morgan, Ryan Orr, Robert Sams, Koen Swinkels, Eddy Travia and Andrew White. Special thanks to Dave Babbitt for explaining several econometric models and to Jonathan Levin for his extensive assistance in refining the private incentives versus public goods issues.

Endnotes

[1] The bulk of this paper is based off a presentation I gave on March 27, 2014 at the Institute for the Future (slides). I can be reached at: tswanson@gmail.com

[2] While in practice most users and developers consider it part of the public domain, Satoshi Nakamoto posted a short explanation for why he chose an MIT license over a GPL. See also Why was the MIT license chosen for Bitcoin?

[3] The 8 identities of Bitcoin by William Mouyagar

[4] The term cryptoledger is used for both aesthetic purposes, as dashes become distracting, and because it also encompasses non-blockchain based Merkle tree consensus systems such as Ripple (which uses a cryptographic ledger as well). One reviewer suggested that this is ambiguous however, noting that "calling Ripple a "consensus ledger" as opposed to a "blockchain" is not a very clear distinction. Ripple is indeed effectively a blockchain since the nodes leave a public trail of their signatures on the transactions and updates to the ledger. The only really important distinction is that it is an identity-based algorithm rather than proof-of-work." However, according to David Schwartz, chief cryptographer at Ripple Labs, the history of the ledger does exist but unlike the blockchain it is not required at all to validate the last closed ledger. For a blockchain to be valid the entire chain has to be stored somewhere. The entire history of the ledger can be thrown out and the Ripple network can continue to securely operate like nothing happened. This topic will likely fill volumes in the years to come.

[5] The author, Satoshi Nakamoto (a pseudonym), states early on a cryptography mailing list that he did it backwards, writing code first then writing the white paper, see the last comment on November 9th, Re: Bitcoin P2P e-cash paper. The whitepaper is: Bitcoin: A Peer-to-Peer Electronic Cash System

[6] Bitcoin is Worse is Better by Gwern Branwen

[7] See How do bitcoin transactions work? from *CoinDesk* and How the Bitcoin protocol actually works by Michael Nielsen

[8] There is arguably actually a third "key" as well, a hash of the public key. See Bitcoins the hard way: Using the raw Bitcoin protocol by Ken Shirriff

[9] Cryptographers at GCHQ, the British intelligence agency had independently invented and used the public-private key Diffie-Hellman technique several years prior to 1976. As a result of this and other mathematical schemas, the entire global financial industry, every diplomatic corps, cloud services and all e-commerce (to name a few) currently rely on cryptographic methods to securely transmit data.

[10] Elliptic curve cryptography was first introduced by Victor Miller and Neal Koblitz in 1985. While Diffie-Hellman can be used for public key encryption, not many people actually use it that way. Also, Diffie-Hellman cannot do digital signatures which is what Bitcoin uses public key encryption for. Furthermore, Bitcoin uses parameters set by secp256k1 (not the exploitable secp256r1). See NSA Backdoors and Bitcoin by Chris Pacia, The Cryptography of Bitcoin by Edward Yang, An Overview of Elliptic Curve Cryptography by Julio López and Ricardo Dahab, ECDSA from StackExchange, Why can't Diffie-Hellman be used for signing? from StackExchange and Cryptography and Contracts by Daniel Krawisz.

[11] I would like to thank Stephan Kinsella for describing and clarifying this point.

[12] According to Black's Law Dictionary entry for, "possession is nine-tenths of the law":
This adage is not to be taken as true to the full extent, so as to mean that the person in possession can only be ousted by one whose title is nine times better than his, but it places in a strong light the legal truth that every claimant must succeed by the strength of his own title, and not by the weakness of his antagonist's.

[13] There is no consensus, as to what *moneyness* attributes a bitcoin represents. One notable paper recently published tackling this issue is Bitcoin: a Money-like Informational Commodity by Jan A. Bergstra & Peter Weijland

[14] A Merkle tree is used to "store" the large transaction history (at the time of this writing, the blockchain is roughly 14 gigabytes and growing). Technically transactions are not actually "stored" in a hash tree per se, but rather the proof-of-work that says a block is valid is based on hashing the Merkle tree input of all the transactions.

[15] Bitcoin uses a modified version of Hashcash which was originally proposed in March 1997 by Adam Back; the actual cryptographic hash function is SHA256d. It should also be noted that he recently voiced some vulnerability

concerns regarding implementing a Turing-complete language with a cryptoledger, see Turing complete language vs non-Turing complete (Ethereum vs Bitcoin)

[16] Or in short, mining as done today has very simple requirements: hard to produce results, yet easy to verify and relatively hard to hardware optimize. This last aspect has changed with the advent of ASICs, yet due to competition there is an "arms race" between semiconductor designers. See The Bitcoin-Mining Arms Race Heats Up from *Bloomberg Businessweek*

[17] Washing virtual money from *The Economist*

[18] There are actually four groups that ultimately provide "consensus": miners, holders of tokens (anyone with a wallet), merchants and web-based services such as exchanges. While miners are usually considered the most powerful (because without them, there would be no network, ledger or authentication) each of these other groups hold some sway. Without exchanges, many participants would be unable to trade bitcoin for fiat or other alt tokens. Without merchants, many participants would be unable to trade bitcoin for goods and services. There is also room to distinguish a "hasher" and a "miner." In the long-term "hashers" may end up causing centralization of network resources into central pools that diminishes the ability for the network to stave off outward attacks. Most "miners" today lack power to select or validate bitcoin transactions. Modern miners simply sell a computing service (hashing) to the mining pools. Decentralized pools like P2Pool would help alleviate some of that concern yet there are financial incentives for "hashers" to use larger pools that create imbalances that are discussed in Hashers are not miners, and Bitcoin network doesn't need them. There are other other participants called "fully validating nodes" which provide a "free," uncompensated service which validate and relay transactions to the rest of the network. According to the Bitnodes projects, as of this writing there are roughly 8,000 such nodes and the new Nodeshares program is trying to increase this number through donations. See also Block chain entry and Selfish Mining: A 25% Attack Against the Bitcoin Network by Vitalik Buterin. The Ethereum project plans to use functional data structures and the trees are called "uncles." See Grokking Functional Data Structures by Debasish Ghosh

[19] Operating a node is not the same thing as mining, running a full node ensures the integrity of the network. Full nodes keep a copy of the entire blockchain. Pool miners do not operate as nodes as they communicate with the pool owner which does operate as a full node. See Bitter to Better — How to Make Bitcoin a Better Currency by Barber *et. al.* and What can an attacker with 51% of hash power do? from StackExchange

[20] One of the best explanations of how hashing works can be found in: Bitcoin Mining Explained Like You're Five: Part 2 – Mechanics by Chris Pacia

[21] See Bitcoin Mining Explained Like You're Five: Part 2 – Mechanics by Chris Pacia and The Marginal Cost of Cryptocurrency by Robert Sams

[22] This effectively means that there could be billions of contracts, not just 21 million.

[23] The Table is from: The Bitcoin Central Bank's Perfect Monetary Policy by Pierre Rochard

[24] Xapo alone raised $20 million earlier this year to provide wallet, vault and insurance coverage for users. See Xapo Raises $20 Million for 'Ultra-Secure' Bitcoin Storage from *CoinDesk*

[25] See Simplified payment verification, Really Really ultimate blockchain compression: CoinWitness by Greg Maxwell and Ultimate blockchain compression w/ trust-free lite nodes

[26] Fake gold bars turn up in Manhattan from *MyFoxNY*

[27] While he did not coin the term, Heinlein popularized it in his novel, *The Moon is a Harsh Mistress*

[28] This price fluctuates and is based on the Cost Per Transaction metric from Blockchain.info, however it is a bit of a misleading figure. A more appropriate figure might be the cost per available transactions - or rather, instead of dividing the cost of the computing network by the number of transactions being handled today, it should be divided by the number of transactions it *could* handle. For instance, if Visa's network dropped to 1 transaction per second, they would likely not immediately have any drastic cost savings and so their cost per transaction would also be relatively high. See also the $50 cited in Bitcoin – A Jack of All Trades is the Master of None by Ken Griffith. If the substitution of appreciation – masked by inflation and seigniorage fees -- with actual privatized transaction costs becomes a reality, *ceteris paribus*, fewer people could transact as existing miners increase fees significantly to cover their capital expenditures. This could reduce transaction volume and based on the comments of one reviewer, eventually could become a spiral of centralization: other unprofitable marginal miners leave the pool, which reduces the utility of the payment network.

[29] What is the Carbon Footprint of a Bitcoin? from *CoinDesk*

[30] Bitcoin's Carbon Emissions: It's All Relative from *CoinDesk*

[31] Gridcoin and Computing for Good attempt to diminish the "wasted" electricity towards an activity with productive utility. More discussion at: Charles Stross takes on the Bitcoin community
[32] Guess what? Dollar bills are madeof cotton from *CNN|Money*
[33] Environmental impact of eurobanknotes from European Central Bank
[34] Cotton and U.S. Currency from Cotton.org
[35] I would like to thank Robert Sams for his feedback clarifying the strict versus extended definition of seigniorage in this section.
[36] Are Virtual "Currencies" Likely to Succeed? by Daniel Thornton
[37] For balance, on this last point one reviewer noted that "in principle this is the case with a cryptocurrency that does not cap its supply. Bitcoin of course does, which is a big problem."
[38] I asked Tristan Winters and he was unaware of who the author was, via ICE Cubed Exchange
[39] The first scheduled halving on the Bitcoin network took place on November 28, 2012; rewards dropped from 50 to 25 bitcoins. See Rewards set to halve for digital money miners from *BBC* and Bitcoin Community Celebrates "Halving Day" from the Bitcoin Foundation
[40] Pay Another Way: Bitcoin from WordPress
[41] See also: the report at Scribd and coverage from *CoinDesk*. Special thanks to Tuur Demeester for highlighting this chart in a tweet. It should also be noted that there is very little research on the volume of bitcoins used in remittances, it is likely quite low. See Why Bitcoin Faces an Uphill Battle in the Remittance Market from *CoinDesk*
[42] In contrast UBS published a paper noting that bitcoin transaction costs hover around 4% and fluctuate as high as 8%. Thus there is a debate as to methodology. See Bitcoins and Banks: Problematic currency, interesting payment system from UBS and UBS: Banks Could 'Absorb the Benefits' of Bitcoin from *CoinDesk*
[43] One reviewer of this manuscript believes it is misleading to say that the average cost of a Bitcoin transaction is not one percent, or that the transaction once inflation is taken into consideration is likely higher, up to 15%. That inflation via quantitative easing (QE) should be factored into all such calculations. This of course is a complex argument and difficult to precisely quantify as these numbers vary from jurisdiction to jurisdiction as capital looks for the highest returns and thus crossed borders creating unforeseen asset bubbles. In contrast, because of its global reach, relative speed to some traditional payments, impossible chargeback or forge, relatively open ecosystem and peer-to-peer bilateral trade Bitcoin could find its niche as a store of value. After all, it has all the advantages of precious metals and could have arguably been used in places like Argentina to stave off the inflation during the 2000s and now 2010s (see Chapter 2 in *Great Chain of Numbers*).
[44] Will Migrant Workers Drive Bitcoin's Mundane Future? from *Bloomberg*
[45] Is Bitcoin the future of remittances? from *CCTV* and Remittance Prices Worldwide from World Bank
[46] Migrants from developing countries to send home $414 billion in earnings in 2013 from World Bank
[47] African Migrants Could Save US$4 Billion Annually On Remittance Fees, Finds World Bank from World Bank
[48] One reviewer noted that this is not necessarily a valid comparison because credit card payments are not necessarily faster than Bitcoin due to charge backs and cancellations: they can be revoked for many months.
[49] In addition to the Hardfork Wishlist, Vitalik Buterin has a running list of issues facing cryptocurrencies: Big Problems in Cryptocurrency and the corresponding video, Hard Problems in Cryptocurrency. Furthermore, Daniel Larimer recently published a description of Delegated Proof-of-Stake (DPOS) which tries to address several of these issues.
[50] Another interesting discussion on the block size issue is Is there a consensus on the blocksize limit issue? on reddit and Bitcoin needs to scale by a factor of 1000 to compete with Visa. Here's how to do it. from *The Washington Post*
[51] Open-Transactions has been working on federated servers and voting pools that may provide for a less-trusted solution. See also Voting Pools: How to Stop the Plague of BitcoinHeists, Thefts, Hacks, Scams, and Losses from Bitcoinism
[52] For a discussion of what an orphan block is see What are orphaned and stale blocks? from StackExchange
[53] Meni Rosenfeld put together an interesting analysis of the various payout methods for mining pools, see Analysis of Bitcoin Pooled Mining Reward Systems
[54] There are other solutions such as merged mining discussed by David Johnston at Coinsummit as well as alternative decentralized blockchains that are integrated with Bitcoin as proposed by Peter Todd and another proposal from Sergio Lerner. See Decentralized Applications - the future of Bitcoin and virtual currencies?, Off-

chain Transactions - Bitcoin 2013 Conference - Peter Todd, [Bitcoin-development] Coinbase TxOut Hashcash, Safe merged-mining and the Bitcoin's Karma and E73 – Reset Your Expectations from *Let's Talk Bitcoin*

[55] See Episode 99 of *Let's Talk Bitcoin* -- Adam Back and Austin Hill have a potential solution to this issue and several other hurdles discussed in the paper. Back also describes more of the process in this thread on reddit.

[56] This is not necessarily the case though as some hobbyist and independent miners profitably rent co-location space and leased servers for their ASICs which includes gigabit bandwidth.

[57] That is to say, given the same hardware, same demand and same network capacity – *ceteris paribus* transaction costs should be the same, either Visa's rates will decrease, Bitcoin's will increase and/or they will meet somewhere in the middle. One additional burden on Bitcoin however is that due to the CAP theorem, decentralization creates (and needs) additional overhead, thus it may actually cost more for some transactions on Bitcoin, such as payments compared to Visa.

[58] See the comments on this reddit thread, particularly from Theymos

[59] Sites like Blockchain.info and BlockExplorer publicly provide the details of statistics like block sizes.

[60] M-PESA and Enabling financial transactions for consumers and businesses: Safaricom's M-PESA mobile money service by Filippo Veglio

[61] Kipochi launches first Bitcoin wallet in Africa with M-Pesa integration from Kipochi

[62] 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*

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

[64] According to an email exchange with Michael Youssefmir, who has previously published mobile data pricing on Ghana, "MPESA was successful because Safaricom had a monopoly and regulators failed to regulate before the system took hold. Successful mobile money systems in the class of MPESA must become defacto standards. The fragmentation and regulation that occurred in other African countries is exactly why we keep having to talk about Kenya and only Kenya. As a defacto standard that is resistant to regulation, bitcoin is an ideal currency and system to serve as mobile money in the developing world."

[65] Fewer than one in three Africans has a mobile phone from *Reuters* and The Sleeping Giants Of African Mobile Payments from *TechCrunch*

[66] Half the World is Unbanked from Financial Access Initiative

[67] Professor Evans uses a different title "Chart 1" than what is in this manuscript. See Bitcoin Payments: Igniting Or Not? by David Evans

[68] 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*

[69] NXT currently has a maximum rate of 255 transactions per block and 1 block is processed every minute, so roughly 4 transactions per second. However, 'transparent mining' is a new feature that is being developed by NXT which will enable it to compete with Ripple and other payment platforms. See Transactions per block and maximum transactions per second from Nextcoin.org and Transparent mining, or What makes Nxt a 2nd generation currency from Bitcointalk

[70] Another reviewer suggested that this was not an apples-to-apples comparison because SMS functionality is built into the feature-phones that Kenyans have. Thus a Bitcoin app would have to be on every phone and there would need to be people willing to accept Bitcoin in order for this to be a fair comparison. While this may be the technical case, the larger issue is that media coverage of Bitcoin dwarfs similar M-PESA coverage in nearly every market, yet despite this, there has been very little adoption due to the reasons discussed in this manuscript (e.g., cumbersome wallets, security vulnerabilities on the edges, no 'smart fine print').

[71] Note that since the original genesis block, individuals have inserted metadata including text and images into the block chain. See Hidden surprises in the Bitcoin blockchain and how they are stored: Nelson Mandela, Wikileaks, photos, and Python software by Ken Shirriff

[72] Even though this is the most widely cited use case in virtually all reports on Bitcoin, there are few surveys done to provide actual data on the volume of Bitcoin -> Fiat (and vice-versa) related solely to remittances.

[73] ACH stands for Automated Clearing House, which is an electronic financial network in the US. In 2012 it processed 21 billion transactions worth a total of $36.9 trillion. See ACH Payment Volume Exceeds 21 Billion in 2012 from NACHA. Other types of clearing house systems are Fedwire and Clearing House Interbank Payments System (CHIPS), both of which handle more than $1 trillion in daily settlements.

[74] This issue was recently highlighted in a very articulate article, Bitcoin – A Jack of All Trades is the Master of None by Ken Griffith. There are other financial startups in the payments space including Coin (a swipeable card) and Ricardo. In addition, Apple is including functionality with new iPhone hardware and software that allows Bob to scan barcodes at stores and instantly pay with his phone instead of going to the checkout. Bob can also pay with a photo of the item. See Bitcoin vs. Coin: Which will have the most success in 2014? From *The Next Web*, Ricardo – An Executive Summary and Apple Pushes Deeper Into Mobile Payments from *The Wall Street Journal*

[75] See Bitcoin Seen as Little Threat to Payment Firms from *Bloomberg*. MasterCard recently launched a new location-based service called Syniverse. See MasterCard Creates New Payment Product With A Company Most Have Never Heard Of. by Brian Roemmele

[76] From definition of CAP theorem

[77] In Satoshi's own words: "We should have a gentleman's agreement to postpone the GPU arms race as long as we can for the good of the network." See Re: A few suggestions and Academics Spy Weaknesses in Bitcoin's Foundations from *Technology Review*

[78] See Hashcash.org and Episode #77 from *Let's Talk Bitcoin*. Last year Back published a brief autobiography on Bitcointalk.

[79] Pool chart as of March 25, 2014: http://bitcoinchain.com/pools

[80] There are some conflicting dates, with September and October "start" dates depending on the source, however his original public statement is still under the original post on the announcement thread for November 27, 2010. This ambiguity is further compounded by a lack of official statement on the website, noting that the pool's first block reward was on December 16, 2010. The timestamp for the first entry on the Bitcoin wiki under Pooled mining is December 24, 2010. BitPenny is the second oldest, with beta tests beginning February 8, 2010 and Deepbit is another early mining pool, beginning operations on February 24, 2011.

[81] Prior to the creation of slush's mining pool, another user, ArtForz was the purportedly the first user to develop a GPU bitcoin mining client in July 18, 2010. During a period of months he also purportedly capitalized off the invention by mining approximately 25% of bitcoins which according to him, later dwindled to less than <1%. See Re: Custom FPGA Board for Sale! and When was the first GPU miner made available publicly? from StackExchange

[82] According to the History of Bitcoin, Slush's Pool reached 10,000 Mhash/s on January 8, 2011

[83] See Mining hardware comparison

[84] See the Red Queen's race and What is the Carbon Footprint of a Bitcoin? from *CoinDesk*

[85] See Re: [ANN][XCP] Counterparty Protocol, Client and Coin (built on Bitcoin) - Official

[86] This is speculation and based on collusion which is disincentivized via seigniorage. Once block rewards diminish and fees float, there is a greater incentive to charge what the market will bear which arguably incentivizes collusion; yet high fees also incentivize new entrants and other competition. See also: Bitcoin and Beyond: The Possibilities and Pitfalls of Virtual Currencies by David Andolfatto

[87] This is a paraphrase from Jeff Garzik, a Bitcoin developer. Furthermore, decentralized pools like P2Pool would help alleviate some of that concern, yet there are financial incentives for "hashers" to use larger pools that create imbalances that are discussed in Hashers are not miners, and Bitcoin network doesn't need them.

[88] Tweet permalink: https://twitter.com/jgarzik/status/429058872725102593

[89] An example is Bi•Fury from Crypto Store. In terms of electricity, this has always been an issue even as far back as 2011, see Bitcoin Mining Update: Power Usage Costs Across the United States from *PC Perspective*

[90] See Episode 99 of *Let's Talk Bitcoin*. Adam Back and Austin Hill have a potential solution to this issue and several other hurdles discussed in the paper. For more about sidechains see merged mining vs side-chains (another kind of merged mining) from Bitcoin Talk and for on a two-way peg see the comments from Greg Maxwell in [Bitcoin-development] is there a way to do bitcoin-staging?

[91] [ANN] High-speed Bitcoin Relay Network by Matt Corallo

[92] The Future of Bitcoin: Corporate Mines and Network Peering? from *Data Center Knowledge*

[93] In his new book on high-frequency trading (HFT), Michael Lewis describes in *Flash Boys* how HFT firms would bid over whose systems were closest to exit and entry router nodes relative to the internet backbone. Shaving the latency time into milliseconds and microseconds created a computational arms war that could replay itself in the proof-of-work segment as well.

[94] Accelerating Bitcoin's Transaction Processing Fast Money Grows on Trees, Not Chains by Yonatan Sompolinksy and Aviv Zohar

[95] Information Propagation in the Bitcoin Network by Christian Decker and Roger Wattenhofer

[96] Selfish Mining: A 25% Attack Against the Bitcoin Network by Vitalik Buterin
[97] Rumours, Panic and a DDoS Attack: Huobi's Wild Week from *CoinDesk*
[98] Other popular tactics, especially in China, is to hack into a financial reporter's Weibo account (the equivalent of Twitter) and post fake news about a coming government crackdown. This temporarily spooks the market causing a sell-off. Hackers will sell bitcoins prior to publishing the fake news and then buy on the manipulated dip.
[99] Merged mine coins are vulnerable if it cannot acquire 51% of the mining capacity to protect it. Coiledcoin attempted to use merged mining from the start but failed to convince at least one pool, which attacked it. See Luke-Jr's statement on Bitcoin Talk. One incentive to DDOS an altcoin is to prevent competition from occurring. Warren Togami (lead developer of Litecoin) warned Litecoin users in November 2013 that they should not antagonize Bitcoin users for this reason, as Bitcoin users have the financial means and technical prowess to DDOS Litecoin forums, exchanges, pools, etc. This phenomenon is not new either as pool operators over the past 4 years have been attacked by a variety of actors (hackers, competitors, etc.). Competitors could hire a botnet to take down a competing pool, the less competition, the more possible chances your own pool has of hashing blocks. It happens globally too as seen with Huobi, a cryptocurrency exchange in China, which underwent a DDOS on the weekend of March 22-23 2014. See Rumours, Panic and a DDoS Attack: Huobi's Wild Week from *CoinDesk*and Safe merged-mining and the Bitcoin's Karma by Sergio Lerner
[100] Selfish Mining: A 25% Attack Against the Bitcoin Network by Vitalik Buterin
[101] In 2011, Sergio Lerner published a paper detailing MAVEPAY, which could in theory achieve 1000 transaction per second purportedly using the same resources as Bitcoin today; see MAVEPAY, A New Lightweight Payment Scheme For Peer To Peer Currency Networks. Jeff Garzik has a demonstration that purportedly reaches 100 per second. See his tweet. Similarly Aviv Zohar and Yonatan Sompolinksy have a paper discussing ways to speed up transaction processing, Accelerating Bitcoin's Transaction Processing Fast Money Grows on Trees, Not Chains
[102] See Transaction fees
[103] In setting a fixed rate, Gavin Andresen unintentionally created a mild distortion that will be fixed when fees can be floated. One modern analogy would be the equivalent of a Federal Reserve Board determining deposit rates by fiat.
[104] Last year Mike Hearn and Matt Corallo added support for micropayment channels to bitcoinj. See [ANNOUNCE] Micro-payment channels implementation now in bitcoinj
[105] Permalink to Gavin Andresen's comment.
[106] 4 New Bitcoin Features Revealed by Core Developer Mike Hearn from *Cryptocoins News*
[107] One reviewer of this manuscript mentioned that as the reward falls, this subsidy will gradually be eliminated and that hash power may fall since right now there seems to be "far too much hashing going on - the threat of double-spend just is not that big." Yet the reviewer does not see a specific reason to expect fees to increase to near the block reward: "users have no incentive to pay such exorbitant amounts rather than just wait a little while longer. Fees will probably remain reasonable, and so hashrate will fall to an optimal level where double-spends occasionally happen (rather than the inefficient status quo where double-spends never happen)." Meni Rosenfeld has an interesting analysis that touches on this point, see Analysis of hashrate-based double-spending
[108] Image from The Tragedy of the Commons from Penn State
[109] This is based on a January estimate in Redecentralization: building a robust cryptocurrency developer network by Jake Yocom-Piatt. One speculative view that may push this upper-bound higher is that perhaps the individual(s) behind Satoshi Nakamoto worked closely with financial trading platforms, HFT systems and Merkle trees and thus may have been fintech engineers. If that is the case, if constructing a decentralized blockchain is *merely* engineering a chain of trustless Merkle trees, then there may be up to a thousand people capable of designing the system (and optimizing it for SIMD like SSE2 based on over ten comments like these and this and this). In fact, firms such as Goldman Sachs may have various types of internal proto-blockchains already, (a Merkle tree database), it is just centralized and lacks an anti-spam mechanism such as proof-of-work. And the more trust you want to remove from a system, the longer your proof-of-work mechanism needs to be (and vice versa). I would like to thank Zaki Manian for pointing this out.
[110] Bitcoin Core Maintainer: Wladimir van der Laan by Gavin Andresen
[111] Bitcoin Core Development Falling Behind, Warns BitcoinJ's Mike Hearn from *CoinDesk*
[112] Unilateral Statement Regarding Mt. Goxfrom an Insider by Jesse Powell. Powell has a very interesting backstory, who, along with other early adopters like Andrew White, attempted to build services and utility to the

network whereas they would have likely made higher returns (via opportunity costs) if they had merely held onto the tokens and free-rode instead. See The Early Days of Bitcoin from *Priceonomics*

[113] This is not to say that altruism and charity cannot or will not succeed in developing the ecosystem further, rather this is a description of how the process is currently being done.

[114] See The private provision of public goods via dominant assurance contracts by Alexander Tabarrok. In addition, one reviewer noted that Bitcoin has not yet picked up as much corporate support as, for example, the Linux kernel, that may be because the core functionality works pretty well and does not have the constant churn of a project like a kernel.

[115] The Linux development process, funding and housing core development within a non-profit foundation sponsored by companies that utilize the code has been the use-case cited for emulating. There are similar governance constraints and free-rider issues in both, yet they diverge in several areas, most notably kernel churn. The opposite of a free-rider is a forced-rider, see Public Goods by Tyler Cowen

[116] One notable piece outside of academia is Markets, Institutions and Currencies – A New Method of Social Incentivization by Vitalik Buterin

[117] Coinometrics

[118] Based on personal correspondence, March 26, 2014. See The difficulties in creating an incentive compatible decentralised payment network: A study of Bitcoin (forthcoming) by Jonathan Levin.

[119] See Auroracoin - Forked and Game Over on Bitcoin Talk and comments on *Hacker News*

[120] It should be noted that only if that size cannot meet all current demand, which is not the case today.

[121] The Bitcoin mining game by Nicolas Houy

[122] The need for efficiency has understandably led to the rise of professionally managed data centers. See Cloud Hashing CEO on Hardware, Network Growth and the Threat of Pools from *CoinDesk*

[123] For balance, not everyone would agree with this conclusion. For instance, Taariq Lewis has provided feedback to this paper and independently came to a different conclusion last year, see Is there a reason why miners should respect the default maximum block size?

[124] Over the past month there have been several mining pools accused of pursuing this nonce-only hashing method. Some interesting discussions have taken place in the following three reddit threads: 80.241.217.46 mining 18 blocks today containing mostly 1 -> 64 -> -128 -> 256 -> 512 transactions, Why Do All the Blocks Hashed by "Unknown" Miners Have a Binary Number of Transactions (64, 128, 256, etc) and Discus Fish mines a zero transaction block. Another name for Discus Fish is F2Pool and it is based in China.

[125] I would like to thank Jonathan Levin for clarifying this issue for me. These ideas will be further discussed in The difficulties in creating an incentive compatible decentralised payment network: A study of Bitcoin (forthcoming) by Jonathan Levin.

[126] Back-of-the-envelope calculations for marginal cost of transactions by Gavin Andresen

[127] Thanks to Jonathan Levin for pointing out this metric. Readers may be interested in the Network Ranking comparison table at Coinometrics

[128] Bitcoin, Ethereum and Pigou: the economics of transaction fees by Robert Sams

[129] One relevant analysis of network propagation is Information Propagation in the Bitcoin Network by Christian Decker and Roger Wattenhofer

[130] One reviewer noted that Sams' model may not be holistic, "The number of orphans are a kind of social cost on the network due to the lost time that some miners expend in creating these blocks. However it might be in the private interest of some miners."

[131] On Transaction Fees, And The Fallacy of Market-Based Solutions by Vitalik Buterin

[132] In Chapter 3 of *Great Chain of Numbers* I briefly mention the mining, forging and consensus method of several other platforms including NXT and Ripple. Ethereum has not settled on a specific mechanism yet (may be a hybrid between proof-of-work and proof-of-stake like Peercoin and may have some kind of "smart fees" algorithm). Peercoin use a hybrid method with its 1% minting incentive offset by a fixed 0.01 destructive transaction fee.

[133] The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries by Joshua Kroll, Ian Davey & Edward Felten

[134] Mike Hearn on Coming Bitcoin Protocol Updates from *Money & Tech*

[135] Jonathan Levin briefly touched on some of these issues at Coinsummit (video)

[136] (PDF) of the news release.

[137] While agent-based modeling uses heterogeneous time preferences, one reviewer wrote, "On the fact that all nodes need to process all transactions, I think to focus on this as a public goods problem is going to miss the point in actually incentivizing individual agents to carry this out. The hypothesis that the private costs are really absent is what can then be consider the commons."
[138] See Agent-Based Modeling of Peer-to-Peer Economic Systems: Exploring Crypto-economic Stability in the Bitcoin Market (forthcoming) by Dave Babbitt
[139] 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.
[140] One reviewer mentioned that this is a *non sequitur*, that because it is hardcoded, it will always be 10-minutes. However, as noted throughout the manuscript, in order to ever change this block time to compete as an RTGS you would need a hard fork to another codebase. If that code changed the block rewards, it could have adverse effects on the incentives to mine. Thus, while it is possible to change the block timing intervals to 1 minute or 30 seconds, not only would seigniorage issues need to be considered but it may have scaling issues that alts such as GeistGeld had (many orphans). See also FastCoin5, Proof-of-Stake and Ripple-like protocols.
[141] See Episode 99 of *Let's Talk Bitcoin*. Adam Back and Austin Hill have a potential solution to this issue and several other hurdles discussed in the paper. Back also describes more of the process in this thread on reddit.
[142] Chart via: https://blockchain.info/charts/hash-rate and for more mining pool, network, and exchange analysis see, Neighbourhood Pool Watch Bitcoin
[143] The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries by Joshua Kroll, Ian Davey & Edward Felten
[144] Apart from academic papers on whether or not cryptocurrencies such as bitcoin are actual "money," probably the second largest grouping of papers published are related to 51% attacks. The network is arguably no more secure today than it was a year ago, perhaps even less so due to centralization of known physical nodes.
[145] Mt. Gox files for bankruptcy, hit with lawsuit from *Reuters* and Chinese Bitcoin Exchanges Prepare to Move Operations Overseas from *CoinDesk*
[146] Bitcoin Mining Boom Sputters as Prospectors Face Cash Losses by Olag Kharif
[147] Bitcoin and the Three Laws of Robotics by Stan Larimer: "Bitcoins can be viewed as a small "share" of the total market cap of the Bitcoin "corporation". The "mining" services that validate transactions and secure the network are paid for in new bitcoins that slowly dilute the "stock" as the corporation's market cap ebbs and flows. You can generally trade your shares for other currencies, goods, and services. Operating rules for the corporation cannot be changed unless a majority of stakeholders vote for them by switching to another version of the software. Interestingly, it is not the holders of existing shares that get to make this decision, but only those "employees" who are contributing their computer resources (mining bots) to run the company. Nothing says a corporation can't be structured to distribute voting rights this way, and that's exactly what Bitcoin has done. Shareholders get equity growth. Employees get voting rights. All "revenue" is paid to the employees as compensation for their work. There are no profits."
[148] An early concept of a larger voting-based system built on a DAO is the Bitcongress Foundation. Furthermore, David Johnston of the Mastercoin Foundation articulated this same software development centralization problem in a January 24, 2014 interview, episode 80 – Beyond Bitcoin Uncut from *Let's Talk Bitcoin*. See also DAC Index
[149] Vitalik Buterin labels it a prototype, stating: "As *Let's Talk Bitcoin's* Daniel Larmier pointed out in his own exploration on this concept, in a sense Bitcoin itself can be thought of as a very early prototype of exactly such a thing. Bitcoin has 21 million shares, and these shares are owned by what can be considered Bitcoin's shareholders. It has employees, and it has a protocol for paying them: 25 BTC to one random member of the workforce roughly every ten minutes. It even has its own marketing department, to a large extent made up of the shareholders themselves. However, it is also very limited. It knows almost nothing about the world except for the current time, it has no way of changing any aspect of its function aside from the difficulty, and it does not actually *do* anything per se; it simply exists, and leaves it up to the world to recognize it. The question is: can we do better?"
[150] If owning a ledger unit (a bitcoin) is the equivalent to owning a share of stock, is there a scenario in which Bob is liable for violating insider trading? That is to say, if Bob is told by Alice who works on the core development protocol that the core development team will announce a new feature (or not release an expected feature), and takes a long or short position, is Bob liable for violating securities regulations? If as Daniel Larimer and others suggests, bitcoin is a real "security" or "share," what legal ramifications does that entail?

[151] Richard Feynman first popularized this superficial hand-waving phrase 40-years ago through his memorable lecture, Cargo Cult Science. The name is derived from the actions of a South Pacific tribe located on the island of Tanna in Vanuatu. See In John They Trust from *Smithsonian* and Cargo Cult in Port Moresby (video)

[152] See The Shareholder vs. Stakeholder Debate reconsidered by Rüdiger W. Waldkirch and How to Bureaucratize the Corporate World by Ben O'Neill

[153] Some of these governance issues are discussed in The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries by Joshua Kroll, Ian Davey & Edward Felten

[154] Despite the enthusiasm, competence and funding, the likelihood of success is not a given for any startup. And after years of experimentation there are several ways to try and mitigate and plan around known issues of founding a new company. See Death and startups: Most startups croak 20 months after their last funding round from *Venture Beat*, The Venture Capital Secret: 3 Out of 4 Start-Ups Fail from *The Wall Street Journal*, Fighting co-founders doom startups from *CNN|Money*, Why Small Businesses Fail: SBA from *About.com* and How Many New Businesses Fail in the First Year? from *eHow*

[155] 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

[156] JP Koning discusses these *moneyness* aspects including capital accumulation at Moneyness

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

[158] These comments were later removed from the forum. The thread involved was Re: [ANN][XCP] Counterparty Protocol, Client and Coin (built on Bitcoin) - Official and An Open Letter and Plea to the Bitcoin Core Development Team from Counterparty

[159] Developers Battle Over Bitcoin Block Chain from *CoinDesk* and reddit comments

[160] One reviewer noted that "suppose Counterparty and other systems take off and there is a million transactions; Bitcoin is at a cumulative total of 36m transactions ever (stats) so that it is even more popular. Then 80 bytes + average transaction size of 1kb * 1m = 1.08k * 1m = 1GB, which costs $1/30^{th}$ of a dollar in storage space (as seen in Forre.st storage analysis), which for any mining pool is trivial (they do not need it to hash a prospective block), trivial for any developer with their own blockchain, and even over the 10,000 active nodes is a small sum."

[161] While now relegated to historical minutiae there is no "master" key to the protocol, there is an alert key. See What is the Alert system in the bitcoin protocol? How does it work? from StackExchange

[162] There are actually four groups that ultimately provide "consensus": miners, holders of tokens (anyone with a wallet), merchants and web-based services such as exchanges. While miners are usually considered the most powerful (because without them, there would be no network, ledger or authentication) each of these other groups hold some sway. Without exchanges, many participants would be unable to trade bitcoin for fiat or other alt tokens. Without merchants, many participants would be unable to trade bitcoin for goods and services.

[163] An Introduction to BIP70 by Kevin Greene

[164] The Fifth Protocol by Naval Ravikant

[165] This comment has since been removed from the forum.

[166] Similar to the quote attributed to Henry Kissinger: "Who do I call if I want to call Europe?" See Kissinger says calling Europe quote not likely his from *Businessweek*

[167] If all pool operators were contactable, does not petitioning their opinion and vote amount to little more than politics, which was one of the advantages Bitcoin purportedly has over traditional monetary systems involving the need to lobby certain policy makers? Furthermore if centralization continues, issues surrounding cartelization, collusion and rent-seeking behavior could become a factor (i.e., with barriers to entry because transaction fees are decided by miners, they may have an incentive to collude instead of "compete" as they did regarding seigniorage).

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

[169] Image and data via: Re: [ANN][XCP] Counterparty Protocol, Client and Coin (built on Bitcoin) - Official

[170] From Chapter 3, *Great Chain of Numbers*. Note that Counterparty will likely become Turing complete as well (they will probably use Vitalik Buterin's library). They are working on it and will release it on testnet first. Many thanks to Taariq Lewis for his feedback and pointing this out.

[171] Interestingly enough, one of the typical "first uses" of smart contracts utilizing the Bitcoin protocol is in fact, assurance contracts which Mike Hearn has described in detail in a variety of venues including at the Bitcoin 2012 London conference (video).
[172] Blockchain address: http://blockchain.info/address/1EXoDusjGwvnjZUyKkxZ4UHEf77z6A5S4P
[173] Backed by $5 Million in Funding (4,700 BTC), Mastercoin Is Building a Flexible, New Layer of Money on Bitcoin from *MarketWired*
[174] See I burned BTC through blockchain.info, how do I access my XCP? from Counterparty.co and the exact address was 1CounterpartyXXXXXXXXXXXXXXXUWLpVr. On the first day a user would receive 1500 XCP for 1 BTC. By the end of the fundraiser, it was 1000 XCP for 1 BTC. Ultimately 2,648,756 XCP were created in total.
[175] Bitcoin Series 24: The Mega-Master BlockchainList by Antonis Polemitis from Ledra Capital
[176] LTBCoin's utility bridges the user-created asset category as well as crowdequity. It could potentially be used as an "app-coin" as well.
[177] From Chapter 7 in *Great Chain of Numbers*
[178] Visa uses an externality model. For more on the study of Information Security see Pricing Security by Camp & Wolfram, Why Information Security is Hard -- An Economic Perspective by Ross Anderson, Measuring the Costs of Retail Payment Methods by Hayashi & Keeton
[179] The most popular end-user Linux distributions are... from *ZDNet*
[180] QixCoin is purportedly the first Turing complete peer to peer currency platform. See also 25-second irreversible confirmations for instant payments by Sergio Lerner
[181] NimbleCoin is a "2.0" next generation platform that uses an ASIC unfriendly-PoW mining algorithm and has a Turing complete scripting language.
[182] Original thread: [ANNOUNCE] New alternate cryptocurrency - Geist Geld at Bitcoin Talk forum. Charlie Lee's Litecoin presentation at BTC Miami Conference has some interesting notes about early altcoins (video) (slides)
[183] Another problem with very fast block times for proof-of-work systems is that even if they were lowered to 5 seconds, putting it on par with an RTGS, the network is the whole network is not even aware of blocks within 5 seconds. Even with smaller block sizes orphan rates will likely go up which in turn could lead to higher requirements on transaction fees.
[184] Lee's proposal was made on a Dogecoin reddit thread; see also Charlie Lee Proposes Merged Mining of Litecoin and Dogecoin from *CoinDesk*
[185] For an explanation see Economic profit vs accounting profit from Khan Academy
[186] The difficulty rate is not an externality like tech improvement but a derivative of the current (or two weeks prior) supply of hashing power. In the long run, electricity will be globally arbitraged to regions with the cheapest electricity rates (in addition to private property ownership). While imperfect, one analogue is actual gold mining as it also involves capital expenditures and mines are opened and closed based on the market price fluctuations. Yet it could take some months to shift your operations and may not be that obvious or profitable to do it continuously thus 'time preference' is another related variable.
[187] Proofofexistence and BTProof
[188] Personal correspondence, March 23, 2014
[189] Munibit is described in Chapter 8 of *Great Chain of Numbers*
[190] Based on personal correspondence, March 25, 2014
[191] Subledger
[192] I would like to thank Andrew Miller for his feedback related to the incentives being overlooked and how they all can be overcome. It will likely be many years before more of these hurdles become readily apparent.
[193] Vitalik Buterin has a thought provoking article discussing some of the motivations for creating altcoins including experimentation with faster confirmation times, see The Altcoin Debate Continues
[194] My thanks to Taariq Lewis for pointing this out in a recent reddit thread.
[195] One reviewer mentioned that one hypothetical scenario is one in which Visa is vulnerable to something blockchains are not. But aside from physical issues (such as a war or terrorist attack), this is not likely as Visa's data centers are actually spread around globally. Furthermore their actual network is so difficult to attack (since keys expire in less than 3 seconds) that it is much more profitable to merely exploit the edges of the network, vendors and merchants with security vulnerabilities such as Target. Furthermore, if projects like Ethereum make it profitable to once again mine with laptops, botnets will likely come back into the game as they did with pre-FPGA Bitcoin.