

The
ANATOMY
of a Money-like
Informational Commodity:



A STUDY OF BITCOIN

TIM SWANSON

The Anatomy of a Money-like Informational Commodity: A Study of Bitcoin

By Tim Swanson

© Copyright 2014 by Tim Swanson

Cover art credit: Matt Thomas and Invisible Order

This manuscript is released under the Creative Commons - Attribution 4.0 International license: to copy, transmit, share, adapt, remix, make commercial use of and freely distribute this work.



Table of Contents

Preface	4
Acknowledgements	5
Introduction	6
Chapter 1: Bitcoin in theory and practice	9
Chapter 2: Public goods	24
Chapter 3: The Red Queen of Mining	40
Chapter 4: A Bitcoin Gap	78
Chapter 5: Bitcoins made in China	91
Chapter 6: Living in a trusted, post-51% world	105
Chapter 7: Network effects	117
Chapter 8: TCIPcoin and User Adoption	122
Chapter 9: Deflation in theory and practice	137
Chapter 10: Bitcoin's command economy and knock-on effects	163
Chapter 11: Zero-sum Entrepreneurship	176
Chapter 12: Token movements and token safety	188
Chapter 13: Social engineering and groupthink	208
Chapter 14: Separating activity from growth on Bitcoin's network	224
Chapter 15: What Altplatforms can teach Bitcoin	236
Chapter 16: Potential alternatives and solutions	250
Chapter 17: Legal specialization	267
Chapter 18: Conclusions	281
About the author	285
Endnotes	286

Preface

This book is a compilation of research I have written and presented over the past four months, revised, updated and corrected relative to the original source material.

The purpose of this manuscript is to continue the dialogue on issues that are increasingly important to the direction of cryptoprotocols, specifically Bitcoin, and decentralized applications in the near future.

This book is divided into three sections. The first third describes the current state of software and hardware development. The middle portion reflects on the economic conditions within the Bitcoin network as well as user adoption. The last third covers alternative platforms and legal considerations that could impact the on-boarding of users onto the Bitcoin network. While there is some repetition and overlapping throughout the following chapters the redundancy is necessary as this field of study is simply put: hard.

Tim Swanson

San Francisco, August 2014

Acknowledgements

I would like to thank the following people for providing encouragement, feedback, constructive criticism, contrarian views and anecdotes over the past several months:

Cal Abel, Derek Au, Dave Babbitt, Kevin Barnett, Isaac Bergman, Gwern Branwen, Austin Brister, Richard Brown, Oliver Bruce, Anton Bolotinsky, Vitalik Buterin, Preston Byrne, Hudson Cashdan, DC, Joseph Chow, Ben Coleman, Nicolas Courtois, Zavain Dar, Wendell Davis, Robby Dermody, Mark DeWeaver, Ray Dillinger, Tom Ding, John Dreyzehner, James Duchenne, Dan Forster, Byron Gibson, Philipp Gühring, Brian Hanley, Martin Harrigan, Marshall Hayner, Alexander Hirner, Karl Holmqvist, Ron Hose, Petri Kajander, Zennon Kapron, CukeKing, John Komkov, Andrew Lapp, Sergio Lerner, Jonathan Levin, Adam Levine, Matt Lewis, Taariq Lewis, Adam Marsh, Andrew Mackenzie, Andrew Miller, Alex Mizrahi, Pamela Morgan, Massimo Morini, Marco Montes Neri, PN, Pieter Nooren, Dan O'Prey, Ryan Orr, Jackson Palmer, Andrew Poelstra, Antonis Polemitis, John Ratcliff, Robert Sams, David Shin, Greg Simon, Peter Surda, Koen Swinkels, Ryan Terribilini, Peter Todd, Eddy Travia, Chris Turlica, Bryan Vu, Jack Wang, Dominic Williams, Andrew White, Yanli Xiao, Joshua Zeidner and Weiwu Zhang.

Throughout the book I refer to their insights. This is not an explicit endorsement of their opinions or services but rather serves as an on-the-ground reference point. Nor by providing me with quotes do they endorse this book or my opinions. Furthermore, in the interest of financial disclosure, I do not currently have any equity positions in the firms or companies discussed throughout, nor was I provided any financial compensation for the inclusion of companies or projects. This book was entirely self-funded; no government, organization, company, institution or individual provided financial compensation or remuneration for the creation or direction of its content.

Introduction

My title comes from a paper, *Bitcoin: a Money-like Informational Commodity*, by Jan Bergstra and Peter Weijland who attempted to classify Bitcoin through an ontological analysis, showing that it is not even “near money” only “money-like.” The paper analyzed existing literature and clarifies why we cannot technically call Bitcoin the various things it is now popularly labeled – such as a “cryptocurrency.”

More specifically, Bergstra and Weijland mention the disadvantage of calling Bitcoin a Candidate cryptocurrency (CCC) is that “there is no known procedure for leaving the candidate status.”¹ However in a recently published paper, *Formalising the Bitcoin protocol: Making it a bit better*, W.J.B. Beukema claims that by specifying the protocol in mCRL2 (a formal specification language used for modelling concurrent protocols) and verifying that it “satisfies a number of requirements under various scenarios” we have just such a procedure:²

These findings contribute to the position of Bitcoin as a (crypto)currency, as we have to some extent proven that Bitcoin satisfies properties it should at least have in order to be safe to be used as currency.

According to Dave Babbitt, a Predictive Analytics graduate student at Northwestern University, “it sounds like there is sufficient justification to call Bitcoin a crypto-currency, right?”³ The problem with that, according to Bergstra and Weijland, is that confirming its status ‘depends on a plurality of observers, some of whom may require that a certain acceptance or usage must have been arrived at’ before it can be classified as such:

Upon its inception Bitcoin did not possess that level of acceptance, and for that reason Bitcoin has not started its existence as a cryptocurrency. Being a cryptocurrency is a status that a system may or may not acquire over time. Assuming that Bitcoin is considered to be a cryptocurrency at some stage then there will most likely be variations (alternative designs and systems) of Bitcoin around (perhaps hardly used any more) which have not been that successful. Such alternative systems should be given the same type, so that Bitcoin might be considered a successful instance of that type. Clearly CC cannot be that type as it contains only systems that have already become successful to a significant extent. Because being a cryptocurrency is the primary success criterion for Bitcoin its classification as a cryptocurrency amounts to a value judgment or a quality assessment rather than as an initial type.

Thus in line with Babbitt’s reasoning, it is okay to assess the quality of Bitcoin as that of a cryptocurrency, but initially it was something else. And that something is a Money-Like Informational Commodity (MLIC) – viewing Bitcoin as a system providing a platform offering the following features:

1. a system for giving agents access, and

2. facilitating the exchange of that access, to
3. informationally given amounts measured in BTC (the unit of Bitcoin), through
4. the scarce resource of collections of accessible (to the agents) secret keys, and
5. a bitcoin as a unit of access within this system.

In his view, “we can see that bitcoins were initially ‘a commodity, the substance of which consists of information that is independent of any accidental carrier of it, while access to it is scarce’ and only later were valued as cryptocurrency.”

User behavior may change but based on their analysis and existing behavior seen on the blockchain, bitcoins are probably most appropriately called a money-like informational commodity.

As the following chapters will detail, competing special interest groups and stakeholders continually tug at several public goods – such as the underlying core blockchain development within Bitcoin – to move it into a direction that intersects with their goals and agendas. While stalemates do occur, at some point a compromise is reached and the same process repeats, often overlapping with other developmental threads.

Today Bitcoin (the network and the token) is primarily used for goods and services that existing systems such as credit cards and fiat money have limited accessibility for. Yet it is important to distinguish between what a bitcoin (the token) is and is not. As explored below in length, bitcoins do not create value, they merely store it. In contrast, entrepreneurs and companies create value. They do this by selling securitized equity (stocks) in exchange for capital, whereupon they reinvest this towards additional utility creation. As it lacks equity, governance or any formal or informal method of feedback, Bitcoin – a static, fragile institution – is not a company which in turn creates public goods problems.

Other areas this report covers include the cost of maintaining the network. The transaction processing equipment (miners) have no cost advantage over existing value transaction infrastructure, rather Bitcoin’s initial competitive advantage was decentralizing trust and obscuring identities – both of which are progressively compromised. Acquiring and maintaining hashing machines, electricity and bandwidth have real costs – and nothing inherent to the Bitcoin transactional process gives it a significant cost advantage over existing electronic payment systems. Rather, as noted below, the relatively higher costs of doing business (the cost structure) of incumbent platforms and other non-decentralized systems is typically related towards compliance costs which Bitcoin-related enterprises are increasingly having to shoulder. BitLicenses, for example, add additional financial requirements to companies in this space and incidentally could in fact insulate Bitcoin from alternative competitive protocols and ledgers whom lack the capital resources to compete, thereby ceding it monopoly-like status.

A number of other issues are also covered including the impact these types of decentralized systems may have on the legal profession and consequently numerous lawyers have been consulted to provide their insights into how this type of disruption may occur.

These challenges in turn may explain the wide chasm between interest in Bitcoin and meager adoption rates. In many ways this dearth of adoption is tautological: decentralized networks will only be used by users who need decentralization. Bitcoin, the network, like any transportation network will be used by people who need to use it because it satiates certain needs and not necessarily used by people that early adopters want or wish used it. Consequently, Bitcoin solves some needs, but it is not a Swiss Army knife pain killer with innumerable feature-based check-boxes; it has real limitations that are detailed in each chapter below.

Despite the skepticism and critical analysis of this ecosystem, there are numerous bright spots that are highlighted along the way including portions of the community who look beyond zero-sum activities – beyond day trading or gambling – some of whom are genuinely trying to and likely will create wealth generating businesses.

There is a lot to look forward to but it is also important to be realistic about the ramifications of Bitcoin. It is not a jack-of-all trades nor a panacea for all the worlds' ills. It may solve some issues in niche areas, but it likely cannot do the vast majority of the tasks that its passionate supporters claim it can. In fact, it is being shoe-horned into areas it is not competitive. And this is not for a lack of trying. It is largely due to the underlying microeconomic attributes, incentives and costs within the network itself, many of which were not apparent until the past year or two.

I assume that the reader is familiar with the economic concepts of marginal value as well as a general idea of how a blockchain works.

Chapter 1: Bitcoin in theory and practice

Bitcoin is a nominally decentralized cryptographically controlled ledger released into the public domain via an MIT license in January 2009. 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.⁴ 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 a decentralized ledger called a cryptolledger.⁵

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.⁶ 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 a 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:⁷

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.

It is worth pointing out that despite the claims by some Bitcoin adopters, bitcoin was not the first digitized or cryptographic cash-like system – both Digicash and Beenz were developed a decade prior to the release of the first blockchain. Similarly, fiat or as some advocates prematurely call it “old world currency” has been digitized (electronic) and cryptographically secure on a variety of centralized ledgers for years. In fact, by 1978 all financial institutions in the United States were able to transfer Automated Clearing House (ACH) payments back and forth.⁸

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.⁹ 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.¹⁰ This technique is called public-key encryption and this particular method (ECDSA), has been used by a number of institutions including financial enterprises for over a decade.¹¹¹² 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.

Is the private-key property?

Economics does not have a category of “property,” as it is the study of human actors and scarce resources.¹³ Property is a legally recognized right, a relation between actors, with respect to control rights over given contestable, rivalrous resources.¹⁴ 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.¹⁵ 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.¹⁶ In other words, ownership is conflated with possession in the eyes of the Bitcoin protocol.¹⁷ 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 a block reward, or what economists call seigniorage.¹⁸ Seigniorage is the value of new money created less the cost of creating it.¹⁹ As described later in chapter 3, due to the underlying mechanics of this system, the costs of securing the ledger can be described as the following: the marginal value of securing the ledger unit equals the market value of that ledger unit.²⁰ This is formulated in the equation, $MV=MC$ where M stands for marginal, V stands for value and C stands for cost. This can also be written as $MR=MC$, where the marginal revenue equals the marginal cost (e.g., maximizing profit).²¹

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.²² 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.²³²⁴

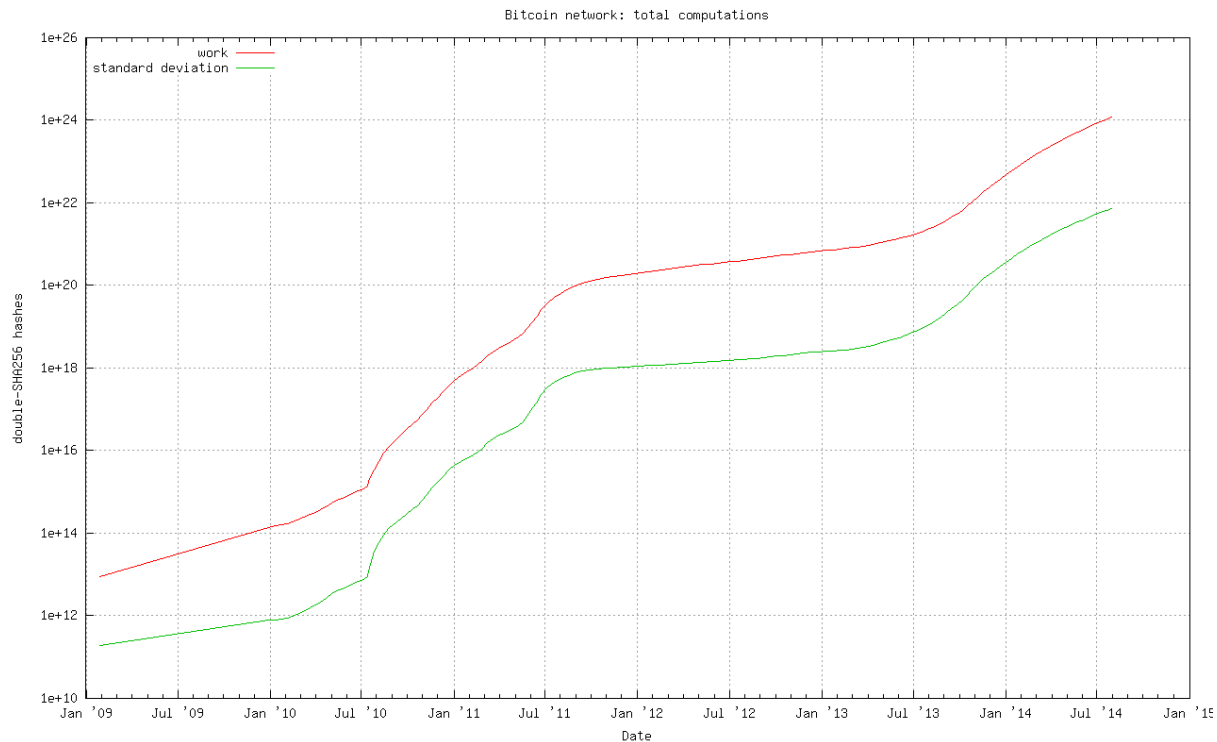


Image credit: Peter Wuille via <http://bitcoin.sipa.be/>

By January 2014, the computational power of the network reached 200 petaflops, roughly 800 times the collective power of the top 500 supercomputers on the globe.²⁵ Though, technically speaking, the Bitcoin mining to supercomputer analogy is not an apples-to-apples comparison because supercomputers are more flexible in their tasks (can do general purpose computations) whereas ASIC mining equipment can only do one task: repeatedly brute force a hash function. On August 1, 2014 the estimated number of hashes of work in the blockchain passed 2^{80} (a number which is used as a barometer for measuring the vulnerabilities of other security systems) and around September 30, 2014 the cumulative number of hashes will reach 2 yottahashes.²⁶ The discussion as to whether or not hashrate is a valid measure of qualitative security is discussed later in this book.

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 of blocks 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”).²⁷ As of this writing, the height of the longest chain has just over 311,000 blocks. 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).²⁸ Approximately every 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.²⁹ 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.³⁰

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.³¹ Every 210,000 blocks (roughly every four years) this amount is split in half; thus today miners are collectively rewarded 25 tokens and by around August 2016 the amount will be 12.5 tokens.³² 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 network itself is located in geographically disparate locations, both the transportation mechanism and processing are 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*	<i>Free and 100% reserve</i>
Transportation	Expensive	Inconvenient	<i>Free & Easy</i>
Security	Physical	Institutional	<i>Cryptographic</i>
Fiduciary media	Inevitable	Inherent	<i>Impossible</i>
Recordkeeping	Manual	Manual	<i>Automatic</i>
Counterfeiting	Impossible	Inevitable	<i>Impossible</i>
Issuance	Mining	Politics	<i>Algorithm</i>
Payment clearing	Expensive	Centralized	<i>Cheap & Distributed</i>
Scarcity	High	Arbitrary	<i>Fixed - 21 million btc</i>
Authentication	Expensive assay	Trust counterparty	<i>Built-in</i>

**fractional reserve banking*

Figure 1: The chart (above) was created Pierre Rochard and frequently appears as an educational tool on a multitude of sites, however it is inaccurate in most categories.

Figure 1 attempts to show the transaction cost advantages a cryptocurrency such as Bitcoin purportedly has over fiat and precious metals, however there should be an asterisk next to many of the categories.³³

While **built-in authentication** is technically true, securing signatures is becoming one of the most expensive parts of Bitcoin due to hacking an 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 multimillion dollar investments including \$40 million by Xapo and \$12 million by BitGo.³⁴

In terms of **storage**, the blockchain currently requires over 25 gigabytes of space.³⁵ In addition to the 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 that is being tackled through a method originally detailed in the Bitcoin whitepaper, called Simplified Payment Verification (SPV). Thus adding new data types such as contract storage to it, 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). With the advent of Colored Coins, metacoins and sidechains, all of whose data is also stored on the blockchain, disproportional rewards will likely be provided to miners creating additional security concerns discussed in chapter 14.

There should also be another asterisk next to **Counterfeiting Precious Metals**. Because of similar densities and therefore weight, gold-coated tungsten bars are a possible way to defeat this.³⁶

In addition, another asterisk should be placed next to **Transportation**, because transporting bitcoins is not free. As Robert Heinlein might note, there is no such thing as a free lunch.³⁷ For example, on-chain Bitcoin transfers are significantly more expensive than traditional credit card transfers, not cheaper. The actual costs of bitcoin transfers are masked by price appreciation and token dilution in the form of scheduled monetary inflation. Though technically speaking, even with its scheduled creation of bitcoin tokens, the currency has mostly deflated, except in its fall from its peak. This is discussed later in several chapters.

For instance, each day, approximately 3,600 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 \$625, bitcoin miners are collectively receiving \$40 per transaction they process.³⁸ This price fluctuates and it should be noted that the marginal costs of adding transactions is almost zero.

Consequently, because neither the storage nor the payment clearing is **cheap**, it is not competitive relative to other platforms such as credit card systems.

In July 2014, Richard Brown explored how the current card payment system works and why Bitcoin is not going to replace it any time soon.³⁹ Unfortunately most Bitcoin advocates are not very familiar with the “chaordic,” as Dee Hock described it. This is the method by which the card issuers and merchant acquirers cooperate, as it is in their best interest to do so. Disrupting this interwoven system with something slower and less consumer friendly such as Bitcoin, is not likely to bring forth mass consumer adoption.⁴⁰ Brown concludes with:

Think about what Visa and Mastercard have achieved: they offer *global acceptance* and *predictable behavior*. Wherever you are in the world, you can be pretty sure *somebody*

will accept your card and you know how it will work and that there is a well-understood process when things go wrong. This offer is powerful. Ask yourself: if you could only take one payment instrument with you on a round-the-world trip, what would it be? If you couldn't stake a stack of dollar bills, I suspect you'd opt for a credit card.

And this predictability – a consequence of the rulebook – is important: consumers enjoy considerable protections when they use a major payment card. They can dispute transactions and, in some countries, their (credit) card issuer is jointly liable for failures of a merchant. Consumers *like* to be nannied... even if they have to pay for the privilege!

So for those who aspire to overturn the incumbents, you need a strategy for how you will become the consumer's "default" or preferred payment mechanism.

American Express has achieved this through a joint strategy of having large corporates mandate its use for business expenses and offering generous loyalty benefits to consumers... they effectively *pay* their customers to use their cards.

PayPal has achieved it through making the payment experience easier – but note, even here, many PayPal payments are fulfilled by a credit card account!

And this is why I harbor doubts about whether Bitcoin will become a mainstream retail payments mechanism, at least in the major markets... why would a consumer prefer it over their card? Perhaps the openness and possible resistance to card suspension/censorship will attract sufficient users. But it's not obvious.

This will be discussed at length later but the key here is once again that actionable incentives ultimately outweigh philosophical rhetoric.⁴¹

Another uncompetitive aspect is that **the cost of Bitcoin transportation and security** incentives via seigniorage is not lower than that of fiat.⁴² The US 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. The US government may have spent more in *absolute* terms than miners spent on operating costs (electricity), but then the outstanding value of fiat is much greater than the 'market cap' of Bitcoin by several orders of magnitude. 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 book, 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. This is discussed at length in chapter 3.

Continuing from the chart above, **static issuance via algorithm** – or inelastic money supply – as we will come to see, is actually a detrimental aspect to the ecosystem and certainly not an advantage.⁴³ And, as detailed in chapter 9, having **100% full reserve** is not a feature, it is a bug that holds and prevents the network from reproducing or creating an actual banking system.

Similarly, the security of digitized fiat currencies are arguably just as secure (via **cryptography**) as cryptocurrencies such as bitcoin; no one steals money off Fedwire or Visa's system, it is the edges of the network that are – even in the world of cryptocurrencies – the most vulnerable.

The **scarcity** of bitcoins, as described in chapter 6 is also arbitrarily set and provided to miners irrespective of the transactional utility they provide to the network which negatively impacts the sustainability of the network. Similarly **counterfeiting** is not impossible just relatively cost prohibitive for marginal attackers.

For instance, in June 2014, L.M. Goodman concisely explained the game theory incentives within the network that make this cost prohibitive:⁴⁴

Part of Bitcoin is indeed math based: its cryptography. Cryptography makes computational guarantees based on widely believed (but not yet proven) mathematical conjectures. For instance, Bitcoin payments rely on signatures which are computed using exponentiation (or multiplication, depending on how you think about it) in an abelian group. Faking those signatures would require solving the discrete logarithm problem in elliptic curve groups, a problem that the mathematical, computer science and cryptographic community considers very unlikely to be solvable efficiently on a classical (non quantum) computer. In this context, “not efficient” does not mean “too costly” or “impractical”, it means that the amount of computing power needed to solve those problems reaches literally astronomical proportions.

However, the cryptography in Bitcoin is the easy part. The safety of the Bitcoin protocol strongly relies on the impracticality of forking the block chain. The assumption made is that miners are incentivized to behave honestly with pecuniary rewards. This makes it costly to attack the system, and even gives a would be attacker an incentive to still behave honestly. This set of incentives is carefully balanced to maintain honesty in the system and avoid conflicts of interests. This really is the heart of the block chain, and it relies on game-theory not mathematics. Yes, game theory is a branch of mathematics, but to call Bitcoin a “math-based currency” because of its reliance on game theory would be like calling plumbing “biology based” since plumbers happen to be biological organisms. There are no mathematical or even computational guarantees, only a set of incentives. This isn't to say that the design of incentives in Bitcoin isn't clever or even artful, but to call the currency math-based, or worse math-backed, is either dishonest or ignorant.

Later in chapter 6 the discussion of mining pool centralization including GHash.io will include further details such as the costs of associated of brute forcing the network which is an illustration of how the network is increasingly less **distributed**.

Laslty, one popular tool that many high-net worth holders of bitcoin use to protect their bitcoins is called a “paper wallet” which is an *ad hoc* type of **fiduciary media**. Thus while Bitcoin is billed as a virtual network, its new money (bitcoin) looks in some ways a lot like “old money” (fiat paper).

Thus altogether the only attributable advantage that Bitcoin appears to have left (based on Rochard’s chart above) is **recordkeeping**, yet there are innumerable types of accounting systems by dozens of vendors that are much more cost effective to implement and maintain.

Paying for decentralization without reaping its benefits

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)⁴⁵

While HyperDex, developed by Sirer *et. al.* and Datomic may have resolved this trifecta, and there is some argument that Bitcoin may have as well, yet the Bitcoin network is not immune to a variety resource constraints.⁴⁶

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 – not to process transactions but to increase their statistical odds of finding a block.⁴⁷ In fact, by October 2010, Satoshi Nakamoto (the protocol designer) himself expressed surprise when he learned of the powerful GPU-based systems that ArtForz and tcatm (Nils Schneider) had created stating, “Seriously? What hardware is that?”⁴⁸

Consequently, as multiple CPU cores were sidelined by GPUs, GPUs were likewise sidelined by field-programmable gate array units (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 application specific integrated circuits (ASICs) – computers specifically designed to do one sole task: brute force a hash function called SHA256d.⁴⁹ 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/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 drive towards efficiency.⁵⁰

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).⁵¹ 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.

While the size and composition of pool operators have changed over the past 5 years, the current composition and distribution of hashrate looks like Figure 2.

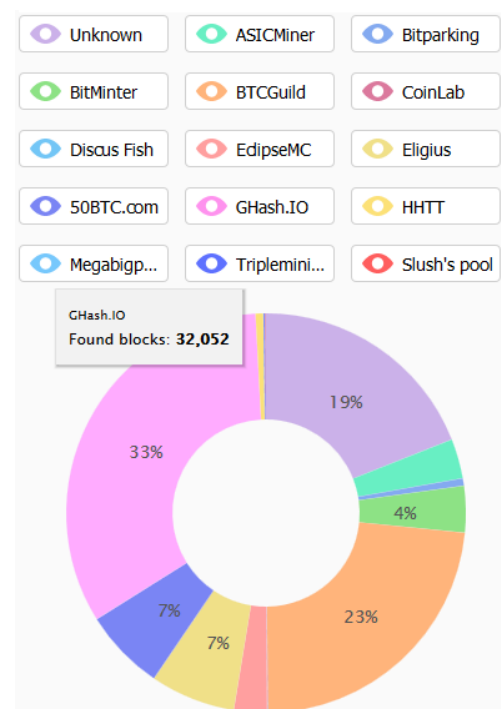
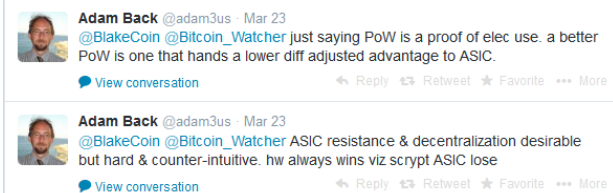


Figure 2: Mining Pools as of August 3, 2014
Source: <http://bitcoinchain.com/pools>

Bitcoin core developer Jeff Garzik has pointed out the ironic nature of this phenomenon on several occasions. In March 2014 he noted:⁵²

The definition of a miner is someone who collects bitcoin transactions into a block, and attempts to produce a nonce value that seals the block into the blockchain.

According to BFL_Josh's off-the-cuff estimate, we have about 12 miners in bitcoin.

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).⁵³ 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.⁵⁴

Another lower cost option that some hobbyists have utilized is purchasing a small USB ASIC miner (e.g., BitFury); however, the problem is that you would need to rely on whatever marginal 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 bitcoin 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).⁵⁶ 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 is integral to a couple new projects including Blockstream as well as PeerNova.⁵⁷

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, most operators have to continually sell their tokens for fiat, to pay for operating and capital costs.

Consequently, once the window of profitable 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. While here 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:⁵⁸

- 1) create a distributed denial of service (DDOS) against competitors, and
- 2) “selfish mine”⁵⁹

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. Token-fiat exchanges such as BTC-e, Huobi and the late Mt. Gox also were under relatively continuous attacks.

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, depressing the price. These hackers will use this time to purchase the tokens and then stop the DDOS, allowing the exchange to come back online, which in turn restores consumer confidence and thereby typically raising the price of the tokens. Another method that has been done in the past with frequency:

Bob the attacker will deposit Bitcoins or fiat onto an exchange. They will exchange bitcoins for fiat 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 money supply manipulation.

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 non-profit mining pool, publicly explained that he unilaterally utilized the mining pools resources to conduct a 51% attack against the alt Coiledcoin (attempting to ‘merge mine’) which had just been released.⁶⁰ 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.

Selfish mining

As mentioned above, one potential problem that has arisen over the past 5 years is a form of “cheating” called selfish mining – an attack vector announced by Ittay Eyal and Emin Gun Sirer and most succinctly described by Vitalik Buterin.⁶¹ 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.

It is not clear how to monitor for this because, as we will delve into later, the stochastic process – the variance of block rewards – makes it difficult to distinguish between when a mining pool actually found a block versus intentionally trying to game the system.

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.⁶² 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 mining pools on the Bitcoin network each 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.⁶³ In theory, 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.

Why do fees matter? Why not remove fees altogether?

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

Gavin Andresen was most recently 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.⁶⁴ In his own words:⁶⁵

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.

Andresen highlighted this challenge again in May 2014, noting that rising transaction fees could effectively price poor people out of Bitcoin.⁶⁶ Other 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).⁶⁷ And as block rewards halve every four years, miners will likely charge higher transaction fees to

make up for the loss of income originally provided via seigniorage.⁶⁸ Yet as will be discussed in the following chapters, it is unlikely that these fees alone – a fee structure which currently enables free-riding – will suffice in incentivizing the labor force (miners) to continue securing the network.⁶⁹

This specific issue again, illustrates the difference between a theoretical public good and how it is treated in practice. The purported abuse of Bitcoin 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 (e.g., a tragedy of the commons).⁷⁰



Chapter 2 will look into more of the public goods issue inherent to Bitcoin and Bitcoin-like systems.

Chapter 2: Public goods

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. This chapter will discuss several version of public goods within the Bitcoin protocol and ecosystem.

Financial incentives for developers

Despite the fact that the code is open-sourced and has been available for five years, with the possible exceptions of 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 without the assistance of others.⁷¹ 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 the Bitcoin protocol has no unified corporate or organizational sponsor and has no responsibility to reward code contributions, there is no financial incentive to be a core developer. In other words, 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.

Currently there are only five people who are partly funded to work on the Bitcoin protocol: Gavin Andresen, Wladimir van der Laan and Cory Fields who are paid by the Bitcoin Foundation, Jeff Garzik at BitPay and Mike Hearn who spent a portion of his time at Google working on Bitcoin-related efforts. Hearn has actually voiced his concerns several times over the past few months regarding this phenomenon – the dearth of funding despite the hundreds of millions of dollars in value being extracted by portions of the ecosystem.⁷² The internal disputes with what can and cannot go into the core code base, was explained by Hearn in June 2014:⁷³

The only people doing any kind of heavy lifting on the protocol today are people paid by the Bitcoin Foundation. When I say ‘people,’ what I actually mean is Gavin [Andresen]. There are only three people paid by the Foundation to work on bitcoin, code-wise. And of those, Wladimir [van der Laan] and Cory [Fields] refuse to work on the protocol, partly because of the social issues that have come up.

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 works.⁷⁴⁷⁵

This issue was highlighted in a recent report from *Bloomberg* who spoke with several Bitcoin Foundation board members. According to Micky Malka, managing partner at Ribbit Capital,

“We have to find ways that allow more upside for the people who are working on the protocol.”⁷⁶ And Mike Hearn explained that the informal system of part-time volunteers, “is not sustainable. You can’t have an infrastructure held together by chewing gum and sticky tape and people who work evenings and weekends.”

Furthermore, Bitcoin, the network, is not self-perpetuating or self-repairing, if it breaks someone has to fix it.⁷⁷ While it is resilient from certain shocks to a degree, it is not anti-fragile as some proponents claim. In fact, Jeff Garzik pointed this out in mid-July 2014, “Bitcoin is just a machine. It can be bought. Or attacked. Or broken.”⁷⁸ Or as John Normand wryly asked, “who does one call when there is a problem with bitcoin?”⁷⁹ Funding those who have to fix it (the core developers) is another public goods problem.

How to make Bitcoin development profitable enough to incentivize skilled talent to fix bugs? 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.⁸⁰⁸¹ In addition to CrowdCurity, two such systems under development are Eris and Lighthouse (which Mike Hearn is working on) and will be discussed later.⁸²

This also ties in with the existence of altcoins (alts). There are at least two economic reasons for why making and deploying alts will continue into the foreseeable future:

- 1) Scarce labor. The pool of engineers capable of building a blockchain is small but growing. If you have the ability to do so, then it also stands to reason that you would like to be compensated for the work you provide. What this means is that because there is no financial incentive to contribute to Bitcoin, there may be an incentive to profit on making an altcoin or altplatform. Unless you create a company that can hire each and every person capable of learning about building these platforms, there will always be competition and an incentive to make an alt which provides its developer with financial remuneration.
- 2) ASICs. As described in multiple dimensions, ASICs are a depreciating capital good that only have a short time frame, a very small window of opportunity (roughly 6 months) to profitably hash nonces. Once they lose their competitive edge, they must be offloaded and replaced with something more powerful. ASIC owners therefore have an incentive to either sell these to a different party willing to take on the risk of never recovering their capital expenditure, or the owner can turn the ASIC and point it towards a more profitable altcoin or alt platform. Because alt tokens are typically open-sourced, the barrier to entry in terms of creating a simple clone is relatively low, especially with turnkey providers like Coingen or Razorcoin. Thus there is a built-in incentive to eke out the last *util* of capital stock which means a continued cycle of concocting new alts.

Just as holding press conferences to talk down price inflation has historically proven to be a futile task, no amount of ‘jawboning’ will remove these economic incentives. Although the new

sidechains proposal will likely bring mindshare (and market share) back to the Bitcoin platform, unless this company (or others like it) can continually hire an increasingly growing developer pool and simultaneously buy all deprecated ASICs, then alts will continue.

Because of the core incentives, these two issues will reappear multiple times throughout this book.

Two markets and non-sustainability

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.⁸³

One expert who has begun discussing these issues however is Jonathan Levin, a post-graduate student at Oxford and co-founder of Coinometrics.⁸⁴ 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. In a normal market the agent would pay a cost for the provision of the private good. In Bitcoin this is currently masked by the blocks rewards. It is not clear that if the market become more reliant on transaction fees that these would necessarily equate to the efficient level due to the ability to free ride on the public good of a high hashrate.⁸⁵

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). Or in other words, a significant portion of the user base that does not include a fee for their transaction is free-riding off the security paid for by not just via inflation but also by those willing to pay higher fees to miners for quicker access to a block. This is an issue that is described later in chapter 3.

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 is a problem that faces most proof-of-work-based cryptocurrencies including Auroracoin, which underwent a 51% attack on the weekend of March 29, 2014.⁸⁶ That is not currently the case with Bitcoin, however, several mining pools including Deepbit and most recently GHashi.io have achieved larger than 51% of the network hashrate over short time horizons.

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 (currently set at 1 megabyte) whose provision was originally incentivized via seigniorage but will later turn towards transaction fees.⁸⁷ And as noted in the previous section, the current direct 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 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 bitcoins in approximately the year 2020), and transaction fees raise to market levels, there is a possibility that the costs of a transaction will dramatically rise and may push Bitcoin into niches for low volume, high value transactions. Simultaneously, the on-chain network may be nominally 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

In February 2014, Nicolas Houy published a paper that looked at this transaction fee and mining issue in terms of a Nash equilibrium.⁸⁸⁸⁹

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.⁹⁰⁹¹ 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.⁹² 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.

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). That is to say, the block rewards "would have to fall to 2.03 BTC or transactions fees to rise to 0.00123BTC in order for the largest mining pool, GHash.io, to include a positive number of transactions."⁹³ This empirical data set is known and has made some observers, including Gavin Andresen in the past, to hypothesize as to why miners include transactions at all, is it merely out of altruism?⁹⁴

For example, an interview last year, Andrew Miller, a PhD candidate at the University of Maryland explored this issue, stating:⁹⁵

The biggest risk to Bitcoin is that the altruistic model isn't realistic, people aren't mining because they're altruistic, they are doing it for money. So then the risk becomes that the incentives are misaligned and that people will begin cheating each other just out of normally predictable, economically rational behaviour, so that's what I mean by systematically self-destructing, self-crumbling fallacy. If you can make a lot of Bitcoin by harming the Bitcoin network, then you can expect that pretty soon, someone will figure out how to do so.

[...]

It's very possible because of scalability problems that it will become much cheaper not to validate Bitcoin transitions, and at that point, we'll definitely need to realize that we'll have to look at a rational model rather than an altruistic model, because if it starts being too expensive to be altruistic, then nobody's going to be.

In April 2014, another Bitcoin core developer, Mike Hearn, described this challenge, of miners who do not include transactions because it is not as profitable to do so:⁹⁶

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

In his paper, *Creating a decentralised payment network*, Jonathan Levin addresses the conundrum that Houy raises:⁹⁷

Note that in order for us to remain at the equilibrium number of transactions processed, the cost of an individual transaction in Bitcoin terms has to remain constant and hence increase in USD terms. An increase in transaction fees in USD terms may result in fewer transactions being processed on the network. Earlier this year the minimum transaction

fee set by the core development team was debased to account for the price of Bitcoin rising (Hearn 2014). In the future, a debasement in the minimum transaction fee might result in fewer transactions being processed as a result.

The ‘debasement’ that Levin refers to is the decrease in direction transaction fees that developers ‘slashed tenfold’ earlier this year.⁹⁸ Though it bears mentioning that not all pools have updated this software nor do all wallets support this automatically. Users may have to manually change the fee amount and as explored in the next chapter, mining pools may not immediately place low-fee transactions into a block.⁹⁹

Chapter 3 will describe in further detail the mechanics and incentives for centralizing a farm and pool.

Robert Sams, a former hedge fund manager and co-founder of Swiss Coin Group has written on this issue, an issue he dubs a tragedy of the *transaction verification* commons.¹⁰⁰ 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 cost 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. 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.¹⁰¹¹⁰² 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.

Securing information

Since the genesis block there has been between \$1 to \$3 billion worth of capital and operating expenditures related to building the current Bitcoin network. Gil Luria at Wedbush Securities estimates that around \$200 million has been invested, yet the higher limit is more accurate figure as there is an economic law that dictates the costs of mining (as described above as well as later in Chapter 3).¹⁰³

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 transaction fees as some low-fee transactions are left unconfirmed in the mempool for hours). 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 in theory just as secure (or a hybrid of the two), 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.

In the Tezos position paper, L.M. Goodman independently drew similar conclusions:¹⁰⁴

[T]he proof-of-work system puts the miners, not the stakeholders, in charge. Forks for instance require the consent of a majority of the miners. This poses a potential conflict of interest: a majority of miners could decide to hold the blockchain hostage until stakeholders consent to a protocol fork increasing the mining rewards; more generally, they will hold onto the hugely wasteful system that empowers them longer than is economically beneficial for users.

The current narrative suggests that an arbitrary issue that may be limiting wider spread usage of the Bitcoin network as a payment platform is the artificial 7 transactions per second limitation and subsequent confirmation delay.¹⁰⁵

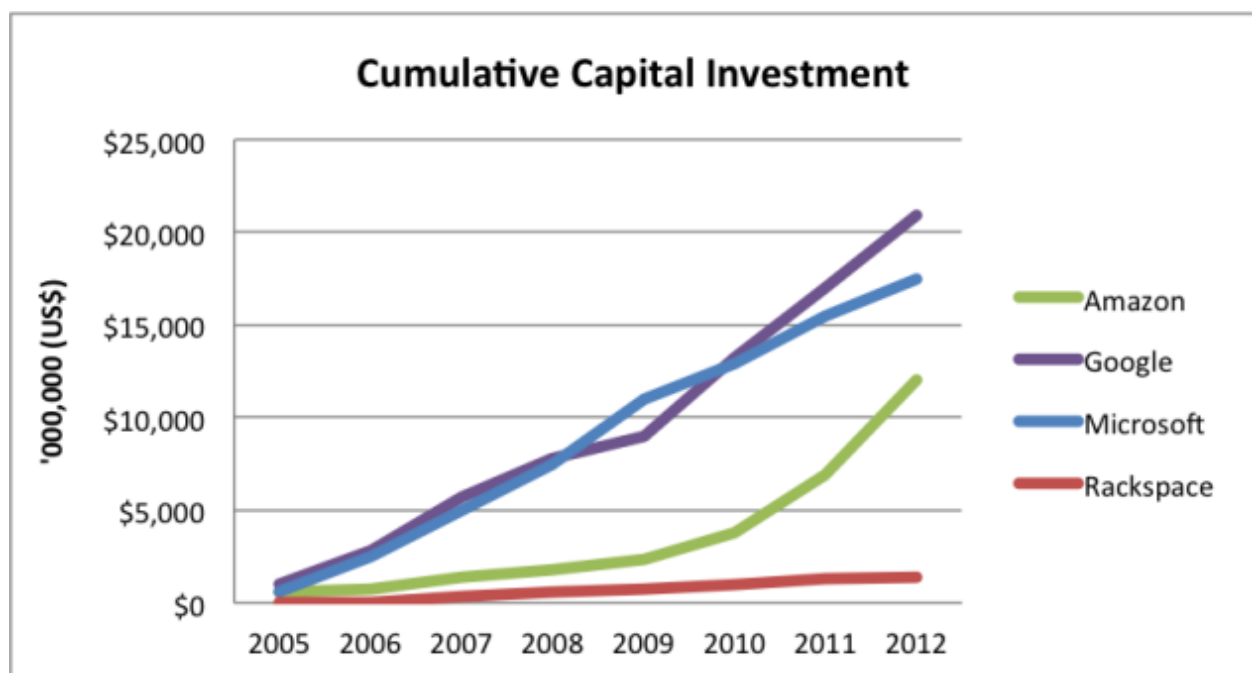
Yet despite the continual mining investments, the Bitcoin network operates at roughly the same performance as it did five years ago, with 10 minute confirmation times. While speculative, if a payment processing company such as Visa spent between \$1 billion and \$3 billion on hardware and yet their overall network performance had not improved, the CTO would arguably be under pressure to resign.¹⁰⁶ Yet there is no such accountability in Bitcoin because it is a public good. There may still be attempted solutions however, as Adam Back and

have proposed a method for capitalizing off this underutilized capacity via merged mining with sidechains in Blockstream involving several other core developers.¹⁰⁷ Yet it bears mentioning that sidechains could introduce other security vulnerabilities and does not (in its current form) lead towards decentralization.¹⁰⁸

While there are hypothetical workarounds to the transactional limit such as Sergio Lerner's proposed DECOR protocol – which when paired with GHOST can potentially reach 2,000 transactions per second, it is doubtful that this alone will on-board real-time gross settlement (RTGS) users because any technological benefit that Bitcoin is privy to, will likely benefit the competition as well.¹⁰⁹

For comparison, last fall, Visa reached 47,000 transactions per second at the Gaithersburg IBM testing facility.¹¹⁰

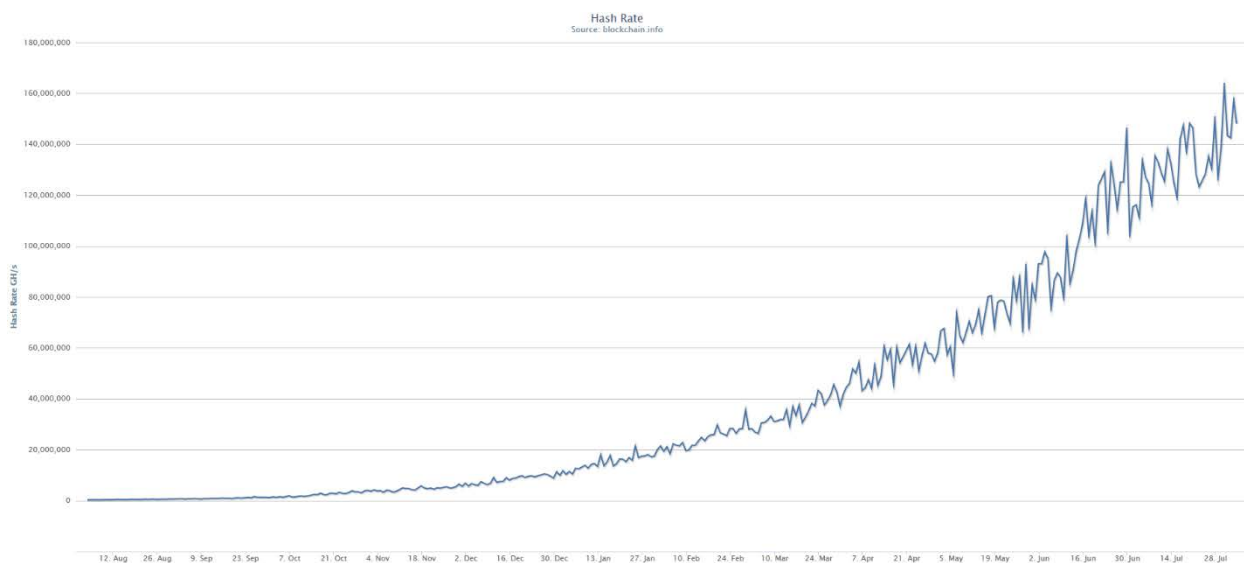
For perspective below is a chart from an August 2013 *Gartner* report illustrating the cumulative capital investment of four technology companies:¹¹¹



This is actually a measure of “the total investment in real and virtual revenue-generating IT assets” and not books or chairs. If the CTOs at these enterprises spent \$1 billion annually on hardware without any measurable gains in underlying performance, they too could face pressure to resign like their hypothetical peer at Visa.

Continuing, L.M. Goodman noted a similar conundrum, that miners upgrading their system does not increase the transaction processing capacity of the network:¹¹²

The race to build more hashing power (by developing ASICs for instance) means that the cost to pull off a 51% attack on the network increases. In this respect, the network is more secure. Note however that the amount of money spent on mining and mining equipment must be approximately equal, in the long run, to the amount of bitcoin paid in transaction fees or created through mining. Given off chain transactions, this could dwindle to very low levels in the future. However, the processing power itself doesn't matter. The only thing that matters is that something expensive is being irreversibly spent, to make it hard to attack the network. Spending money on computing power has the nice property that you can easily prove it online, but the computations themselves are deliberately done on worthless problems. Emphatically, this computational power is not used to validate transactions, an operation which only takes a modest amount of computing power. More hashing power does not mean that the Bitcoin network can process more transactions per second or process them faster.



Above is an image from Blockchain.info which illustrates the total hashrate of the Bitcoin network between two dates:¹¹³

- August 4, 2013: 332,726 GH/s
- August 3, 2014: 148,091,576 GH/s

This is a 445x 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. As discussed later, economists would say that the marginal productivity of labor in Bitcoin is zero. Irrespective of the amount of miners (labor) that are added to the network, no additional output (bitcoins) is created, thus there is no real economic advantage of having more than one miner on the network.

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) or decentralized autonomous corporation (DAC), 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.¹¹⁴¹¹⁵ Yet, since development and direction of the Bitcoin protocol itself is not handled by direct “votes” it is not technically a company.¹¹⁶¹¹⁷

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, believing 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.¹¹⁸



Because some aspects of development have come under the purview of the Bitcoin Foundation, the current Bitcoin ecosystem is a blend between “shareholder” and “stakeholder” system.¹¹⁹ 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, and 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*.

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, and the hashrate. Currently block rewards subsidizes this public service as transaction fees do not cover the cost of maintaining the hashrate. There is a scarce resource, block size, yet 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 highlighted when the halvings of the next block rewards take place – from 25 bitcoins to 12.5 bitcoins in mid-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.¹²⁰

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.¹²¹

While discussing the marginal costs of cryptocurrency production, Robert Sams, co-founder of Swiss Coin Group, notices a similar type of free-riding that is not equivalent to buying gold as some proponents claim:¹²²

The scenario gets worse when we relax the monetarist assumptions (latent in the above analysis) of stable money velocity and demand proportional to tx growth. You don't have to be a Keynesian to see how a large quantity of Bitcoin balances are held for speculative reasons. The high level of coin dormancy in the Bitcoin blockchain is as conclusive empirical evidence of this as there can be.

Bitcoin, therefore, has a free rider problem, whereby speculative coin balances, which benefit from the system's costly hashing rate are effectively subsidised by those who

use bitcoins primarily as a MOE. These speculative balances repay the favour by adding a toxic amount of exchange rate volatility, providing yet another reason for the transaction motive to run away from log coin MOE. As time goes on and the coinbase declines, this inequitable arrangement only gets worse.

An MOE stands for medium of exchange and log coins are at one end of a spectrum that represent the logarithmic money supply protocol. This is discussed later in chapter 9.

Coupled with the lack of incentive to work as a core developer, this situation can be summarized as a socialization of labor and privatization of their gains. Yet simultaneously, holding bitcoins itself, so the argument goes, purportedly helps to develop and market the product (because it increases the price level 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).¹²³ However, as of this writing, empirical evidence has yet to verify this narrative .

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. 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’

FUBU stands for: for us, by us. Many early bitcoin adopters have distinct philosophical views that they would like to have carried over with the mass adoption of bitcoin. One of these is that the Bitcoin network is only to be used for specific types of transactions that follow a specific workflow. Or in other words: use the network for how we, early adopters, want it to be used, not for how it can be used via clever workarounds. Yet, because token ownership and network usage are open to new participation by individuals and companies without those same views and values, an impasse occurs.

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 that will be described at the end of the book. It is a decentralized database of encrypted keys that 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.¹²⁴

The background in a nutshell was that on October 24, 2013, then-lead Bitcoin developer Gavin Andresen announced that in an upcoming patch 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. 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:¹²⁵

- "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 particular interest.¹²⁶

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.¹²⁷ 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 (though Ford actually won a patent infringement suit levied by George Selden).¹²⁸ 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, so the argument goes, is prohibitively difficult because you would need to supposedly overcome network effects.¹²⁹ Or in other words, usage of the code and hashrate is permissionless, yet modifying the code (to provide for transaction inclusions) requires permission. “Permission” required for features that involve protocol change is really the permission of 51% of the network. In addition, while these developers may have significant influence over what version of the code miners accept, ultimately it is the miners that decide.¹³⁰ It also bears mentioning that nodes also have voting power as they choose which software to run and they can reject or accept changes that miners want to accept / reject.

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, 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.¹³¹

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.

In the end Counterparty used a solution that did not involve OP_RETURN and while both camps have moved on since this event, one understated issue going forward will likely need to be addressed to prevent similar problems from occurring in the future: 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.

How to contact mining pools?

During this debate between Counterparty 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 works:

“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?”¹³²

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 hashrate?¹³³ 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 qualitative safety of decentralized proof-of-work systems?¹³⁴

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 and more recently in March 2014 presented by Peter Todd regarding tree chains.¹³⁵ The following chapter will discuss mining in detail.

Chapter 3: The Red Queen of Mining

The discussion over the actual costs of maintaining a decentralized seigniorage network is a new area of research. In practice it appears that the logistical cost of operating the Bitcoin network rises linearly with its total value. More efficient mining gear does not reduce energy use of the Bitcoin network. It only raises the network difficulty. The proof-of-work method used to mitigate rogue attacks, must expend real work, which means it must consume energy.¹³⁶ Consequently, the price of bitcoin reflects its demand which in turn incentivizes hardness, which reflects how much work goes into the proof-of-work scheme, which directly converts into how much energy is being expended. This chapter will discuss these costs at length.

Mining most proof-of-work-based (PoW) cryptocurrencies (such as bitcoin and litecoin) is an increasingly energy intensive operation; the fact that all seigniorage gets burned up from hashing is the essence of crypto scarcity.¹³⁷ Nobody has an incentive to produce additional units of the token without this subsidy. Some commentators seem to think that it is an inherently beneficial phenomenon, that the 'market cap' is greater than the cost of minting the coin. But the fact that $MV > MC$ (marginal value is greater than the marginal cost) is the reason policy makers typically argue that money needs to be a state sanctioned monopoly.¹³⁸ In contrast, private seigniorage incentivizes the production of money until $MV = MC$ (marginal value equals the marginal cost).¹³⁹

On this point, in a response to Tyler Cowen, an economist who has written on competing private cryptocurrencies, Robert Sams explains how the marginal cost of new coins is the cost of hashing a block:¹⁴⁰

This is a long-time objection to the workability of competitive, privately issued fiat currencies. The cost structure of their production cannot be rationalised with their value. A market of competing fiat currencies with "stable" purchasing power will generate too much seigniorage to their issuers, inviting more competition until the purchasing power of these media rationalise their cost of production.

If we can't lean on the economics of network externalities, what's wrong with this argument?

First of all, Cowen speaks of a "cryptocurrency-generating firm" that issues "blocks of cryptocurrency". The idea here seems to be that the marginal costs of creating a crypto coin are close to zero (it's just data after all), most costs being the fixed costs of setting up the cryptocurrency system.

But this has things the wrong way round. Creating a new crypto currency is as easy as forking the Bitcoin source code, hacking it, and throwing the fork up on a code repo. Fixed costs are practically zero. Marginal costs, however, equal the electricity costs (and amortised hardware costs) of solving a new block of transactions, as each new block

contains a mining award for the peer whose hashing finds a solution to the system's hash problem. This is how new coins are created.

Because outputs (blocks) are fixed, the amount of inputs will vary according to profitability forecasts.¹⁴¹ That is to say, economically rational miners will direct their depreciating capital goods towards the most profitable activity, comparing the expected mining award to the variable operating costs (electricity, mostly).¹⁴²

The price level of tokens such as bitcoin are determined by market participants based on supply and demand.¹⁴³ The value of a token serves as a signaling mechanism for miners to either partake in the effort to hash blocks or to redirect their effort towards other more profitable tokens relative to the difficulty rating.

In addition, there is one variable cost that all large scale mining operations must take into account: electrical costs. For the same reason that cloud computing providers such as Facebook, Microsoft and Google have scoured the globe for prime locations based on reliable always-on electricity, settling down in areas like Prineville, Oregon or Wenatchee and Quincy, Washington (whose facilities are powered by the Wanapum Dam) 98% - 99% of the operating costs for large professionally run mining pools boils down to electricity and cooling costs (extracting the heat produced from mining is a real economic cost).¹⁴⁴

This past spring, Andrew Poelstra, a graduate student in Canada, published a paper regarding ASICs and decentralization. In one passage he notes that:¹⁴⁵

[D]edicated hardware brings us closer to the thermodynamic limit, and is therefore eventually a good thing for mining decentralization. Also, because ASIC's produce more hashes for the same amount of energy, they produce stronger proofs-of-work with proportionally less environmental impact.

This is false as it is conflating network difficulty with probability of successful attack. Only capital burned influences the latter.¹⁴⁶¹⁴⁷ The only thing that would cause less environmental impact without affecting security is an increase in the price of electricity which is discussed later. Even at the thermodynamic limit, network difficulty will still fluctuate with the price of electricity and the price of bitcoin. Thus, the difficulty can change but capital spent hashing remains the same (and vice versa). Furthermore, centralization is incentivized due to network propagation constraints, an issue that Jonathan Levin dubs "Hash War 2.0." As a consequence peering agreements now exist among the larger pools, to propagate the blocks faster by removing all of the unnecessary hops and overhead a decentralized network creates.¹⁴⁸¹⁴⁹

Because mining rewards were fixed with the genesis block in 2009 (providing a fixed income on a scheduled time table), and market participants are able to determine the percentage of the overall hashrate at a given time that their mining equipment represents, seemingly simple calculations are required to gauge the potential profitability of their mining activities.¹⁵⁰ In practice however, hash rate calculators are not accurate in the long-run.

Dave Hudson, a network expert and statistician at HashingIt and Vice President of software architecture at PeerNova, explains that:¹⁵¹

Hash rate calculators have a huge problem as a result of the randomness shown by the statistics. All they can do is measure the event rate and make an estimate of the rate, based on the block finding rates. They have no way of telling if the statistics for any given period of time were normal, low, high, very low, very high, etc.

Laborers on the Bitcoin network must account for the capital costs of their hashing equipment, rent for the land, administrative overhead, taxes and increasingly important, the energy costs which can be very specific to their locality, depending on the equipment's geographic location. All of these costs are tallied against an inelastic wage which can only be attained if the hashing equipment they control is able to outcompete other such miners – it is a zero-sum, no honorable mention, game. And it can be scaled.

The Hashrate Wars

This subsequent escalation, dubbed a “hashrate war” (the competitive fight for ever increasing hashing equipment) created a technological S-curve that looks similar to the chart below:¹⁵²

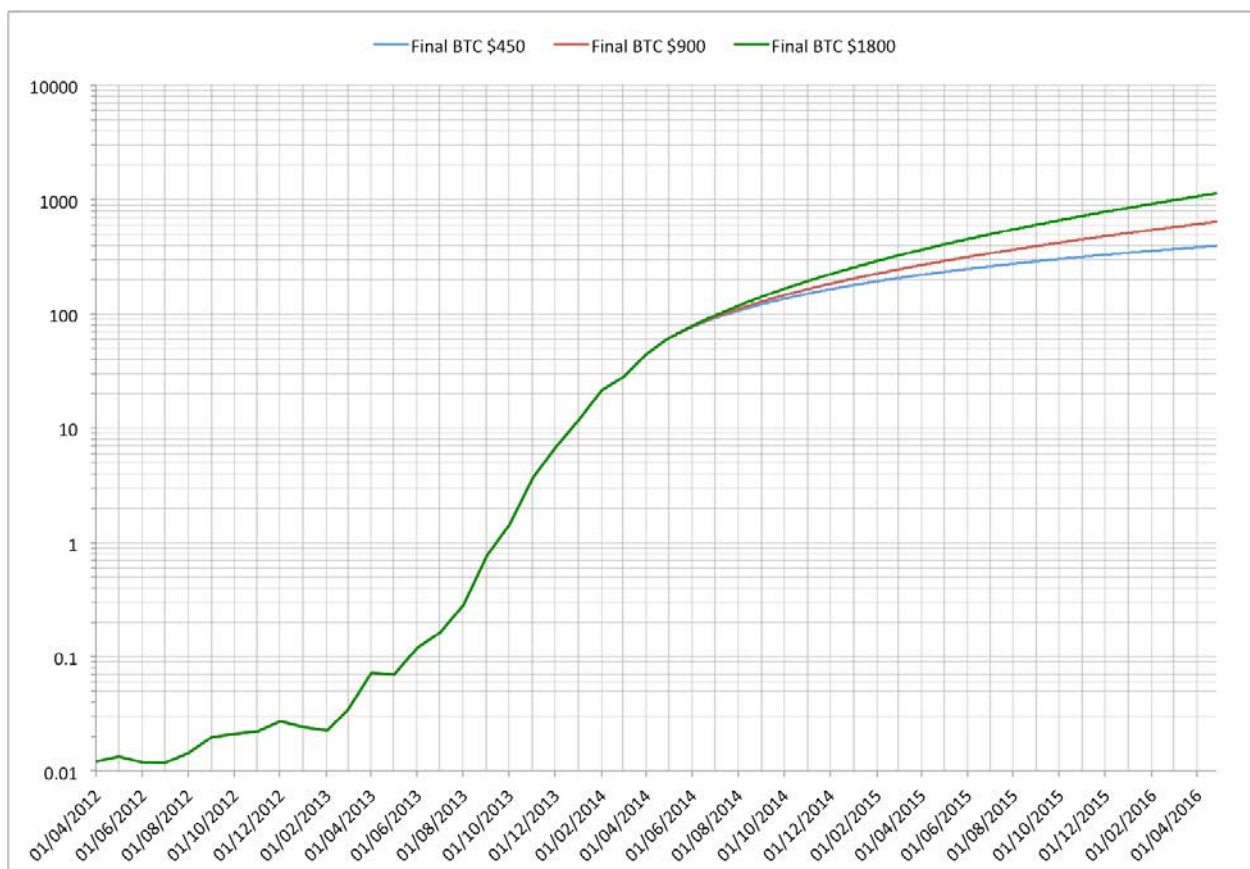


Image credit: Dave Hudson Source: <http://hashingit.com/analysis/24-megawatts-of-mining>

The vertical axis in the chart above is logarithmic and illustrates the hashing rate (showing that it will slow down once ASICs hit fabrication node limitations). The horizontal axis projects two years into the future.

If it continues to taper off at its current rate, the hardware side could potentially become commoditized in the next 3-4 years whereupon a miner's competitive advantage will solely lie in energy arbitrage. Why? Because the jumps in fabrication generations by mining manufacturers have finally caught up with the bleeding edge (20nm at TSMC).

We can see this in the following chart:¹⁵³

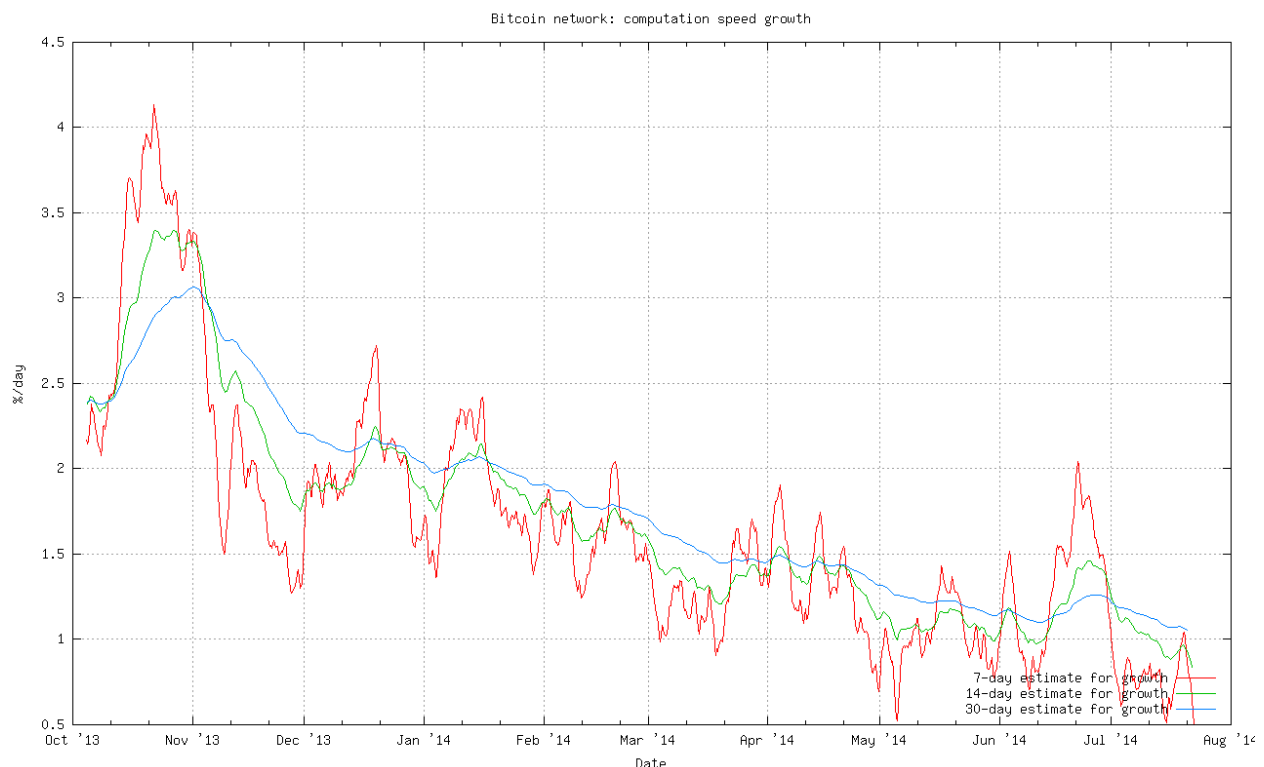


Image source: <http://bitcoin.sipa.be/>

What this illustrates is that the growth in computational speed is declining over time. Part of this is a function of decreased token values during the spring of 2014 but professional farms have also collectively caught up in terms of mining system performance and consequently they revert to the median. In this case that means the industry stabilizes at less than 1% growth day-over-day in network speed.

Throughout the spring and even into June 2014 there was discussion as to whether or not a 2%-3% rate would push the block halving up by several months, from August 2016 into March 2016.¹⁵⁴

Yet according to Dave Hudson, this is not sustainable:¹⁵⁵

“I think it's more like early July [2016]. March isn't even close to possible. What everyone is forgetting is that difficulty changes absorb hashing rate increases amazingly well, especially short term bursts of hash rate. Even with the most steady 1% expansion for the next 23 months we only pull in the date by 90 days, but if we were to see that same 983x increase in hash rate over the next 24 hours then the difficulty would fully absorb it within 2 diff changes and we'd only pull in the date by 4 days.”

Either way, ignoring all of the various issues related to public goods challenges and game theory (such as “selfish mining”), this system may have served the bootstrapping phase but it looks as though it ultimately becomes an environmental white elephant. Satoshi Nakamoto, the pseudonymous creator of the protocol foresaw this noting in the original FAQ that “When Bitcoins start having real exchange value, the competition for coin creation will drive the price of electricity needed for generating a coin close to the value of the coin.”

Thus the relationship between enterprise value and hashing power has been known for some time and will be detailed in full below.

An additional challenge however, presents itself when this seigniorage subsidy is halved, a structural feature of most cryptocurrencies. With Bitcoin, every 4 years (or every 210,000 blocks) the subsidy is reduced by 50%. This is equivalent to the miners – the labor force – being told they would receive a 50% pay cut. While this issue typically remains hidden and muted when token values appreciate and rise, in the long term continual halvings discentivize laborers from providing security and utility to the network. There have been several “cryptocurrencies” whose labor force fled after their profitability period was over – most notably with Auroracoin – and as a consequence the network was left insecure and vulnerable to double-spending attacks (called a 51% attack).

One such popular token that is currently facing this dilemma is Dogecoin, which is losing 20-30% of its security force every 2 months. While there are potential solutions Dogecoin developers could adopt, incorporate or migrate to, because Dogecoin is still relatively young it has the flexibility of moving towards a different security mechanism. This issue has the potential to become systemic – and thus more difficult to address – in other digital currency ecosystems. This is discussed later in chapter 15.

Calculating the costs

As noted in chapter 2, there is no such thing as “free” in bitcoin transactions. Someone pays both in terms of inflation and in transaction costs. Since the genesis block, between \$1 to \$3 billion worth of capital and operating expenses spent towards building and maintain the current Bitcoin network.¹⁵⁶ In fact, the costs may be even higher once botnet externalities are factored in.¹⁵⁷

Chart 1: Estimated lower bound costs

	Bitcoin	Litecoin	Namecoin
Time period	July 18, 2010 - July 18, 2011		
Open & close	\$0.08 - \$13.68 per bitcoin		
Weighted annual value	\$3 per bitcoin		
Money supply added	2,625,000 bitcoins		
Estimated seigniorage	\$7,875,000		
Time period	July 18, 2011 - July 18, 2012	October 11, 2011 - October 11, 2012	
Open & close	\$13.68 - \$8.90 per bitcoin	\$0.00 - \$0.088 per litecoin	
Weighted annual value	\$5 per bitcoin	\$0.02 per litecoin	
Money supply added	2,625,000 bitcoins	10,500,000 litecoins	
Estimated seigniorage	\$13,125,000	\$210,000	
Time period	July 18, 2012 - July 18, 2013	October 11, 2012 - October 11, 2013	October 16, 2012 - October 16, 2013
Open & close	\$8.90 - \$85.51 per bitcoin	\$0.088 - \$1.96 per litecoin	\$0.055 - \$0.458 per namecoin
Weighted annual value	\$50 per bitcoin	\$1.50 per litecoin	\$0.25 per namecoin
Money supply added	1,750,000 bitcoins	10,500,000 litecoins	2,625,000 namecoins
Estimated seigniorage	\$87,500,000	\$15,750,000	\$656,200
Time period	July 18, 2013 - July 18, 2014	October 11, 2013 - July 11, 2014	October 16, 2012 - July 16, 2014
Open & close	\$85.51 - \$619.78 per bitcoin	\$1.96 - \$7.76 per litecoin	\$0.055 - \$1.90 per namecoin
Weighted annual value	\$500 per bitcoin	\$10 per litecoin	\$1.50 per namecoin
Money supply added	1,312,500 bitcoins	7,875,000 litecoins	1,968,750 namecoins
Estimated seigniorage	\$656,250,000	\$78,750,000	\$2,953,125
Total lower bound cost	\$764,750,000	\$94,710,000	\$3,609,325

This view is fully integrated and Chart 1 (above) provides a lower bound estimate of this relationship.¹⁵⁸ The total lower bound cost is an approximation of the aggregate weighted annual value. Thus, all things being equal, \$656,250,000 is the lower bound cost to extract and maintain the Bitcoin network since July 2011. Similarly, approximately \$94,710,000 was spent on infrastructure for Litecoin seigniorage over the past 33 months and \$2,953,125 for Namecoin seigniorage for the past 21 months.

This intersects with a common refrain in Bitcoin public forums during 2014, “\$600 million has been irreversibly spent securing the Bitcoin network.”¹⁵⁹ This does not seem like a particularly positive data point to focus on as virtually all other industries that utilize capital machinery also undergo some form of irreversible capital depreciation. If this was a favorable attribute, marketers at automobile companies would likely be using it in television advertisement, “nearly \$1 billion has been irreversibly spent building an engine for the new Lexus ES350.” But they do not brag in commercials that they burnt \$1 billion in resources and capital (coal, steel, alloys) to build their wares – that would look conceited and vain. Furthermore, the quantity of the funds involved does not necessarily reflect the performance of the engine or the vehicle. Alternative consensus mechanisms such as proof-of-stake or the Ripple protocol purportedly provide roughly the same level of security and trustlessness yet at a fraction of the capital requirements.¹⁶⁰

In an open market, prices serve as signals to market participants to either enter or exit a market. In the case of Bitcoin, the value of the token provides one quantitative signal to miners to either continue hashing or to stop. While there are exceptions to the rational economic actor (*homo economicus*) when it costs more to hash than miners receive, miners will each have to decide whether to continue or not. Because it is a competitive marketplace and because

each mining operation has different economies of scale, marginal players may be purged from the seigniorage market due to their inability to compete when token valuations are lower than the amortization rate of their depreciating capital goods.¹⁶¹

There are at least five exceptions to this rule however:

- hobbyists and researchers
- wishful-thinkers
- botnet operators
- political actors
- individuals looking for “virgin” coinbases

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

Well-wishers notably include an Austrian-based family that *Bloomberg* interviewed in April 2014. Even though the family owned a power plant and also received subsidies from the government, because of the volatility in token prices which have dropped more than a half since their peak in late November 2013, their mining pool was still operating at a net loss.

One of the sons in the family acknowledged these market challenges, concluding that “[i]f you’re mining at this stage, you’re not doing it to make dollars, you’re doing it because you believe it will go up.”¹⁶² In other words, they were hedging their losses in their income statement with future residuals from potential price appreciation.

Yet it would likely be cheaper for this family to simply shut the pool and the power plant off and simply purchase tokens instead, stepping aside as other mining pools with larger operating margins would continue seigniorage. This limitation is typically measured via a discount function $[f(t)]$, which attempts to quantify the expectations and low time preferences of miners. For instance, even if Bob’s operating costs were higher than the block rewards, he might mine today with the expectation that the price increases. As noted above, some miners do not necessarily want or need to sell today, Bob could store 50% of the bitcoin and effectively buys future network security on that price expectation creating temporary additional hashrate overhang.¹⁶³

Botnets are the third and perhaps hardest to qualify or quantify due to their opaque nature yet fine-tuned *modus operandi*. In a sense, botnets are the most rational economic actors because they seek, at the expense of the machine owners, to achieve one sole purpose, mining tokens at the absolute minimum of cost to the beneficiary of these activities.¹⁶⁴ And because both their electricity and capital costs are “free” (appropriated from their legitimate owners), they can and still do scale tens of thousands of highly inefficient hashing systems (desktop and laptop computers) to squeeze out *utils* for their operators and in this case, nonces for bitcoin.

As noted by James Wyke in SophosLabs research, there are unseen damages that botnets cause. In addition to destroying the lifetime cycles of the computers (wearing down the CPU, GPU, hard drive and memory) botnets also consumes bandwidth which, while marginal among a handful of computers, is very large when scaled to 100,000 or more. It also, in the words of Wyke's, "deprives hard-working legitimate Bitcoin miners from generating those coins and therefore receiving payment."¹⁶⁵ Furthermore, there is the cost of electricity which someone must pay for, and the increases in difficulty rating which requires "legitimate" miners to increase their investment in hardware in order to obtain the same return. That is to say, these botnets are artificially inflating the difficulty rating which in turn pushes out marginal, legitimate miners. Until these botnets are removed, they are effectively rent-seeking off the entire ecosystem and distorting the difficulty rating.

And even with the advent of ASICs, this is not an easy problem to solve. In November 2013, E-Sports Entertainment was fined \$1 million USD after an investigation uncovered that an employee had inserted rogue code into an anti-cheating software program used by gamers in CounterStrike competitions.¹⁶⁶ The code would activate the GPUs at night, turning the host machines into a GPU farm that during its short duration, mined a total of 30 bitcoins. Again, while ASICs largely remove this ability for botnets to exist and compete with anything lower than a few million infected systems, the flip side is that massive centralization has taken place within the Bitcoin mining ecosystem, creating potential social engineering vulnerabilities.

While the ZeroAccess botnet mentioned above was declared defeated in mid-December 2013, Symantec published an estimate in October 2013 on these externalities of running the ZeroAccess botnet.¹⁶⁷ Based on 1.9 million infected machines, they projected it generated \$2,165 per day mining bitcoins while using 3,458 MWh/day of energy (one infected computer consumes 1.82 kWh per day). For perspective, this is enough energy to power 111,000 homes each day.¹⁶⁸ This externality has not been factored into the seigniorage chart above. And it was not the only botnet as others such as Trojan.badminer and Ulfasoft from the TDSS rootkit could be used to generate tens of thousands of dollars each month in ill-gotten gains, which was not accounted for in Figure 1.¹⁶⁹

All told, according to research published in *Botcoin: Monetizing Stolen Cycles*, as of August 2013 they had identified more than 2,000 executables that connect to mining pools to mine bitcoins; 74% of which connected to public pools, the remainder connecting to private (dark) mining pools.¹⁷⁰ This same research found that another large botnet, DLoad.asia had amassed more than 100,000 computer drones between 2011 through 2012 and received at least 10,000 bitcoins during that time frame.

Although ASICs have largely made even large botnets uncompetitive, malware operators still continue to use them, sometimes targeting altcoins with lower difficulty thresholds.¹⁷¹¹⁷² In fact, in July 2014, Facebook broke up "Lecpetex," a 250,000 computer botnet which functioned both as malware, stealing bitcoins and also as mining software for litecoins.¹⁷³

In another recent case illustrating the externalization of costs, security researchers Rob Ragan and Oscar Salazar cobbled together a makeshift botnet by using free trials and freemium accounts at a variety of cloud providers.¹⁷⁴

One of their first experiments with their new cloud-based botnet was mining the cryptocurrency Litecoin. (That second-most-used cryptocurrency is better suited to the cloud computers' CPUs than Bitcoin, which is most easily mined with GPU chips.) They found that they could produce about 25 cents per account per day based on Litecoin's exchange rates at the time. Putting their entire botnet behind that effort would have generated \$1,750 a week. "And it's all on someone else's electricity bill," says Ragan.

As time goes on, other exploits will likely arise, including using power plant subsidies in China - now the location of several mining pools that not only have access to subsidized electricity but do not have to worry about many environmental externalities.¹⁷⁵¹⁷⁶

While there are likely a variety of market distortions in part due to arbitrated electricity prices, botnets and a variety of uncertainty in legal frameworks, even relatively large capitalized companies in this mining space inadequately hedge risk. In November 2013, Alydian filed for Chapter 11 protection in bankruptcy court.¹⁷⁷ It was an ASIC-based hosted mining company ("outsourced mining"), one of the first in which customers simply buy shares of hashrate and the maintenance and management of the equipment occurred on site at Alydian's facility.¹⁷⁸ During the subsequent hearing, it was reported that rapid increases in the global hashrate for Bitcoin in November 2011 resulted in the company's underinvestment in mining hardware - planned in the summer of 2013 - not being sufficient to generate income in after a sharp increase in the network's hashing power in November later that year.

The fourth major exception are individuals intentionally mining at a loss in order to extract "virgin" coins, those without any history thus providing greater anonymity. Because these coins have not been used before, there is no history linking them to any previous trade or transaction. Consequently, they can use these tokens to protect their identity when exchanging bitcoins for illicit trade (e.g., black market activities). It is unclear how much mining of this type is taking place.

A team of researchers at the University of Munster explained how in practice, not all bitcoins are the same:¹⁷⁹

Bitcoins are not alike. Each transaction is a descendant of a unique transaction history, which is readily available in the public block chain. Therefore, markets participants can, in principle, scrutinize the history and become selective in which transactions they accept; or, with more granularity, how much they value it. The fact that most participants do not differentiate for the time being is hard to justify with economic rationality. A necessary consequence of differentiation is that market prices reflect the information encoded in the transaction history. Dealing with bitcoins of two kinds (e.g.,

black and white, under the poison policy) may be manageable, essentially at the cost of lower liquidity in both market segments. Pricing every history individually poses new challenges to the design of market mechanisms, for example at exchanges; but it also affects every small merchant who accepts bitcoins in exchange for goods or services.

[...]

Taking the uniqueness and identifiability of Bitcoin transactions beyond the question of pricing offers interesting new insights. Precious metals or official currencies are designed as homogeneous goods. This ensures fungibility: quantities are exchangeable and divisible, a precondition to fulfill the monetary function as unit of account. Bitcoin transactions, by contrast, are heterogeneous goods, differentiated on a quality dimension. The valuation of this quality is subject to individual preferences. This threatens the function as unit of account, as detailed above in Section 5.1

This issue intersects with metacoins and colored coins discussed later in chapter 14.

Lastly, the final exception are state actors. At this time it is unclear what, if any, government agency is mining but the costs of which would in any case be externalized to taxpayers. This is briefly discussed in chapter 14 regarding an NSF researcher who used government owned supercomputers to mine bitcoins.¹⁸⁰

As a consequence, the true costs of operating the network are almost certainly higher than the lower bound estimate because of botnets which essentially steal and externalize resources costs, well-wishers who continue despite financial incentives to liquidate, privacy-oriented miners seeking virgin coins and hobbyists who may have ideological inclinations and see their mining as “donation” and “charity” to the community.¹⁸¹

Bitcoin: a peer-to-peer heat engine

While there will be volumes more written on the econometrics of Bitcoin’s underlying incentive mechanisms, in April 2014 Danny Bradbury published some important research on an issue that no one could have foreseen in 2007 – 2008, the years in which Satoshi Nakamoto, ostensibly designed the system: what are the actual energy and infrastructure costs for seigniorage?¹⁸²

Ignoring for the moment the anecdotes in Bradbury’s series, we now know that there is a near-precise model that describes the cost of running and maintaining the network. The way the cost estimate is determined is through how Bitcoin acts as a decentralized waste heat creator that activates and deactivates heat generation based on market participation and pricing signals. What do the randomizations necessary for cryptography and the waste heat produced by computing devices have in common? One word: “exergy,” a term of art describing the maximum useful work possible during a process that brings a system into equilibrium with a heat reservoir. Exergy is always destroyed in the seigniorage hashing process - for example - if a token's value increases to \$1,000, this means that at most \$1,000 worth of waste heat will be

generated somewhere in its creation. This can be in the form of actual electricity-to-heat conversion, but currently the bulk of it throughout the ASIC manufacturing (e.g., CAPEX) and logistical supply chain as well as new market participants coming online seeking rents arising from their production of this ledger unit.

Where that same token is valued by the market at \$500, that means that *ceteris paribus*, it collectively costs the network \$500 to operate per token generated (+/- several percent). This then means if the price were to go up to \$1,000 again for an entire year, approximately \$1.3 billion worth of operating costs (e.g., infrastructure capital expenditures) will subsequently be spent to "extract" tokens and process transactions at this higher price. This is known in advance due to the monetary base expansion built into the code; this year (2014) the money supply on the Bitcoin network will expand by approximately 1,312,500 bitcoins or 11.1% of the total bitcoins ever created (i.e., scheduled inflation). As the market value of these tokens fluctuates, miners (seigniorage crafters) will turn off, on, dispose of or acquire machines depending on whether it is profitable to do so.

What this means is that if a bitcoin reaches \$10,000 in value, then at least \$13 billion worth of capital expenditure will be invested in extracting it.¹⁸³ Scale each bitcoin up to \$100,000 and the infrastructure alone would cost more than the entire market capitalization of several global payment processors (e.g., MasterCard spent \$299 million on capital expenditures in 2013), yet likely without providing any immediate benefits to customers or merchants.¹⁸⁴¹⁸⁵ This concept is debatable and discussion about it, including proposals from core developers such as Peter Todd and Adam Back, will continue to be researched and published in the coming months.¹⁸⁶ While there are plans in the works to modify the Bitcoin core code to address these issues, as the code sits today, the provision of additional hash power will not result in faster confirmation times or greater transactional capacity. Furthermore, at this scale centralization will likely become crystalized because miners incapable of breaking even at \$100,000 a token will be purged from the marketplace. The only miners capable of participating at this level will likely be professionally run datacenters with peering agreements and increasingly capital intensive economies of scale.¹⁸⁷¹⁸⁸

At a stable \$1 million per token, mining facilities would need to efficiently utilize and dissipate \$150 million of exergy per hour, limiting their geographic locations to a global handful capable of powering the internal infrastructure (e.g., next to multiple power plants dedicated solely to it).¹⁸⁹ This will change again in two years due to block reward halving but is used for illustrative purposes. In other words, non-marginal mining operations will and have become fully professionalized IT teams (CEX.io, Cloudhashing) that model their budget from earnings projections and an estimated revenue stream from seigniorage. Price volatility may cannibalize their accounting profit and ultimately can purge them as well (as described below).

Another related issue to this is equating hashrate with security; this is arguably a *non sequitur*. Hashrate is an arbitrary metric that fails to fully qualify the security of the network, or the

quality of network performance, either of which is dependent on a number of other factors including the wide distribution of the blockchain.¹⁹⁰

To equate hashrate to security is akin to Soviet-era planners boasting about the tonnage of each car at a state factory produced to demonstrate these automobiles' "performance." Though a mass-produced Yugo or Lada from the Eastern bloc might indeed move via a combustion engine, a more accurate gauge and metric of performance would be an F1 auto that is a unique product which is amenable to ongoing maintenance and upgrades. Since some Bitcoin advocates claim it is a real-time gross settlement (RTGS) platform, a more accurate comparison would be with Visa, which processes on average 3,000 times as many transactions each second than Bitcoin does currently.¹⁹¹ As we shall see below, funds invested in the Bitcoin network are not being utilized to actually enhance its performance or its security.

Robert Sams, co-founder of Swiss Coin Group, has written about this noting that:¹⁹²

Hash rate says nothing about security, it's the amount spent on hashing that matters. If there were a way of requiring miners to hash using an abacus, hash rate would be tiny but network just as secure if same amount of capital was spent employing dextrous human calculators.

Efficiency of converting a scarce resource into hashes has no social benefits here. (Except that it correlates with tx verification, where efficiency is beneficial).

You ultimately have two problems to solve: what tx fee maximises fee revenue for miners? Second, is that maximum sufficient to cover the required hashing costs for minimum security?

Because of how they are interconnected, additional hashrate may provide utility for transactions. However after 51% of the hashrate it is exergic deadweight relative to security.¹⁹³ Thus there are likely other more accurate metrics for measuring and qualifying the security of the network.

A million dollar bitcoin

Ceteris paribus, as has been established above, the cost of creating a new bitcoin (capital depreciation, electricity, property lease), will eventually equal its market exchange value on average.¹⁹⁴

Below is a chart I used at the beginning of the chapter to estimate the historical lower bound costs.¹⁹⁵

Chart 1: Estimated lower bound costs

	Bitcoin	Litecoin	Namecoin
Time period	July 18, 2010 - July 18, 2011		
Open & close	\$0.08 - \$13.68 per bitcoin		
Weighted annual value	\$3 per bitcoin		
Money supply added	2,625,000 bitcoins		
Estimated seigniorage	\$7,875,000		
Time period	July 18, 2011 - July 18, 2012	October 11, 2011 - October 11, 2012	
Open & close	\$13.68 - \$8.90 per bitcoin	\$0.00 - \$0.088 per litecoin	
Weighted annual value	\$5 per bitcoin	\$0.02 per litecoin	
Money supply added	2,625,000 bitcoins	10,500,000 litecoins	
Estimated seigniorage	\$13,125,000	\$210,000	
Time period	July 18, 2012 - July 18, 2013	October 11, 2012 - October 11, 2013	October 16, 2012 - October 16, 2013
Open & close	\$8.90 - \$85.51 per bitcoin	\$0.088 - \$1.96 per litecoin	\$0.055 - \$0.458 per namecoin
Weighted annual value	\$50 per bitcoin	\$1.50 per litecoin	\$0.25 per namecoin
Money supply added	1,750,000 bitcoins	10,500,000 litecoins	2,625,000 namecoins
Estimated seigniorage	\$87,500,000	\$15,750,000	\$656,200
Time period	July 18, 2013 - July 18, 2014	October 11, 2013 - July 11, 2014	October 16, 2012 - July 16, 2014
Open & close	\$85.51 - \$619.78 per bitcoin	\$1.96 - \$7.76 per litecoin	\$0.055 - \$1.90 per namecoin
Weighted annual value	\$500 per bitcoin	\$10 per litecoin	\$1.50 per namecoin
Money supply added	1,312,500 bitcoins	7,875,000 litecoins	1,968,750 namecoins
Estimated seigniorage	\$656,250,000	\$78,750,000	\$2,953,125
Total lower bound cost	\$764,750,000	\$94,710,000	\$3,609,325

While there are at least five exceptions, as noted above, if a token is worth \$1 then no more than \$1 worth of operating costs will be used to extract that rent by an economically rational miner (*homo economicus*).¹⁹⁶ Similarly, if a token is worth \$1,000, then mining farms will only operate their hashing systems at just below breakeven (otherwise they could simply turn off the machines and allow other mining pools to create seigniorage).

In practice, many miners do not do this as many believe that any operating loss would eventually be recouped through token appreciation (as noted by the Austrian family). Since this is the case, Bob effectively buys future network security on that price expectation creating temporary additional hashrate overhang – additional deadweight loss which is anything above 51% of “honest” network hashrate. However unless a survey is done of miners operating at losses, the additional extra operating costs are likely difficult to estimate (hence the lower bound estimate).

One notable comment I have received since originally writing about this issue was the following, “that power consumption is already as high as it will ever need to be. A million dollar bitcoin will not cost more to process and transactions add nothing to the costs; the cost of transactions will go down as volume increases.”

This is false. If each token is worth a million dollars then why would not more people enter the market if you can produce one for \$500? What would happen in reality is that if the token increased to \$10,000 then \$100,000 and \$1 million the same signaling mechanism tells miners when to operate and when to turn off their machines. If a token reached a price level of \$1 million today, everyone on the planet would likely try to hash blocks with every available computing resource until that breakeven equilibrium was reached (e.g., once operating costs reached token rents). Whereupon, marginal mining participants would once again become

purged from the market place as professionalized datacenters capable of profitably scaling are built, merged and acquired. Being purged does not affect the price of the token but it does lead to centralization; as token prices increase only those miners capable of *profitably* operating at the new level will be able to compete on seigniorage.

In other words, the logistical cost of running Bitcoin rises linearly with its total value.¹⁹⁷ More efficient mining gear (such as ASICs) does not reduce energy use of the Bitcoin network, because the number of such installations rises to the profitability limit. It only raises the network difficulty. The proof-of-work method must expend real work, which means it must consume energy. Therefore, the price of bitcoin reflects its demand, which incentivizes difficulty (hardness), which reflects how much work goes into the proof-of-work scheme, which directly converts into how much energy is being expended. The end result is that at this level, at \$1 million per token, a mining facility would need to expend a similar amount of energy (since ~98% of operating costs are related to electricity). There are very few locations on the globe capable of generating that kind of electrical production.¹⁹⁸ For instance, in 2016 when block rewards halve, if token values were \$1 million then mining facilities would essentially need to expend \$12.5 million in electricity every 10 minutes or \$1.8 billion in electricity each day.¹⁹⁹²⁰⁰

Again, the reason why is because, token values signal to miners when to operate and when to shift their labor elsewhere.

For instance, in July 2014, CoinTerra, a mining manufacture announced that it had “signed a multi-megawatt datacentre deal with colocation and managed service provider CenturyLink.”²⁰¹ And that that in addition to selecting CenturyLink for its “efficient cooling system” that CoinTerra initially began its search for colocation providers “by looking for commodity power.” Why? Because a rack (42U) of CoinTerra mining equipment consumes 25 kWh of power. According to the same report, an estimated 15% of the total bitcoin hashrate is generated from CoinTerra mining systems. They are also building a 20 MW data center in Canada.²⁰²

And while capital costs still arguably play the most important role in determining whether marginal participants should choose to join the mining effort in the first place, there is a major reason why large mining facilities have not set up in Denmark or Germany. For example, in 2009 Google purchased an old paper mill and set up a data center facility in Hamina, Finland due in large part to its energy infrastructure which was ideal for cooling purposes.²⁰³ Similarly, BitFury, a VC-funded mining manufacturer, purchased an old bank, also in Hamina, Finland to capitalize off the geographic cooling advantages.²⁰⁴

BitFury, whose mining equipment accounts for roughly 40% of the bitcoin network hashrate, also recently built a new 20MW power plant near Tbilisi in the Republic of Georgia all in a bid to compete in the hosted, cloud mining space discussed in Chapter 5.²⁰⁵ It also needs this energy because on the manufacturing side, according to Henry Yeh, managing partner at Binary Capital:²⁰⁶

What I see as happening is that [BitFury is] going to produce so many ASICs and there's only so many 1MW, 20MW or large megawatt facilities. It's just physically impossible to bring up that many facilities in a short span of time.

Similarly, MegaBigPower (MBP) which claims to be the largest North American Bitcoin mining provider, is developing a franchisee model, building facilities spread across the US, each that "will host between one and five megawatts in electrical capacity." As part of this effort, MBP is working with a California-based Acquirer as a lead franchisee and will, "embark on a 50MW power build with Acquirer over the next six months." MBP also announced that it is working with CoinMiner as a partner as well. CoinMiner's CEO explained that as part of this deal, "I'd like to see us up in the 10 megawatt range sometime by mid-next year."

And that:

Notably, CoinMiner is aiming to support its own business model by tapping into alternative energy sources in The Finger Lakes region in New York, where the mine is based. He cited hydropower and methane power as two possible sources, adding that these efforts, combined with local subsidies for new businesses, are giving them a boost as they ramp up.

All told, based on current market prices, mining companies and users will spend at least \$600 million on infrastructure in the second half of 2014.²⁰⁷ Subsidies are also discussed in chapter 5.

This energy arbitrage issue was discussed in a paper published in September 2013, *Bespoke Silicon*, wherein Michael Taylor explains the evolution of chip designs and Bitcoin mining hardware from CPUs through the customized hardware that led to ASICs. In the section on hardware scaling he foresaw the same type of energy scouting that is occurring today noting that:²⁰⁸

However, unlike in the "race to ASIC" days, the cost/performance difference of future generations of hardware will not be great enough to quickly obsolete the last generation. Rather, it will be energy costs that are likely to dictate which ASIC will be the most profitable. This is especially true in the case where there is a supply glut of chips of a given generation, such as is likely to happen in the next year, as the NREs have been paid, and the three groups are simply paying wafer costs now. One can imagine Bitcoin users dumping their chips, and groups with access to cheap energy buying them for almost free and putting them back to use for mining. Of course, there are two factors that dictate energy costs – the cost of energy, and the energy consumption of the part.

The parties with the greatest advantage will be those that have cheaper access to large quantities of energy and already have their mining hardware paid off when returns on hashing were higher. Cheaper energy allows these parties to pay off their newly

acquired hardware over longer cycles, and to continue to operate even when \$ per Gh/s, as shown in Figure 3, drops precipitously low. Others may have an advantage because they have more energy efficient hardware designs. Optimizing Energy Efficiency. BFL's 65-nm part hashes at 5.5 W per Gh/s, while Avalon's 110 nm part is 9W, and ASICMINER's 130-nm is 8W. Post-Dennard Scaling [2] predicts that a 14-nm process could allow energy efficiency to improve another $65/14 = 4.6$ to around 1 W per Gh/s.

NRE stands for non-recurring engineering is the one-time cost to research and develop a new product. Dennard Scaling, named after Robert Dennard, states that as transistors get smaller their power densities stay the same.²⁰⁹ It bears mentioning that a year after Taylor's paper was published, Spondoolies (an Israeli-based mining manufacturer) has improved on this ratio to 0.58 W per gigahash/s.²¹⁰ And in September, the same company plans to ship a 4.5 terahash/s system that consumes 3000 W.²¹¹ This is not an endorsement of this company or product, but just an illustration.

One common conjecture is whether or not solar power or nuclear power could change this. Unfortunately, this is purely a matter of expending energy and not about what exactly is generating it. Even if you were to replace all the coal powered plants in China (or elsewhere for that matter) with renewable energy, mining facilities would still consume and expend electricity at roughly the same value as a token because $MV=MC$.²¹² It would likely be even more expensive because current photovoltaic panels take 2-7 years if installed properly to return to the user the amount of energy that went into making them. That assumes perfect efficiency of use of all the possible energy the panel can produce. In reality, it takes 5 -15 years if the panel is installed optimally and maintained well. If the panel stores in a battery and inverts off the battery, then it takes more time. If it is not installed or maintained well (e.g., it gets dirty, a tree grows to shade it) the panel may never return the energy that went into it. That energy to make the panel is subsidized Chinese coal power. So in this scenario Bob is borrowing forward a lot of high-carbon energy when he installs a solar panel.

Can distributed workloads create lower energy requirements?

No. Another interesting story in China is a Bitcoin start-up in Beijing that fleshed out a business proposal with a well-known telecommunication provider to integrate ASIC chips inside routers. At the time, the thought was this telecom company could sell the routers globally and users could receive a steady stream of income as routers are typically left on day and night. Ideally this would involve some kind of 70/30 split in which the start-up would receive 30% of the bitcoins generated and the customer would receive the other 70%. Yet the reality of developmental process illustrates how this is unprofitable. It takes between 3-9 months to design an ASIC from scratch and tape-out (3 months assumes double shifts). By the time an ASIC passes its verification process, tapes-out, goes through maskmaking, is shipped to the client, integrated into the router and shipped globally, the ASIC is no longer capable of profitably hashing. In other words, supply chain integration and logistical deployment will likely

prevent the dream of everyone globally of having an ASIC processor on their smartphone *profitably* hashing away at block headers based on electrical consumption alone.

But what happens once the ultimate thermodynamic efficiencies of ASICs are reached; would that lead to any different geographical distribution?

No. Andrew Poelstra's paper (discussed later below) on this subject attempts to broach this topic and comes to the conclusion that once the thermodynamics of a chip are reached, this would lead to decentralization.²¹³ For the sake of argument, assume that someone like Nvidia, BFL or KnC creates a chip at the Planck length (ℓ_P).²¹⁴ However even at that level, a rational actor would not set up a large pool in San Francisco because of relatively high operating costs. Or in other words, even with the most efficient chip design, the sole competitive force would be electricity. If that is the case, then the chips would simply end up wherever the cheapest energy source is, potentially leading to centralization. While the issue as to the degree to which centralization is occurring is actively being discussed, this does not necessarily impede the networks current effectiveness, though it could lead to social engineering challenges.

And again, over the past 24 months mining equipment typically had a profitability window of roughly 3-5 months whereupon it became obsolete, but this "race" will soon be over. A 10% improvement alone will likely not make investing into new mining hardware profitable. More precisely, a 10% improvement in mining hardware efficiency does not provide a competitive advantage over someone who has access to energy at half the cost (as seen with the S-curve at the beginning of the chapter). Thus the energy limits are real and will likely put an upper bound to its ultimate size as described below.

Energy limits

The issues above are *dissimilar* to the claims that the internet will not be able to scale, this includes anachronistically hackneyed claims that the internet cannot do voice, quality voice, video or anything larger than a few kilobytes per second. Those were largely caused by immature software stacks and hardware constraints. In contrast, for the Bitcoin network (and other cryptocurrencies using a PoW mechanism), the built-in thermodynamic hurdle still remains. In the event that the token appreciates (which disincentivizes spending due to volatility and also incentivizes continued speculation and stockpiling), the network will cost as much as it is worth.²¹⁵

Following the block reward halving in 2016, a million dollar token would hypothetically incentivize \$656.2 billion in expended energy (exergy) per annum, or roughly the current GDP of Switzerland.²¹⁶ There is no way around the exergetic requirements, it is built into proof-of-work mechanisms and because of a type of *regulatory capture* (i.e., miners will only hash and protect code that is profitable to them) the PoW mechanism will likely never be switched to something less capital intensive like proof-of-stake.²¹⁷

Fred Trotter, a data journalist, calls this process malignant computing:²¹⁸

We have a similar problem with the use of computation in markets. We can call this *malignant computation*. This is when computation starts to ensure its own survival at the expense of the overall marketplace. The Skynet hypothesis is a boogeyman intended to scare the young and the paranoid. The real threat from AI is that it will become so good at the pointless tasks that we have given it that those pointless tasks will become a black hole of resources.

Restated, while there may be a hypothetical scenario where Bitcoin could evolve to some more energy efficient block verification model, this is an unlikely possibility because the miners will never agree to it. Furthermore the price is a lower bound estimate due to exceptions like charitable donations of hashrate.

The end result is a joke a friend in China told me last year when I was helping him build a Litecoin hashing machine: taken to an extreme, bitcoin mining (or litecoin mining for that matter) would eventually gravitate to facilities located in the Arctic Ocean, which acts as a natural heat reservoir and dissipater.²¹⁹ Peered together with microwave towers these pools would provide the financial backbone – to a network funded primarily through gambling revenue, the networks on-chain “killer app.”²²⁰

Incidentally, the Hamina, Finland site used by Google purportedly features, “underground tunnels running to the Baltic sea, which Google utilized to cool the facility’s servers. The company included the tunnels in the new data center design, utilizing pumps to push cold sea water from the Gulf of Finland into the facility’s cooling system.”²²¹ Another report notes that Google, “uses the sea to replace the chiller in its cooling system, collecting cool water from an inlet pipe located about 7.5 meters beneath the service of the Baltic Sea. The water then travels into the facility through large tunnels carved out of granite, and is used in a water-to-water heat exchanger.”²²²

Perhaps the Arctic Ocean joke was not too far off the mark.

Mining revenue versus profit

Many cryptocurrency adopters mistakenly think that mining is cheap, free or miraculously perpetual.

For instance, Dave Carlson, founder of MegaBigPower explained at Coinsummit in July 2014:

“In the next two years 2.6 million bitcoins will be produced. At current prices that’s a \$2 billion market opportunity. How much does it cost to invest, to capture a large market share of that \$2 billion? It’s far less than \$2 billion. You could invest \$100 million and capture a significant share.”²²³

This is incorrect. What does happen, as in any resource extraction process, is that the token price provides a signal to market participants who will conduct a cost-benefit analysis to see what their profit margin is.

In theory, what will happen is that more participants will come online to compete for rents on that ledger unit, squeezing margins to roughly zero. That is to say, new participants will expend capital and in this case purchase hashing equipment to acquire these coins yet because the difficulty rating scales in conjunction with hashrate, on the margins there is no collective “market opportunity” – the spread is arbitrated until equilibrium is reached. Mining, or more precisely private seigniorage, is a zero-sum game; no value is added or extracted and only one system can win the reward while everyone else losses.

Earlier this summer, Gavin Andresen explained this in further detail:²²⁴

Mining is a zero-sum game.

Unless you have some innate advantage you should not play zer-sum games. In the case of mining, my advice would be not to play unless you have early access to more efficient hardware or cheap/free electricity.

The only other reason I could see to mine would be if you want to speculate on the value of Bitcoin going up, and are living somewhere where you can pay for mining hardware (and electricity) but cannot work for or buy bitcoins directly.

The same reasoning applies if you are mining for alt-coins; yes, it is possible you get lucky and buy the right hardware at the right time and mine the right coin. But that's not likely, unless you have some special knowledge or hardware or talent.

As previously noted, the marginal productivity of labor in Bitcoin is zero. Each of the participants would be better off if they simply bought bitcoins and held instead. Taking the logical next step, just one miner would process all transactions – though that would defeat the purpose of decentralization.

In practice, there are a variety of market imperfections that mean that a few companies can make bumper profits from mining.²²⁵ The primary one which is mentioned in this chapter is the bottleneck over chip manufacturers. Another is the fact that the block reward return is stochastic and hence to \$ 2 billion may in fact only be \$1 billion dollars. There are existing economies of scale and few participants rather than many. Thus the theory of constant equilibrium is not quite valid (yet). This market is still very volatile and with numerous imperfections. Over the long run the theory will like hold true but certain market imperfections could prevent the equilibrium from arising in the next 2-3 years.

Ray Dillinger, who interacted with Satoshi Nakamoto on the original Bitcoin announcement list and who is still actively providing commentary in the community, independently observed the same equilibrium phenomenon:²²⁶

I think the economics of “mining” reveal a design flaw in proof-of-work cryptocurrencies.

The idea that people can ‘farm’ the money supply by buying and powering hashing hardware guarantees that the difference between the amount of value produced and the amount of resources expended will approach zero.

It’s something like a tautology, where people are spending money in an auction for the right to print money. Such an auction is more or less guaranteed to bring the costs of printing money right up to its value, which is an unnecessary (and unwanted) feature.

Aside from externalities and subsidies in the markets for electrical power and waste heat making the auction unfair from the beginning, that simply is not a necessary feature of a currency. Certainly no government-issued fiat currency is so resource-intensive to supply. But that comes about mostly because the government can impose additional costs (such as jail time) on unauthorized printing which are not borne by those doing authorized printing.

And that distinction between “authorized” and “unauthorized” is something that peer-to-peer and distributed systems don’t have access to.

Thus the potential market is not \$2 billion in profit as Carlson alludes to but rather \$2 billion in revenue with low to no profit margin. The only participants who actually gain rents on securing the network and processing transactions are those farms which acquire the newest and best hashing equipment first. The other participants, a significant portion of who operate at losses, must hold onto the mined tokens with the hopes that the tokens themselves appreciate in value.

This should not be taken as a slight against the mining industry, miners are the backbone of the network – they are the network. Yet just as it would be disingenuous to claim that gold or iron extraction today had a 20x upside, it is similarly a *non sequitur* to claim that the upside in bitcoin mining over the next 2 years is 20x. It is likely zero. Or in other words, if mining hardware becomes three times as efficient, *ceteris paribus*, the amount of hardware that's mining will triple yet the number of bitcoins mined is not tripled as difficulty adjusts in tandem.

This misunderstanding of the network and infrastructure costs is very common in this space. In a discussion with Hass McCook, author of the paper "An Order-of-Magnitude Estimate of the Relative Sustainability of the Bitcoin Network" explained to me that:²²⁷

The purpose of the part of the paper covering the environmental impact of maintaining a banking system was to demonstrate the huge impact of just hiring an army of rent-seekers (not including constructing skyscrapers etc.), to set a baseline figure of this impact, and to highlight the gift that we have been given by bitcoin to ensure we don't replicate this in the future. In September this year, we will have a 6TH miner which only needs 2,500W (spondoolies SP30), and I'm sure than in September 2015, we will have a 12TH rig that uses the same amount of power. And in September 2016, a 24TH rig that uses the same power, and so on, as has been happening in the PC industry for the past

three decades. \$/kWh and tCO₂/kWh will continue to decrease on a yearly basis too. It would not surprise me to see the marginal cost and impact of electricity decrease by 95% as we move to emission-free decentralised solar and other renewable power by the end of the decade, with bitcoin companies being young and dynamic enough to take advantage of this advancement, whilst the old, inert and encumbered banking system simply cannot and will not. We are already at this tipping point, as can be seen in the auto industry with the move to hydrogen fuel cells and electric power.

Generally speaking, the people who disagree with this reasoning are either paid by banks, are upset that they were not early adopters of bitcoin, or have a world-view and education so narrow and shallow that it does not extend past the confines of their local neighbourhood, coupled with the inability to look 10 years into the future, despite already witnessing first hand the remarkable technological progress that can be made in a full decade. Fortunately, the materialisation of this reasoning is a sure inevitability due to the millions of man-hours of work by the world R&D community who are concerned not with such narrow-minded opinions and internet-troll-reasoning, but in the pursuit and dissemination of knowledge, and the improvement of humanity. "Sustainable" is more profitable in the long-run, and the most sustainable systems and companies, by definition of the word, "sustain" for the longest period of time. Sustainable digital currencies are here to stay, people should start to accept and deal with this fact of life.²²⁸

This is a common conflation error: the cost of transmission with the cost to maintain the network. What is left unsaid in both his paper and this specific exchange is that protocol will adjust the difficulty rating linearly with the hashrate wiping out any gains made by solar energy; gains are a mirage. If you double the efficiency of mining systems the number of mining equipment (or miners) will merely double and the network costs remain the same. Therefore the higher the token market value is, the higher the hashrate, leads to a correspondingly larger environmental impact.

In essence, this endless cycle is a working illustration of the Red Queen effect. Or as Nick Gogerty, creator of Solarcoin analogized:²²⁹

The Red Queen is originally from Alice in Wonderland. In the Queen's race everyone runs faster, but you never get ahead," he says. "The same happens in hashing. All of the participants are co-adapting. You have to keep adapting to keep up.

Furthermore, even if the energy source is nominally free (such as solar power) the costs for solar panels is not. Capital has to be spent by someone, somewhere to maintain the network. And if there is a profit margin, such as the kind McCook hypothesizes, outside observers would use a cost-benefit analysis to see if they can also attempt to extract a portion of those margins. What then happens is a competitive race to equilibrium, where the capital costs of maintaining the network equals the costs of the token itself. Or in this case, a world covered by solar panels to power mining farms.

The source of energy is not important to Bitcoin, what is important is the exergy – creating proof-of-work-based blocks by dissipating energy. There is no “free energy” anywhere in this process as it is not an issue of physics but rather of economics. In an open market any competitive infrastructural edge one firm has (such as utilizing the Carnot cycle, a flywheel, a Stirling engine or ASIC heated homes) could eventually be replicated by competitors just as cloud computing centers do today with advantageous geographical climates (e.g., Iceland, Finland, Siberia).

Cryptographer and protocol designer Ben Laurie also observed this pattern three years ago:²³⁰

Even worse, it is clear that arriving at the equilibrium state for Bitcoin is incredibly expensive: half of all the computing power in existence must be burnt, in perpetuity, maintaining agreement about the current state of the currency.

Actually, in practice, it is more than half of all computing power (50% of the honest nodes): it is all computing power that is “burnt.”

This totality of economic activity that is essentially “lost” was concisely explained in L.M. Goodman’s Tezos position paper:²³¹

Unfortunately, proof-of-work arbitrarily increases the costs to the users without increasing the profits of the miners, incurring a deadweight loss. Indeed, since miners compete to produce hashes, the amount of money they spend on mining will be slightly smaller than the revenues, and in the long run, the profits they make will be commensurate with the value of their transaction services, while the cost of mining is lost to everyone.

This is not simply a nominal effect: real economic goods (time in fabs, electricity, engineering efforts) are being removed from the economy for the sake of proof-of-work mining. As of June 2014, Bitcoin's annual inflation stands at a little over 10% and about \$2.16M dollars are being burned daily for the sake of maintaining a system that provides little to no security over a centralized system in the hands of ghash.io.

For instance, to use the most optimistic value point that some early adopters have suggested: a \$1 trillion bitcoin will incentivize \$1 trillion worth of energy (and capital) expended to secure it. \$1 trillion is approximately 1/72nd of the world’s annual GDP. Assuming such a market value was placed on just one bitcoin five years from now, a competitive mining industry would expend \$12.5 trillion worth of energy and capital every 10 minutes to secure the network, or \$1.8 quadrillion a day which is approximately 25x of the world’s current annual GDP.

As noted later in chapter 5, other externalities intervene long before this. If we presume that such a coin could exist, what it would require is that the \$1 trillion bitcoin be sold immediately at the expected value. No existing entity could bankroll holding a nearly \$1 trillion investment (absent weakening of the dollar worse than the Russian ruble) for any length of time. This

would further imply that the market cap of all bitcoins would be at least 10^{19} which is 2.5 million times current M0 (notes and coins in circulation). As explored in chapters 9 and 10, this is unlikely to ever happen. And there are major uses of electrical power that would create hurdles, limits to the amount of energy that can be transported by the electrical grid. For instance, Germany's grid cannot deal with more than 45 gigawatts of power at this time.²³²

Interestingly enough in the concluding remarks of his paper McCook sees the proportionality:

Adding CAPEX and OPEX results in a cost to mine a Bitcoin of \$630, and a total yearly cost of \$827.8 million. Interestingly, this is the exact Bitcoin price at time of writing (Monday July 7, 11:00 UTC). It should be expected that price of Bitcoin should grow proportionally with the cost of network CAPEX and OPEX based on hash-rate from this point forward. This goes a long way to explain the cyclical bubble nature of Bitcoin's market price, and gives us insights into local minimum prices after a burst bitcoin cycle bubble.

Again, there is no unearned income on the margins in a competitive mining marketplace, virtual or physical.

One real world facsimile to this resource extraction process is the Mountain Pass rare earth mine in California. It shut down in 2002 in part due to environmental restrictions and also due to the then-low prices of rare earth elements (REE). REE are a set of 17 elements on the periodic table that are increasingly used by technology companies for hardware devices. After a set of export restrictions put in place by China (which is the largest exporter of REE) effective September 1, 2009, the market prices for REE rose such that by 2012 the Mountain Pass mine was reopened because it was economically cost effective to do so.²³³²³⁴ Bitcoin mining farms face similar cost and profitability analysis.

One last point regarding McCook's paper is the claim that, "At 0.75 million tonnes of CO2 produced per year, Bitcoin has 99.8% fewer emissions than the banking system."

In a previous paper I came to a similar erroneous conclusion, but this is not an apples to apples comparison. Bitcoin (the network) does not perform any of the same functions of a banking system nor is it transacting anywhere close to the volume of trade that the current system does because it does not have a mechanism for savings, lending, collateralization and so on.

For the sake of argument, let us assume that McCook's numbers are correct. Based on CapGemini's World Payments 2013 report one reddit commenter noted that CO2 cost per transaction for global non-cash payments worldwide was .00116 tons.²³⁵ And that based on the global Bitcoin transaction volume last year (21.7 million) that Bitcoin actually consumes 30x more CO2 per transaction than the existing global non-cash payments worldwide.

CO2 comparisons of incumbent payments versus Bitcoin	
Global non-cash payments worldwide (2012)	333 billion
CO2 Cost per transaction	.00116 tons
Global bitcoin transaction amount past year	21,747,368
CO2 Cost Per transaction	.0345 tons
Bitcoin currently consumes 30x more CO2 per transaction	
Current Bitcoin max transaction volume (7 transactions/second)	110,376,000
CO2 cost per transaction	.0068 tons
Bitcoin uses 5.9x more than current banking system	
Visa theoretical maximum transaction volume	126,144,000,000
CO2 cost per transaction	.003 tons
Visa is 50% more efficient than the current max Bitcoin potential	

For comparison, according to a US Congressional Research Service (CRS) report updated on July 15, 2014, “Bitcoin daily transaction volume [in 2014] fluctuated in a range of between \$40 million and \$50 million, representing between 40,000 to 80,000 daily transactions.”²³⁶ In addition, in June 2014, according to the Board of Governors of the Federal Reserve System the money stock (M2) or measurement of US money (the sum of currency, demand deposits, saving deposits including money market saving accounts) was about \$11.3 trillion or about 1,000 times larger than Bitcoin.

Similarly the CRS report highlights that in 2013 Visa’s total dollar volume was \$6.9 trillion, “with an average number of daily individual transactions of near 24 million.” And that the daily transactions in dollars on global foreign exchange markets during 2013 averaged over \$4 trillion.²³⁷

These ratios will continually change over time but the claim that Bitcoin is currently greener does not hold up to empirical evidence by a wide degree. Additionally, McCook’s paper does not include the roughly 7,000 verification nodes on the Bitcoin network that are all run at losses and emit additional CO2, or the CO2 used in making those nodes and so forth.

It may not be as calamitous (yet) as Charles Stross’ statement (“a carbon footprint from hell”) but Bitcoin currently has no environmentally competitive edge over the current amalgam of interconnected financial and banking systems nor can it based on how proof-of-work currently works.²³⁸

Hashrate does not determine prices

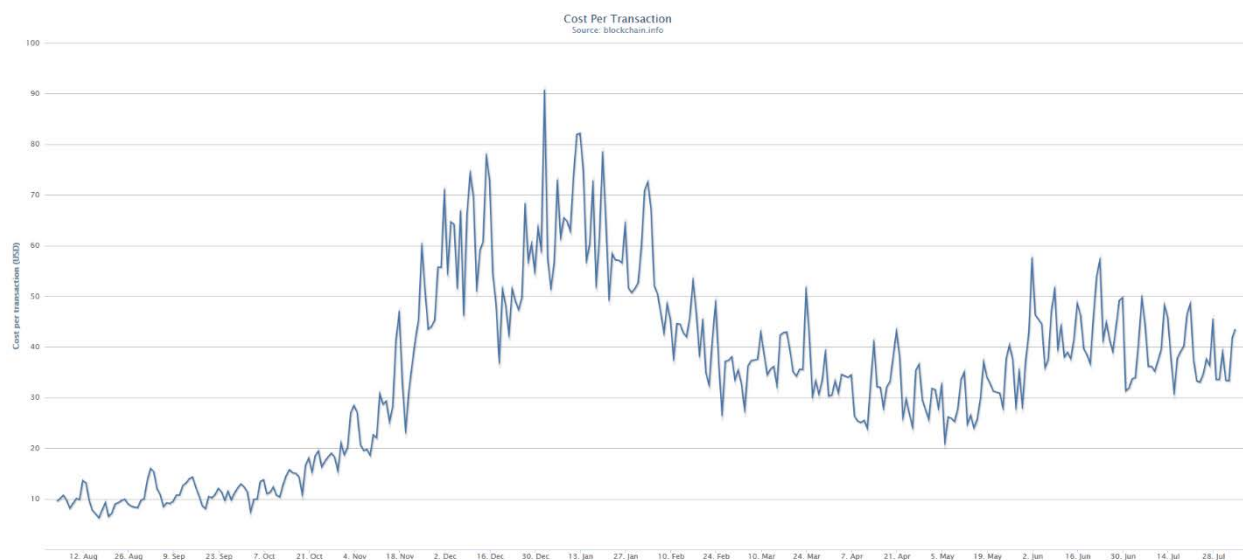
In a competitive marketplace, the economic profit (which includes the opportunity costs of pursuing certain actions) of a good or service typically tend towards zero.²³⁹ That is to say while firms may still have accounting profit, the additional margins in the long run are reduced due to competitive pressure.

Does increased hashrate create higher prices? Empirically no. Over the past 6 months there has been a gigantic leap in hashrate for both Bitcoin and Litecoin yet market prices have decreased in that same time frame. Nor does a block halving lead to a doubling in market value of a token. It is not as if the entire existing mined money supply divides in half over night, rather it is just the block reward that does.

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 profitability per hash and thus disincentivizes the activity.²⁴⁰ And price, as in any market, is related to the supply and demand of the ledger entry.

\$40 transactions

One area of contention within the community is the assertion that the full costs of transacting on the network is being grossly understated. It is not free, it is around \$40 at the time of this writing (paid via token dilution).²⁴¹



Currently no one directly paid even \$90 at its height in December, the cost was borne by every holder of bitcoin through token dilution.

There are actual infrastructure costs that some adopters hand-wave away as if it is run by a miracle. Collectively most of the mining labor force will not achieve an accounting profit (let alone an economic profit); relying solely on the appreciation of the token to pay for their costs.²⁴² Conjoined with an automatically adjusting difficulty rating, proof-of-work via SHA256d or script (which are not the only types) ensures that the marginal value of a token in the long run equals to the marginal cost of securing the network ($MV=MC$). Furthermore, the marginal product of labor (MP_L) is zero, a phenomenon that David Evans addresses in chapter 5.²⁴³ Thus,

despite popular claims to the contrary, Bitcoin is in fact, enormously costly in terms of security relative to other payment and value transfer mechanisms.

Obviously the ratios will shift back and forth throughout time, but decentralization fundamentally insures it cannot be a cheaper or faster payments system than a centralized real-time gross settlement (RTGS) platform. Perhaps Peter Todd's treechain solution (soon to be implemented at Viacoin), Adam Miller's Permacoin, or Proof-of-Activity from Bentov *et. al.*, will be implemented in code but again, why would existing mining pools or farms protect code that is unprofitable relative to their sunk costs (a large minority have not even upgraded past 0.8.5. or 0.8.6 software still, what upgrade would fall within their time horizons)?²⁴⁴ Currently the best incentive compatible candidate is Proof-of-Idle from Tadge Dyrja, yet the changes so far have not been enough to get farms and pools to change and a hard fork risks a serious network partition.^{245 246}

Let's examine the problem another way. If block rewards were entirely removed today, how much of the labor force could continue providing their services in a profitable manner? The answer is probably none, as 99.8% of revenue at the time of this writing comes from the seigniorage subsidy. Hashrate would drop to an equilibrium relative to the transaction fees (or as Kerem Kaskaloglu calls them, "donations"). Since the number one marketing slogan for the network is "transactions are free" you could very well end up with a network that could be insecure from relatively cheap outside attacks because few are willing to pay fees high enough to incentivize that same level of security.

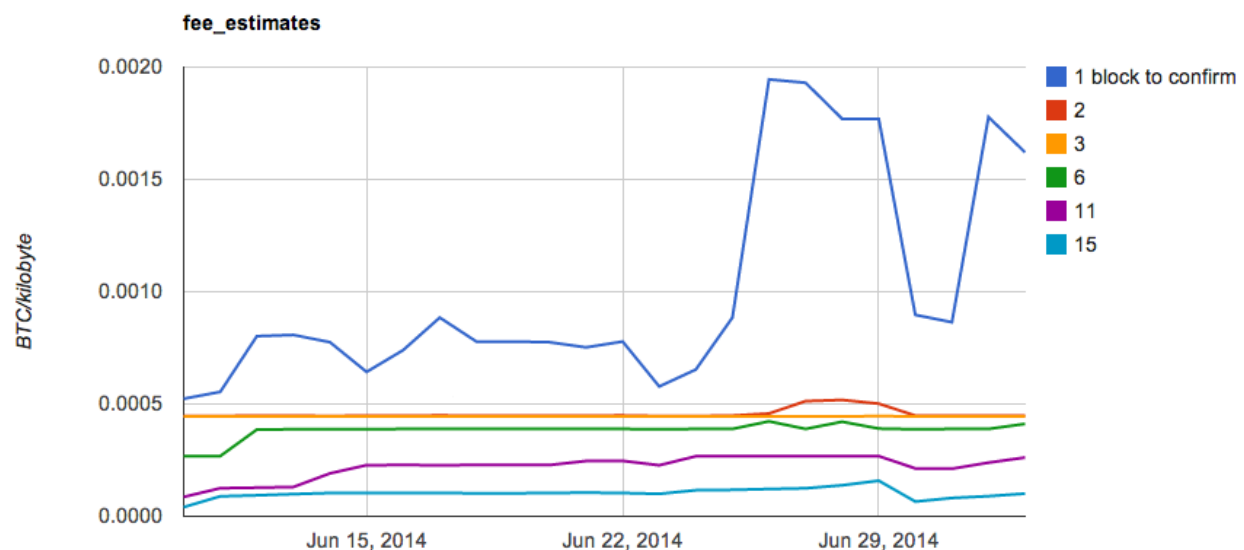


Image source: Gavin Andresen

The chart above was published in July 2014 by Gavin Andresen and illustrates bitcoin fees paid versus blocks-to-confirm over a one month time period.²⁴⁷ Or in other words, the higher the fee a user is willing to pay, the faster their transaction is included in a block (and thereby

confirmed). At a lower fee of around 0.0001 bitcoin (6 cents at current prices), 19 confirmations is roughly 3 hours of waiting time.

In July 2014, Tony Gallippi, co-founder and CEO at BitPay (a merchant payment processing company) explained to *Bloomberg* that transaction fees via BitPay were competitive to the rest of the industry:²⁴⁸

So if the benchmark where you think it is successful is 2%, I don't think we'll have a problem. Right now the average industry is at 1% and the transaction costs are going down from here because every company is able to add scale and add enhanced features. So when you actually look at a service like ours or others, the marginal cost we have to do a transaction is really just related to our overhead, our salaries our servers. It's the distributed network that really helps reduce the costs. You don't have to have a central data center like a Visa or MasterCard or American Express would. The distributed data center of the Bitcoin network is what validates the transactions and it's much more effective than any centralized data centers.

This is untrue; it is a focused benefit to them and a diffused cost to the world. BitPay outsources the actual labor to other parties, in this case about a dozen mining pools and 7,000 verification nodes to independently verify and process the transactions. That "datacenter" of miners costs real money as they remove scarce resources from the real economy such as computers and electricity.

Again, as of this writing those costs amount to around \$40 per transaction. These are hidden fees that eventually will have to be paid directly as the seigniorage subsidy declines. The seen cost, is the BitPay charge of 1% on top of the nominal Bitcoin network fee, which as Andresen illustrated above, varies depending on priority. Or as Peter Todd explained in July regarding the new BitLicense proposals, "a centralized Bitcoin is just a very expensive and uncompetitive copy of PayPal."²⁴⁹ A decentralized version was only less expensive on the edges – but equally as costly in infrastructure transaction costs – as there were no Know Your Customer (KYC) and capital reserve or adequacy requirements. A week after this interview Gallippi announced that in addition to offering its existing plans (such as a \$300 per month business plan with customer service support), BitPay would begin offering a new basic plan including free unlimited processing.²⁵⁰

In contrast, Visa does not externalize its costs onto 7,000 voluntarily run nodes spread around globally; its entire cost structure is built into the interchange fee (the "2%" fee in the example above). So in this case a central data center is more effective.

For comparison, the average network and processing expense per Visa transaction (\$414 million / 77.6 billion transactions) is \$0.0053. Similarly, the direct transaction costs for remittance firms like Western Union are relatively low. Instead, the fee assessed on top of the transactions (for Visa is actually 2.5% + \$0.20 or for Western Union, global average of 9%) goes towards paying for insurance, legal compliance, brick-and-mortar physical locations, fraud

protection and human network on the ground. For instance, current BTC ATMs charge a fee embedded into bid/ask spread. These same costs will likely be levied onto Bitcoin ATM remitters as well; it is not zero percent.²⁵¹

Again, this is not an entirely apples-to-apples comparison because both of these networks just transmit information and are not money creation (seigniorage) networks as well (which Bitcoin is).

Because there are, on average, 3,600 bitcoins created each day and a lower bound cost of securing these is currently around \$650 (MV=MC), the actual operating costs of the Bitcoin network are around \$2.3 million a day or \$854 million a year. When taken into account the relatively low volume of commercial activity on the same network relative to Visa or Western Union, the per transaction and security costs of Bitcoin are very high.

Another facsimile

The zeitgeist of 2014 also involves the decentralization of computing and storage through projects like StorJ, Filecoin and several others. Yet we have seen this before with the internet itself. It started out as a bunch of disparate computers connecting to one another, but eventually moved towards centralized server structures for cost and efficiency purposes. If it is in fact profitable to rent out your storage space, wouldn't Amazon do it with all of its spare storage space? Amazon Web Services (AWS) does not actually rent out their spare capacity, this is a bit of a myth as to how AWS got started.²⁵² They would have run out of spare capacity within two months of launch and actually add the equivalent of their entire ecommerce infrastructure every day.

If this were the logistical case, AWS and Google Cloud could sell their unused capacity and drive the market price down to that of their own offerings which have far superior performance.

In March 2014, to stave off Google, Amazon reduced the price points of its S3 services by an average of 51%:

Tier	New S3 Price / GB / Month	Price Reduction
0-1 TB	\$0.0300	65%
1-50 TB	\$0.0295	61%
50-500 TB	\$0.0290	52%
500-1000 TB	\$0.0285	48%
1000-5000 TB	\$0.0280	45%
5000 TB or More	\$0.0275	36%

Source: Amazon

And according to Quartz, due to price cuts like this, overall usage of Amazon Web Services increased 90% year-over-year.²⁵³

Yet these lower prices came at a cost, impacting Amazon's revenue growth:

Amazon Web Services price cut effect

■ Amazon North America "other" revenue ■ Year-over-year growth



For comparison, Dropbox charges \$1 per gigabyte per month and Glacier is \$0.01 per gigabyte per month although this may not be a fair comparison as they address opposite ends of the storage market; constant synchronization and archival.²⁵⁴

Storage is a commodity market and the price and margins continue to shrink. It is unclear how Bob with an extra 1 terabyte (1 TB) of space will be able to generate profitable revenue on a decentralized platform whilst competing with Amazon. Economies of scale favors centralization due to costs because individuals simply cannot buy a hard drive or bandwidth cheaper than Amazon or Google can. Compute and storage as utilities gravitate towards centralization for the same reason. Thus, why would Bob reduce his internet throughput so that he could make \$20 a year allowing others to access his spare hard drives? Once again, if decentralized storage services were successful or profitable then Amazon and Google would simply sell their spare capacity through this manner at much cheaper rates. Then it will end up becoming centralized like the cloud today.

What about uptime? S3 guarantees 99.9% monthly uptime, (i.e. not more than 42 minutes of downtime per month), yet because of synchronized, overlapping connections via multiple data centers, users almost never experience this.²⁵⁵

What is the down time of the Bitcoin blockchain? Depending on how it is accessed (via a centralized exchange or a desktop wallet), outages can vary from some to none. Yet as copiously noted above, this massive redundancy (or as Tomáš Rosa calls it a “massively replicated system”) comes at a cost.²⁵⁶

Put it another way, there are real costs to decentralization. And axiomatically decentralization of transactions will cost more than a centralized offering would.²⁵⁷ The network would be far cheaper if it was run by just one computer as it was the first year (via Satoshi Nakamoto) but that is not its advantage; distributing trust to prevent (or observe) shenanigans is. And it needs lots of geographically dispersed miners and nodes to do so, both of which are not free to acquire or run. These costs are what we see playing out in the digital currency space today.

This is a point reiterated by Jonathan Levin in his paper:²⁵⁸

The key objective of the system is establishing decentralised trust between anonymous parties. Cost effectiveness, remains a secondary concern. Indeed, a miner providing a cost effective service, obeying the rules of the protocol, may detract from achieving the goal of decentralised trust. In the extreme case where 51% of the computing power on the network is controlled by a single miner at a much lower cost than the rest of the miners, they are not the most efficient operator of the Bitcoin network as there is now trust in a central authority. In economic terms, it is tempting to say that a costly decentralized service provided by small users is inefficient but this would ignore the premise of the system.

Levin then pointed to Peter Todd’s apt definition of miners as service providers:²⁵⁹

When you say these small miners are inefficient, you're completely ignoring what we actually want miners to do, and that is to provide independent hashing power. The small miners are the most efficient at providing this service, not the least.

Modeling behavior

For future cryptolledger designers, these variables may be tunable with agent-based modeling (ABM) such as that proposed by Dave Babbitt (forthcoming) yet due to the *cui bono* mention above, it is unlikely that this can be changed for Bitcoin itself. Consequently Jonathan Levin, co-founder of Coinometrics, wondered “who will break the social contract first?”²⁶⁰

This issue of a social contract was also independently highlighted by Ray Dillinger in May 2014:²⁶¹

For what it’s worth, I’ve been looking at the question of mining (and premines, etc) a bit differently.

In my estimation, the block subsidies and transaction fees are what the investors (or holders) pay the miners to keep the blockchain secure. If these payments get too low relative to the value secured, then the blockchain becomes insecure and you get 51% attacks etc.

In that light the “standard” model we’ve been pursuing of block subsidies halving as the value secured grows larger seems dangerous. As the value we’re trying to secure grows larger, we intend to pay less for security. We shall, in that event, GET less security. I’ve been watching alt chains with faster halving periods dying like flies, and I can tell you for sure that this is something that’s real.

That brings us to transaction fees. We are paying to secure value, and we are not paying transaction fees relative to value. We are paying transaction fees relative to space. Space – which is to say hard drive sectors and network bandwidth – is not what secures our value; what secures our value is a monetary hardware investment in ASICs and powerplants. Which we need in proportion to the value we’re trying to secure. And which we will not get in proportion to the value we’re trying to secure by paying for space instead.

My conclusion is that if we want to keep the network at zero inflation and pay for security out of transaction fees, we should be paying transaction fees relative to the value of each transaction. And if we want to keep the network going without transaction fees that cost a percentage of the transaction, we should accept an inflationary model where each year the block rewards are, eg, 5% larger than they were the previous year. So, in the long run that approaches 5% inflation.

Both of these options are not popular with the current crop of BTC holders.

Again, in practice, a centralized system will be more efficient – copying a transaction once and then twice for security while applying SSL encryption only once is much more efficient than copying all transactions tens of thousands of times over and expending large quantities of

energy to maintain the hashrate for security. For instance, while it arguably would not be as secure, a user could spin up a virtual machine and database on any number of cloud platforms to recreate the same transportation functions as Bitcoin for a fraction of the cost.

Similarly, Bitcoin has the same fraud and theft issues as Visa – as will be discussed later, as many as 30% of all mined bitcoins have been lost, stolen, seized or destroyed. For Visa, these vulnerabilities are on the edges and not in the data centers (e.g., 40 million Target accounts being compromised).²⁶² However, Bitcoin has no way to resolve fraud unless you increase costs through multisig services or customer service.

If Bob wanted to build a system that is exactly the same as Bitcoin, he could just tell Visa to fire everyone in the fraud department, to not offer charge backs (even if the good or service is not delivered by the merchant) and to just charge people the cost of transaction plus a profit margin. He would end up with a Bitcoin-like system but with faster confirmation times as well as room for higher potential transactional volumes. This intersects with one purported advantage that Bitcoin has, no chargebacks (or “double spending”), which is not a feature that benefits consumers but rather only helps merchants which may be one explanation for why consumer adaption for retail purchases remains subdued.

In the end, Bitcoin adopters have to pay real costs for decentralization because being your own bank can be hard and infrastructure is not free. And according to a working paper from Andrew Miller and Joseph LaViola, these costs may be “unavoidable” in order to protect against vulnerabilities such as Sybil attacks.²⁶³

Ideal scenario

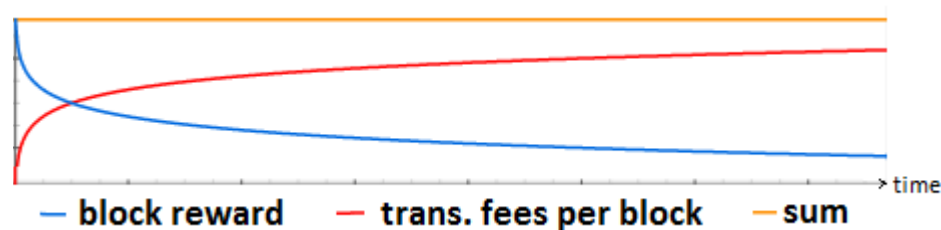


Image credit: Kerem Kaskaloglu

The figure above is from a June 2014 paper published by Kerem Kaskaloglu that illustrates the “ideal scenario” – the continuous switch from block rewards (seigniorage subsidy) to transaction fees (donations).²⁶⁴

But how to enforce this “ideal scenario”? In their paper, *Proof of Activity*, Bentov *et. al.*, explored three different tragedies of the commons, finding one that intersects this impasse:²⁶⁵

It is in the interest of every Bitcoin user that fees will be paid for transactions, to encourage miners to provide the network with a sufficient level of security; however, each user will prefer that others pay fees, while he pays no fee and still enjoys the

network security. Without a way to force users to pay fees, the vast majority of the users will avoid paying, and end up with an insecure system that is of use to no one.

The solution lies within the power miners have to reject transactions if the fee paid is not high enough. However, here we have another tragedy of the commons problem, between the different miners. Without protocol-enforced limitations on what can go into a block, a rational miner will prefer to include every fee-paying transaction, even if the fee is very low, because the marginal cost of including a transaction is trivial. If miners accept low-fee transactions, users will have no reason to pay significant fees, and the total fees that can be collected by miners will not be sufficient to cover the cost of PoW mining.

Obviously the subsidy will not disappear anytime soon, but trying to incentivize people to pay fees for faster inclusion (priority) into blocks when those fees are greater than the equivalent for competing services is an uphill task. This includes other less capital intensive cryptoledgers or “rails” from Ripple, mobile payment solutions from Tenpay (which received a license), Alipay (through Weibo), Google, Apple, or an RTGS from providers such as Visa.²⁶⁶

According to the current narrative, the cost per transaction will eventually go down as the network adds more transactions per block. However the increase in transactions (e.g., the demand for the usage of the network) will also increase the price of bitcoin (due to the demand for tokens) and because the marginal value equals the marginal cost, the argument that more transactions will lower the cost per transaction is not as clear cut. This is not to say that they linearly increase, it is not that simple. Historically both the denominator and the nominator increase. Perhaps upcoming floating fees (‘smartified fees’) will be one potential solution to this challenge.

David Evans, an economist and professor at the University of Chicago, explained this unclear incentive structure as to why would consumers collectively decide to adjust their fee upward:²⁶⁷

The transaction fee is the other possible lever for motivating the laborers. Whether the platform can set or adjust the transaction fee depends on the protocol the platform has adopted and the governance system. Bitcoin, for example, provides for voluntary transaction fees; the idea is that if senders offer a transaction fee, and a higher one, their transactions will receive a higher priority by the miners. Presumably a consensus would emerge. This mechanism for providing incentives is novel and there is no apparent reason why it would enable the revelation of efficient prices for laborers. Also, it is unclear whether the governance system for Bitcoin would enable the platform to establish mandatory transaction fees or to vary these fees based on the demand for effort.

There is a distinct possibility that such fees could price-out a portion of the underbanked in developing countries, some of whose daily wages are less than the cost of a transaction.²⁶⁸

Perhaps it will be surmountable, however for every hardware or software boost Bitcoin receives, there is a potential that other competitors such as Visa could benefit from that as well.²⁶⁹

Or perhaps, as L.M. Goodman argues, the fee structure will fall to an unsustainable degree:²⁷⁰

Indeed, in the long run, the total mining revenues will be the sum of the all transaction fees paid to the miners. Since miners compete to produce hashes, the amount of money spent on mining will be slightly smaller than the revenues. In turn, the amount spent on transactions depends on the supply and demand for transactions. The supply of transactions on the blockchain is determined by the block size and is fixed.

Unfortunately, there is reason to expect that the demand for transactions will fall to very low levels. People are likely to make use of on-chain transaction mechanisms via trusted third parties, particularly for small amounts, in order to alleviate the need to wait for confirmations. Payment processors may only need to clear with each other infrequently.

This scenario is not only economically likely, it seems necessary given the relatively low transaction rate supported by Bitcoin. Since blockchain transaction will have to compete with on-chain transaction, the amount spent on transactions will approach its cost, which, in a modern economy, should be close to zero.

Attempting to impose minimum transaction fees may only exacerbate the problem and cause users to rely on on-chain transaction more. As the amount paid in transaction fees collapses, so will the miner's revenues, and so will the cost of executing a 51% attack. To put it in a nutshell, the security of a proof- of-work blockchain suffers from a commons problem. Core developer Mike Hearn has suggested the use of special transactions to subsidize mining using a pledge type of fund raising. A robust currency should not need to rely on charity to operate securely.

This last point is salient, having to rely on charity is unsustainable. It would be akin to Visa asking the community to help propagate and verify transactions without compensation, which is the unsustainable job that fully verifying nodes are trying to do.²⁷¹

This intersects with another finding in the aforementioned *Proof of Activity* paper, by Bentov *et. al.*, stating:²⁷²

There is also a third tragedy of the commons problem, as the transaction fees are paid only to the miner who created the block, while the cost of propagating, verifying, and storing the transactions is shared by all the nodes in the network. Miners will prefer keeping every transaction to themselves and collecting a fee for it, while avoiding as much as possible the work of propagating it. Having a value cap for each block will not help in this regard, because the users as a whole may still wish to send a very large

amounts of low-value transactions. Here the solution is limits on data size and CPU cycles (currently dominated by ECDSA signature verifications) for each block, which is controversial since many users believe that the block size should accommodate the Bitcoin economy. *Proof of Stake* based protocols offer little help here, as they do not reduce these particular costs.

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

Could additional fees be levied on metacoins or coins located on sidechains to make up the difference? Perhaps in theory, though it is unclear how this could happen with the current codebase without a major hard fork and change in the economic structure of the network. For instance, to remain competitive with traditional incumbents, the fee must remain relatively low, otherwise financial firms will continue out competing them.

Or as Felix Simon wrote in February 2014:²⁷³

In theory, there are all manner of clever things which can be traded in a distributed manner, using the open-source bitcoin protocol; most of them involve “coloring” coins in some manner, so that a bitcoin serves as a token of ownership of something else. There is a lot of valuable rivalrous digital property out there, and a lot of companies, including Thomson Reuters, make a lot of money by helping to manage it. The technology involved tends to be tried and tested (to the point at which any failures are very big news), and the players involved tend to be extremely conservative. On top of that, the costs are often extremely low: the simple transaction costs involved in trading stocks, or large quantities of foreign exchange, are very close to zero these days.

So while in theory there is the possibility of disruption in this space, I’m not holding my breath. The Race to Topple Bloomberg, as the headline of Aaron Timms’s recent Institutional Investor article puts it, has been going on for the best part of 20 years now, with no visible success. (I first asked Mike Bloomberg whether he was worried about competition from the open internet for an article I wrote back in 1996.) I’m happy that Satoshi Nakamoto managed to solve the Byzantine Generals Problem — but while that might be a necessary condition for these particular walls to start falling, it’s far from a sufficient one.

As Simon explains, while cryptoledgers could be used to host a bevy of financial instruments, they might not be able to do so in a profitably competitive manner.

Reading the tea leaves

In the future, merchant processors like BitPay could on-ramp every merchant on the globe and someone else could potentially even solve some of the network delay issues in Jonathan Levin’s upcoming research, through the deployment and use of neutrino detectors.²⁷⁴²⁷⁵

Yet this is not to say that that increased transaction volume will necessarily require more energy usage. Even though transaction are packed into a block which is then processed and paid for almost entirely by seigniorage rewards which itself changes due to the fluctuation of token prices, the relationship between mining and volume is so far, a side note.

No one has to use the actual network (very few in fact do) for value to be burnt through heat processes.²⁷⁶ In fact, over the next 6 years, transaction fees could rise substantially (to offset the diminished block rewards) and as a consequence bitcoins may be solely used as a store of value, transmitted intermittently. Or as Richard Brown surmises: “the opportunity lies elsewhere: high-value payments, smart property and so forth.”²⁷⁷

Limitations

Cal Abel, a statistical modeler, suggested that future research look specifically at the *time value of money* by doing a conventional internal rate of return (IRR) analysis of a miner.²⁷⁸ According to him, “this will give you an idea of the cost of delaying the mining rig and its future obsolescence.” This could be done by quantifying the cost expended for utilities and real-estate and converting this dollar figure into energy by using what he dubs an energy price index (EPI). This could potentially give a researcher a measure of the computational efficiency (hash/joule of primary energy). Or in his words, “There is some quantum limit to the energy of a hash, which converts it into energy. This will give you the thermodynamic efficiency of bitcoin and allow you to measure transactions in terms of their ability to do work.”

Among the largest limitations to this approach however is creating a mean, a weighted average for an ASIC-based actor. Since the process of mining is itself decentralized, finding out the location of the miners – and thereby estimating local energy costs as well as the marginal utility of money (because exchange rates and purchasing power varies) – can be obfuscated in a number of ways. Furthermore, not everyone is using the same set of hardware. In all likelihood, the network is being oversecured by individuals who are providing inefficient hashrate (e.g., operating at a loss) at the network with the future expectation that these token (or more precisely, UTXOs) will appreciate in value.²⁷⁹

For instance, based on calculations provided by Dave Babbitt, if all miners were using a new “Minerscube” system, based on its theoretical hashrate, the Hoover Dam Equivalent (HDE) for wattage consumption of these would be 0.002 HDE.²⁸⁰ In contrast, if miners were all using the original first batch of Avalon, based on current network hashrate this amounts to 0.133 HDE being consumed. Another way of looking at the same phenomenon are estimates by John Ratcliff who based his on the net profit from the sale of bitcoins.²⁸¹ According to his estimates, the lowerbound is 0.25 HDE and the upperbound is 0.5 HDE.

Thus attempting to quantify the EPI will in practice require producing a range of estimates based on confidence values.

Conclusions

In discussing this issue with Robert Sams of Cryptonomics, he noted that, “Economic logic dictates that eventually all mining will become concentrated in certain areas due to electricity arbitrage, which defeats the whole point of proof-of-work (PoW). One subsequent prediction is that the main casualty of this will be the belief that mining should be an anonymous and permissionless activity.”²⁸²

In practice, increased anonymity has not been the case as mining pool operators are now accessible to 3rd parties for a variety of reasons.²⁸³ If PoW is to be workable in the long-run, miners will likely need to authenticate themselves to the network in some way – an issue actively being discussed by Mike Hearn over the past nine months – with some decentralized vetting process acting as a gatekeeper and potentially denying some of these miners the right to mine.²⁸⁴

The environmental dimension and China specifically should be taken with perspective: it is (currently) not a leverage point in the global picture as the automobile itself as a class is a much larger polluter by many orders of magnitude. They were used for illustrative purposes: perhaps other regions like Mongolia or Saudi Arabia will replace China and Moses Lake in the future.²⁸⁵ Furthermore, the backlash towards China in general related to bitcoin price levels is arguably unwarranted – if the purpose of a peer-to-peer decentralized electronic cash system is to enable and empower the underbanked, then developing countries like China should be embraced irrespective of token valuations.

One common hurdle due to the computational arms race that has arisen is that, proof-of-work scaling ends up moving beyond the reach of the intended hobbyist – moving away from “recreational mining.” Consequently, an unintended consequence is that capital accumulation and therefore mining operations end up in jurisdictions that have superior infrastructure and/or lower energy costs. That is to say, while the underbanked and unbanked are supposedly one of the oft cited use-cases for a decentralized electronic cash system, in practice the only way for those residents to participate today is to purchase tokens through an exchange, because they do not have access to capital for mining equipment or competitive energy sources. And in many cases, there are no reliable exchanges (or even ATMs) to buy from. But that is a topic for future researchers.

Internal to cryptocurrency, mining centralization could be viewed as a negative externality and this centralization is being driven by what Sams identifies as large differentials in \$/kWh.²⁸⁶ From this discussion above the key takeaway is the \$/ kWh factor which is the core dimension to mining concentration. Over the past two years the discussion has largely been centered on ASICs *qua* ASICs, which are not really an issue so long as no one entity has a monopoly on the chip design. Instead, \$/kWh is the real driver of concentration and future research can be conducted to propose methods for how to deal with it.

Sams proposed the following situation in which the network would apply a different difficulty to different miners, as a function of the price they pay per kWh.²⁸⁷ According to him, in their view, that would be a levelling and decentralizing force. However, in practice it can only be had

by sacrificing the anonymity and permissionless properties of PoW. Even then, it is not clear how to implement this technically, but it could be an area of research because the handwriting is on the wall for the current model. What is happening – geographic arbitrage – should make that clear to other outside parties.

In terms of Andrew Poelstra's intriguing "thermodynamic limit" to mining, it is valid regarding the physics of the computation. But the economics of mining has gone the opposite direction, a sort of antithesis of the Second Law of Thermodynamics, in the words of Sams "control of mining operations converge to minimal entropy, a monopoly at the limit, where one party with the cheapest source of electricity ultimately controls the network. Heat spreads out, wealth concentrates."²⁸⁸

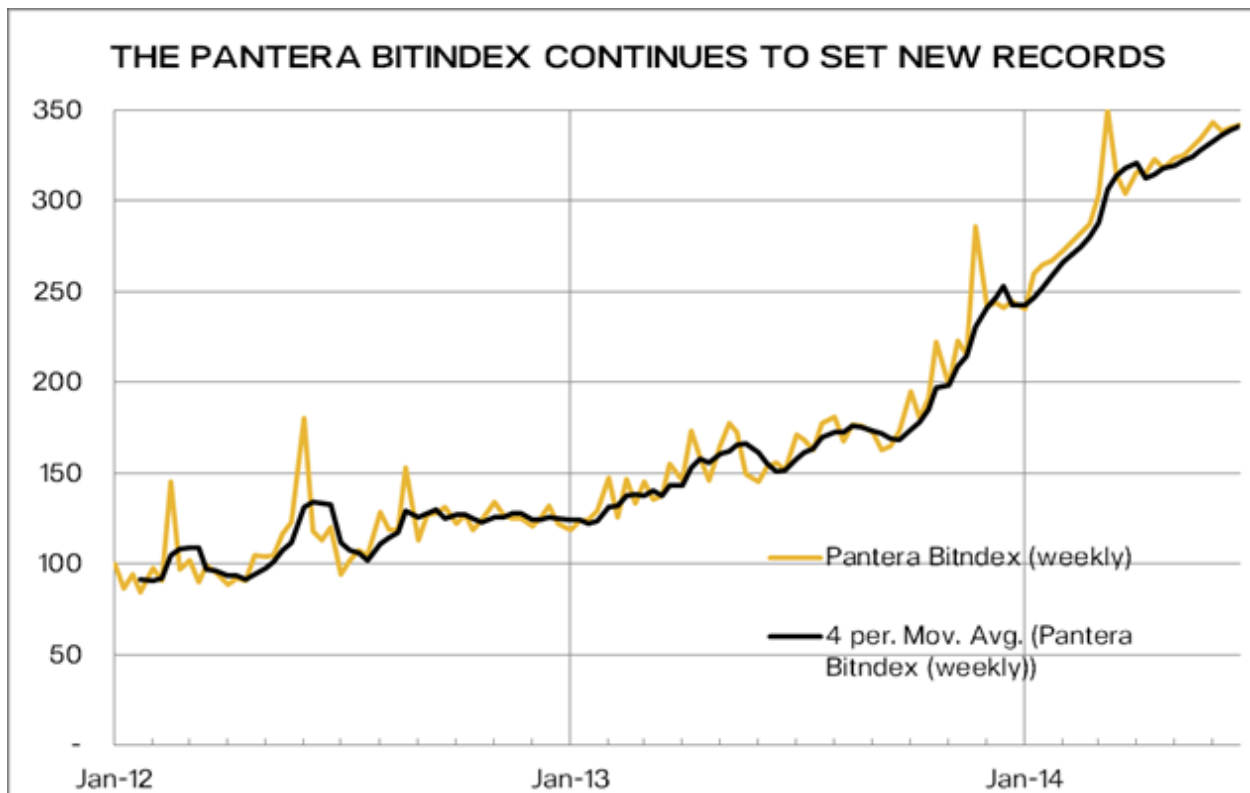
While the amount of energy consumed mining bitcoin will always be at least equal to the value of bitcoin produced this is not to say Bitcoin will fail as an experiment or as a store of value. Energy consumption in the long run is not necessarily a condition for success. And even though a relatively large amount of energy will be consumed while bitcoin "bootstraps itself" – it could decline. Future block halving's may actually end up reducing energy consumption rates if token prices do not rise in tandem.²⁸⁹

This topic will likely continue to fill numerous works in the future and should be looked at again in the coming months and years.

Chapter 4: A Bitcoin Gap

The charts in the chapter below are reused throughout the remaining sections of the book primarily because of their importance in probing the blockchain. Understanding how to read them is critical in discussing how to measure user adoption and growth.

For example, In July 2014, Pantera Capital, an investment fund focused on bitcoin, released their proprietary “BitIndex” which attempts to quantify bitcoin adoption without the use of monetary signals.²⁹⁰



In the chart above, the constituent parts are:

- Developer interest on GitHub
- Merchant adoption as a measure of consumer adoption
- Wikipedia views measuring bitcoin education
- Hashrate by logarithmic scale corresponding to orders of magnitude
- Google searches captured by the number of times “bitcoin” appears
- User adoption as measured by wallets
- Transaction volume on the bitcoin network

The problem with the first 6-out-of-7 components in the Pantera non-monetary index is that they precisely measure the wrong thing, interest, and fail to accurately describe the right thing,

adoption. Furthermore, in their announcement they mention that they intentionally underweight transaction volume; yet this is the only valid measurement in their entire index.²⁹¹

What does that mean?

In *Naked Statistics*, author Charles Wheelan describes a gift he received for Christmas one year: a laser golf range finder that he anticipated would improve his game due to its precision.²⁹² Yet this did not occur because it did not measure what really needed to be measured: accuracy. In his words:

There were two problems. First, I used the stupid device for three months before I realized that it was set to meters rather than to yards; every seemingly precise calculation (147.2) was wrong. Second, I would sometimes inadvertently aim the laser beam at the trees behind the green, rather than at the flag marking the hole, so that my “perfect” shot would go exactly the distance it was supposed to go—right over the green into the forest. The lesson for me, which applies to all statistical analysis, is that even the most precise measurements or calculations should be checked against common sense.

People use Wikipedia to find out information that is complicated, when they do not understand it. Thus, there is a difference between what Pantera wants to measure (adoption and growth) versus what they did measure (interest, education and awareness).

Despite a creative effort, Pantera is not measuring what it is trying to measure. If a key indicator as to whether or not economies (virtual or physical) expand is based on Wikipedia viewership (like Bitcoin supposedly is), then Brazil’s GDP will most certainly see huge growth because the entry for Brazil was ranked 53rd in mid-July 2014.²⁹³ The reality is that Wikipedia views of Bitcoin represents interest or education and not usage or adoption – or in other words, interest grows but adoption does not.

In mid-July 2014, O.J. Simpson was the 779th most popular Wikipedia entry but readers (probably) were not trying to figure out how to lead an interstate highway chase during rush hour. Similarly, several Transformer movie entries rank in the top 350 but it is also unlikely that there was a simultaneous underground, organic movement for creating origami-like talking animatronics on wheels. Interest is not leading to adoption (conversion rates), why? As a friend explained to me, perhaps it is akin to opening lines at a movie: if they like it there will be lines, if they don’t then there won’t be. Maybe people, despite their awareness and exposure to Bitcoin just don’t like it or have no use for it.

The problem with the github commit component is that it is an input divorced from its output and suffers the same problem that *U.S. News & World Reports* (USNWR) statistics fail with in regards to ranking colleges. For instance, some of the metrics for USNWR deal with incoming GPAs, standardized tests and alumni donations which may correlate with a successful collegiate

career for some students but do not necessarily cause it or lead to success afterwards. More on this later below.

What about on the output side of Bitcoin? How do we measure that with the protocol? One is if nodes and miners have upgraded their software.

Or in other words, at least two components of their index can be gamed, github commits and Wikipedia edits, and consequently the future of Bitcoin can get exponentially grander by merely spending a few dollars on Mechanical Turk.²⁹⁴ For instance, Belkin, the electronic manufacturer was in the limelight 5 years ago for astroturfing: hiring people to write 5-star reviews of its products via the Mechanical Turk platform.²⁹⁵ Just as “click farms” have been created to inflate “Likes” on Facebook pages, there is no reason Mechanical Turk could not be used for making Wikipedia edits to juice that part of the index as well.²⁹⁶

Likewise, the number of commits a github repo has, while on the face of it seems to measure developer activity, but it is unclear what the quality of these commits are or whether or not they are eventually removed. Or more importantly, whether or not the code is shipped and installed by miners and verification nodes. And this, the BitIndex does not measure: one-third of all nodes are still running version 0.8.x which are over a year old. Similarly, if a serious flaw and vulnerability was found in the core Bitcoin code base (bitcoind) which caused a cascade of hard forks that destroyed Bitcoin entirely, the github commit component would precisely measure the wrong thing, inputs, rather than an accurate attribute: healthy production code. In fact, that measure would spike, leading observers to believe that this collapse is good news for Bitcoin.

Charles Wheelan also describes this input versus output problem with USNWR which concurrently befalls the BitIndex. For example, why should alumni giving count for 5% instead of 1% or 10% in the USNWR? And what is the exact weighting for these corresponding seven components in the BitIndex? In his words:²⁹⁷

For all the data collected by USNWR, it's not obvious that the rankings measure what prospective students ought to care about: How much learning is going on at any given institution? Football fans may quibble about the composition of the passer index, but no one can deny that its component parts—completions, yardage, touchdowns, and interceptions—are an important part of a quarterback's overall performance. That is not necessarily the case with the USNWR criteria, most of which focus on inputs (e.g., what kind of students are admitted, how much faculty are paid, the percentage of faculty who are full-time) rather than educational outputs. Two notable exceptions are the freshman retention rate and the graduation rate, but even those indicators do not measure learning. As Michael McPherson points out, “We don't really learn anything from U.S. News about whether the education they got during those four years actually improved their talents or enriched their knowledge.”

All of this would still be a harmless exercise, but for the fact that it appears to encourage behavior that is not necessarily good for students or higher education. For example, one statistic used to calculate the rankings is financial resources per student; the problem is that there is no corresponding measure of how well that money is being spent. An institution that spends less money to better effect (and therefore can charge lower tuition) is punished in the ranking process. Colleges and universities also have an incentive to encourage large numbers of students to apply, including those with no realistic hope of getting in, because it makes the school appear more selective. This is a waste of resources for the schools soliciting bogus applications and for students who end up applying with no meaningful chance of being accepted.

Merchant adoption, as we have seen throughout this book, bears little correlation with consumer adoption in Bitcoin. In fact, merchant adoption tripled in the first half of 2014 without a similar increase in consumer usage. Hashrate similarly does not measure adoption, but rather, hashrate. Because of a steady decrease in distributed miners, the network is qualitatively less secure due to centralization and this is not measured or captured by hashrate. The hashrate is distributed not at the mean, but on one tail, leading to cartelization concerns.²⁹⁸ As noted by Jeff Garzik in chapter 1, for all intents and purposes the Bitcoin network is merely comprised of 12 people (mining pools) and at most 7,000 fully validating nodes and declining.

Google searches, as shown in chapter 9, has seen a continual decline since its absolute peak in December and correlates largely with the media boom-bust cycle. Perhaps this will pick up in the future, but this is not an accurate way to gauge adoption. Similarly, the increase in the number of installed wallets is not the same as the number of actively used wallets let alone user adoption.

For example, the amount of downloads of all Linux distributions is in the tens of millions but the amount of active users of desktop Linux is a small fraction of all operating systems by users (it varies between 1%-1.75%).²⁹⁹ Download and installation does not mean usage. As noted later in chapter 8, the Bitcoin Android wallet has had a horizontal usage rate since February 2014 and because it is the most popular wallet it is possible that most other wallet providers have seen similar trends.

For example, the number of Blockchain.info “My Wallet” wallets steadily increase each month yet the corresponding “My Wallet Number of Transactions per day” and “My Wallet Transaction Volume” remains relatively flat the past six months: users probably forgot their wallet password and/or create a new wallet for each of their transactions.³⁰⁰ Or in other words, the number of “My Wallet Users” does not correlate with usage which likely means they are not new users. Contrary to Blockchain.info’s statements, they do not actually have 2 million users as they are conflating wallets with users.³⁰¹ Similarly, as shown several times, the collective transaction volume on the Bitcoin network is flat and has been for 7 months despite significant merchant onboarding and increase in “wallet users.”

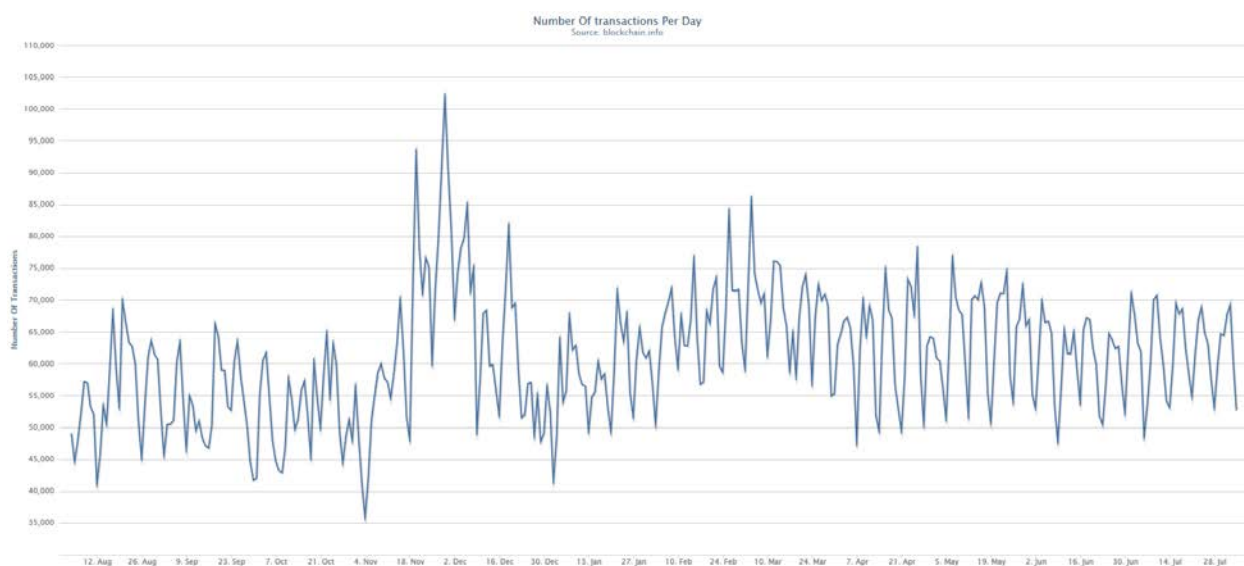
Brett King, author and founder of Moven, independently pointed out a similar phenomenon in July 2014:³⁰²

If we look at the most successful mobile payments initiatives in the US today, then the best candidates would be the Starbucks mobile app, Venmo and Dwolla P2P apps, and the mobile wallets of Google and ISIS. Bitcoin global transaction volume in USD peaked at US\$180 million in June according to Blockchain.info, but the problem we've got is that it is unlikely that that transaction volume correlates with mobile wallet usage, in fact, we know it doesn't. If it did we'd see wallet downloads improving transaction volume.

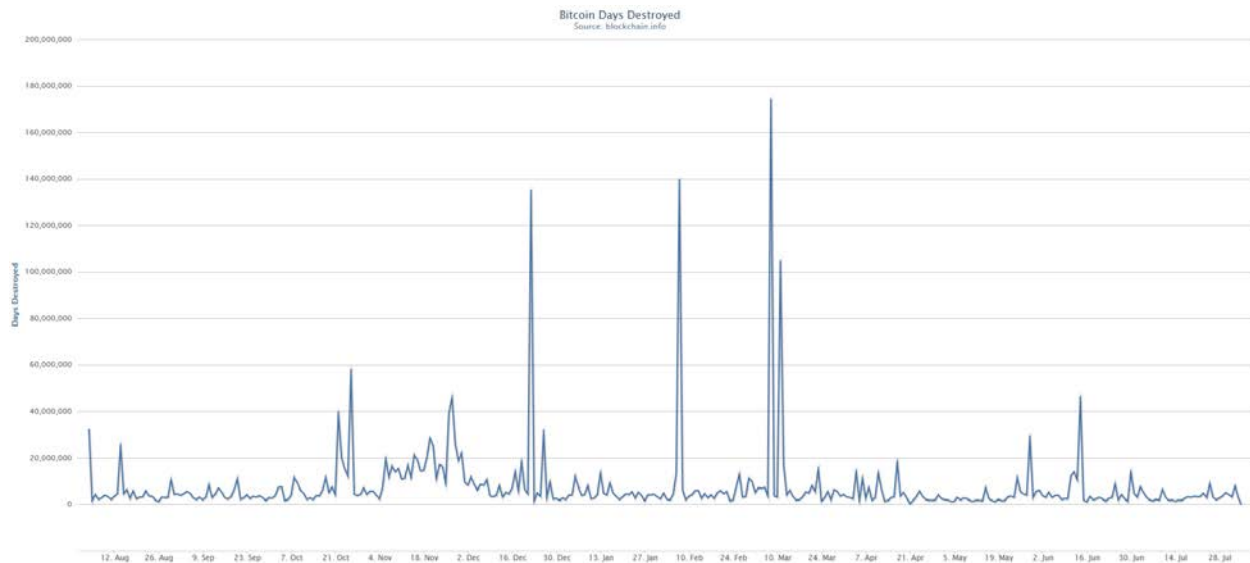
The more likely conclusion is again, these are not new users being added at Blockchain.info but instead are existing users creating new wallets because they misplaced their passwords or for features like Shared Coin (e.g., coin mixing).

How to measure the adoption and growth of bitcoin?

There are four charts that I show throughout this book that use data from the blockchain, the public ledger, which shows what is actually taking place on the network. Instead of guessing with laser range finders, I would argue that the four indicators taken together paint an accurate picture of adoption and usage: Number of Transactions Per Day (Transactional Volume), Bitcoin Days Destroyed, Miner Fees and Total Volume Output. Below is a description of each one.



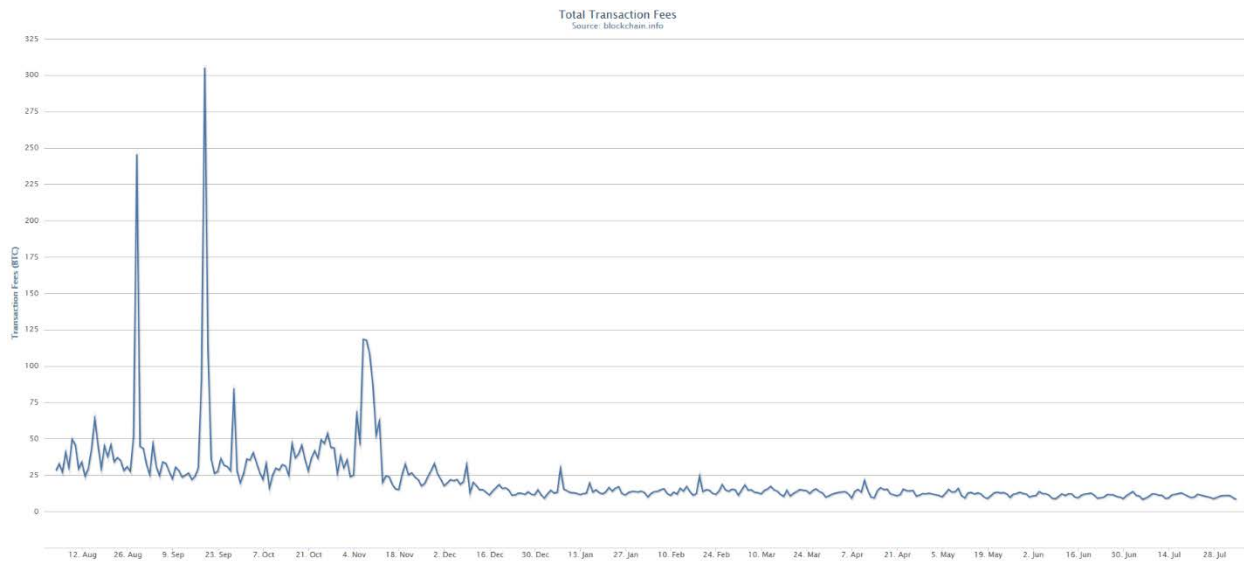
The chart above is the on-chain transactional volume over the past year.³⁰³ As noted throughout this study, in terms of visualizing consumer usage, this is arguably the most important chart. Despite a tripling or even quadrupling of merchant support, there has been very little corresponding on-chain growth. Instead, most of the growth is on the edges, in trust-me silos. The spikes in late November, early December 2013 correlate with the boom in market prices for bitcoins.



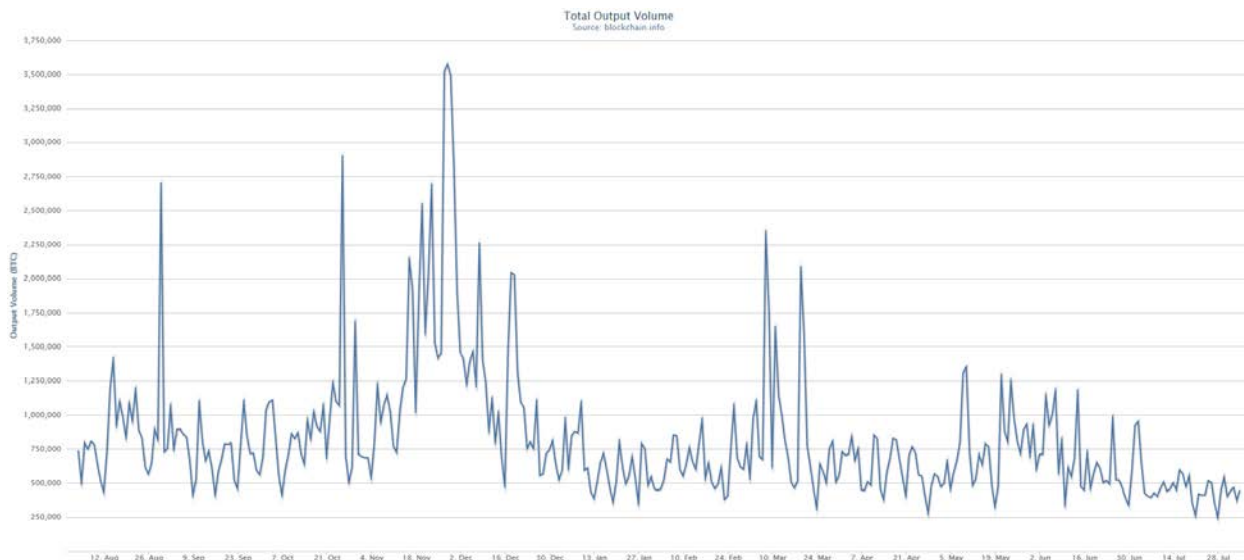
The chart above visualizes bitcoin days destroyed (BDD) which essentially measures old coins that move.³⁰⁴ Basically, the older and larger the amount, the larger the leverage point (as statisticians call it).³⁰⁵ In the case, the occasional leverage point spikes involve exchanges moving wallets from one wallet to another (such as Bitstamp did in November 2013 and Mt. Gox purportedly did in March 2014).³⁰⁶

Regarding BDD, according to Jonathan Levin, “it seems that aside from the big spikes which are ‘security measures,’ there are relatively few Bitcoins that are being actively traded and moved around the blockchain. Estimating this amount of supply comes from pie charts [from chapter 12]. I would give an estimate for this “active supply of bitcoins” by taking the 6 month figure.”

Why is BDD important? It indicates the movement of old, stagnant tokens as shown in numerous graphs. Remember, the liquidity of bitcoin is itself volatile, ranging from several thousand bitcoins a day to several hundred thousand bitcoins a day globally. The “old bitcoin rich” cannot actually liquidate – they are, for all intents and purposes, paper bitcoinaires. Hence the reason why merchant processors in essence are simply exits for early adopters who have bitcoins to spend, yet they rarely spend.



The chart above measures Total Transaction Fees (TTF), the total bitcoin value of transaction fees miners earn per day.³⁰⁷ These are the seen fees and currently represent, at the time of this writing, between 0.2% and 0.4% of the total miners revenue which is more accurately captured in the Cost Per Transaction (via the block reward subsidy) discussed later in chapter 11.³⁰⁸ Nonetheless, TTF is important because if more Bitcoin was attracting more on-chain users, they would collectively be paying more fees to miners for their transactions. As visualized above, TTF has been flat since November 2013 reinforcing the view that there has not been a large growth in on-chain usage (off-chain is not depicted as that information is proprietary).



The fourth chart (above) shows the Total Output Volume, the total value of all transaction outputs per day.³⁰⁹ This is a good measure for visualizing the upper bound, the maximum amount of bitcoins that are sent in any given day. As seen here, the trends correlate with

trading activity centered around the late November, early December 2013 boom. If bitcoin adoption and usage was increasing exponentially as some advocates claim, this chart would capture that.

Yet why doesn't total output volume tell us the whole story of bitcoins used each day? Because it also includes "change" from return addresses which can throw off the real number by an order of magnitude upward; the real number is likely lower than shown above. The issue again is: is Charles Wheelan (or Pantera) measuring what was intended to be measured? Or is he using the laser range finder on the golf course, failing to see the forest for the trees?

For instance, during the early years of the Cold War a Soviet bomber was unveiled, Myasishchev M-4 Molot, that Western intelligence agencies were in retrospect, unable to quantitatively measure leading to false assumptions and policy *faux pas* – a "bomber gap." This *maskirovka* (Russian, for military deception) was recounted in *The Space Shuttle Decision*:³¹⁰

Then, on May Day of 1954, at a public air show, the Soviets showed off a new jet bomber, the Bison. Here was another surprise—a Soviet jet bomber. It was all the more worrisome because no one in the U.S. had known of it until the Kremlin displayed it openly. A year later, in preparations for the next such air show, American observers saw a formation of 10 of these aircraft in flight. In mid-July came the real surprise. On Aviation Day, Colonel Charles Taylor, the U.S. air attaché in Moscow, counted no fewer than 28 Bisons as they flew past a review in two groups. This bomber now was obviously in mass production. The CIA promptly estimated that up to 800 Bisons would be in service by 1960.

In fact, Taylor had seen an elaborate hoax. The initial group of 10 Bisons had been real enough. They then had flown out of sight, joined eight more, and this combined formation had made the second flyby. Still, as classified estimates leaked to the press, Senator Stuart Symington, a former Air Force Secretary, demanded hearings and warned the nation of a "bomber gap." The flap forced Ike to build more B-52 bombers than he had planned, and to step up production of fighter aircraft in the bargain. Yet even when analysts discovered the Aviation Day hoax, they took little comfort. If Moscow was trying to fool the CIA, it might mean that the Soviets were putting their real effort into missiles rather than bombers.

This is similar to the illusion of a Potemkin village (Потёмкинские деревни) a fake village used to impress outside dignitaries. The most infamous was staged when Empress Catherine II of Russia visited Crimea in 1787. Her lover, Grigory Potemkin (namesake of the illusion) allegedly built fake villages with façades in the areas she travelled near; even going as far as to dress up as a villager all in an effort to fool Catherine by concealing the poverty of the area.

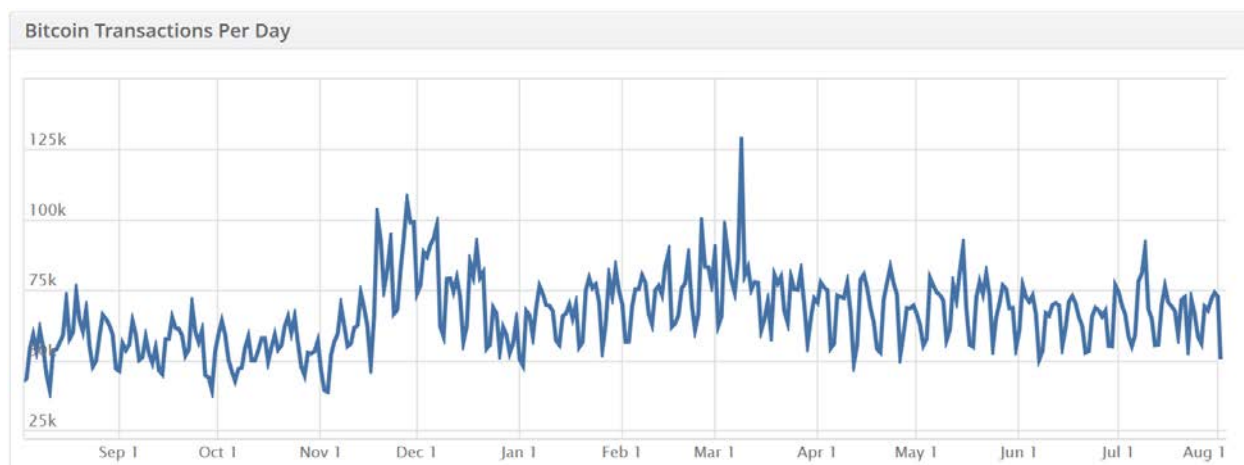
Measuring growth and in this case adoption and wealth is not just for history books but can also help market participants accurately view what is going on in a system like Bitcoin. The contemporary example corresponding to the Bison bombers would likely be subscribers and

commenters at reddit Bitcoin, many of which are sock puppets and/or spam accounts used to game the karma system (i.e., systemically promote a scam or phishing website).



For instance, in the first week of July 2014, reddit subscriptions (pictured above) noticeably jumped by an order of magnitude.³¹¹ Was this new adopters rushing into the subreddit? Possibly, but probably not.

The last chart (below) for this section comes from Coinbase, a large consumer and merchant wallet provider.³¹²



Source: Coinbase

According to Brian Armstrong, co-founder of Coinbase, this also includes off-blockchain transactions (any under 0.25 bitcoins) between Coinbase users.³¹³ As of this writing, 0.25

bitcoins is roughly \$150. What is noticeable is the same trend observed with the on-chain data, relatively flat transactional volume.

Or in other words, the reason the bitcoin price did not jump on news that Dell (the computer company) had partnered with Coinbase and accepted bitcoin payments in July 18, 2014 (as well as other supported merchants in previous months) is because very few people spend bitcoins in general and because there is no reason to use bitcoins to buy a Dell product when the same targeted consumer base already has credit cards. CheapAir.com, an online travel agency, did not fare much better, generating \$1.5 million in bitcoin payments between November 2013 and July 2014.³¹⁴ If the average flight is \$300 roundtrip, this would amount to about 5,000 flights over the span of about 8 months.

It is unlikely that someone who has enough bitcoins to buy a computer or plane ticket doesn't already have a credit card that can do the same thing. Instead, bitcoin holders are going to use bitcoins for things they need which credit cards cannot be used for, not things that advocates on forums think the bitcoin holder needs. Again, there is a difference between the consumer behavior Bob wants to have versus what does happen. And at this time, based on observed actions, bitcoin holders do not necessarily need or want wares from Dell or CheapAir.com.

Bitcoin Market Opportunity Index

To be even handed, Pantera's BitIndex is not the only inaccurate measure of growth and adoption. In August 2014, Garrick Hileman published an experimental Bitcoin Market Opportunity Index (BMOI) which attempts to rank countries that will most likely adopt bitcoin. Based on his metrics, Argentina is purportedly the most likely.

There are a number of fundamental flaws with his model, almost all of which involve the same problems that Pantera had:

Table 3: Bitcoin Penetration Sub Index Variables

Category	Variable	Sub Variable	Source
Bitcoin penetration	Global bitcoin nodes	a) Total Bitcoin nodes	Bitnodes.io
		b) Global Bitcoin nodes per capita	Bitnodes.io / World Bank
	Bitcoin client software downloads	a) Total client downloads	Sourceforge.net
		b) Client downloads per capita	Sourceforge.net / World Bank
	Google 'bitcoin' searches		Google Trends
	Bitcoin VC investment		CoinDesk

Source: Garrick Hileman

Above is a table which describes the variables he used in determining the rank-order of countries.

Yet these metrics are not measuring actual adoption or usage of bitcoin. In actuality:

- Global bitcoin nodes have dropped over the past year. In the past 60 days alone, the number has fallen from 7,672 to 7,089 nodes.³¹⁵³¹⁶
- Bitcoin client software downloads measures wallet inflation, not usage or adoption. Users cannot access the network without bitcoins.
- The search term "Bitcoin" on Google, as shown later in chapter 8, has continually dropped since its peak in December 2013.
- Bitcoin VC investment is not necessarily an accurate metric for measuring usage or adoption. As explored in chapter 13, Cleantech also attracted several billion in VC and angel funding. Yet it was unsustainable as most entrepreneurs were unable to build profitable business models and as a result, many went bankrupt.³¹⁷

The full list of all 37 variables that Hileman uses is, as of this writing, inaccessible.³¹⁸

Hileman's methodology also includes set of variables, 39, including: technology penetration, remittances, inflation, black market, financial repression, bitcoin penetration and historical financial crisis. As of this writing, the full set of variables are unavailable.

Using a series of equations and weightings, he then produces the following table:

Table 5: BMOI Top 10 Countries

Ranking	Country Name
1	Argentina
2	Venezuela
3	Zimbabwe
4	India
5	Nigeria
6	Brazil
7	United States
8	Nicaragua
9	Russian Federation
10	Iceland

Source: Garrick Hileman

The table (above) is a list of countries that are, according to Hileman, the most likely to adopt bitcoin. Ignoring the economic issues discussed later in chapters 9 and 10, it is unclear how Zimbabwe, India, Nigeria or Nicaragua could adopt it from an infrastructure point of view.³¹⁹ It is also unclear why policy makers in the remaining countries would officially adopt it as well.

To compound matters, it is unclear what adoption actually means using this methodology. Does this mean that Argentinian central bank will begin buying bitcoins on the open market and then pay overseas bond holders with bitcoin?

In his words:

One of the first questions that arises in constructing a bitcoin adoption index is: what type of adoption should the BMOI measure?

For example, should the BMOI focus on where bitcoin is most likely to be used as a store of value? Or should it measure bitcoin's commercial potential as a medium of

exchange? And which of these two is more likely than the other to influence bitcoin's geographic progression? The answers to such questions have a significant influence on the choice of index variables and weightings.

These are important questions and are thoroughly dissected later in chapter 9 and 10. The short answer to the second question is that bitcoins are a poor store of value due to their volatility – in the process of editing this book the market price of bitcoin fluctuated about 11% (between \$564-\$634).³²⁰

Furthermore, it is unclear how Argentina's policy makers could adopt bitcoin as-is today. The monetary stock ("market cap") of bitcoin is about \$7.7 billion. On August 1, Argentina defaulted on about \$29 billion in debt.³²¹ The logistics of how this transition could take place is not clear in Hilemann's explanation and since Argentina's bondholders would likely want to instantly cash them in, trying would crash the market. This is further explored in the following chapter.

Mobile goal posts

As seen in throughout this chapter, a quandary for this space is that few people are actually looking at data that reflects the real health of the network. On the one hand there is a public, independent, transparent database called a blockchain that advocates are quick to point to as a disruptive technology because it is purportedly immutable. Yet when it comes to looking at behavior on this blockchain, very few people or organizations have discussed what is actually happening on it preferring to look at indicators that may be more favorable to their inclinations.

More often than not, such discussion devolves as the "goal posts" – the metrics considered as valid – are moved to some undefined point in time in the future in which these same measurements are then allowed to be valid. In the interim, the sole barometer and focus by many, seems to be price levels, which if John Kenneth Galbraith's works (discussed later in chapter 13) are any indication, could be a sign of unsustainable bubble activity.

Arguably the primary technological breakthrough is the blockchain and bitcoin (the currency or commodity or luxury good) is simply the first "appcoin;" one of many.³²² In fact, there are at least 83 other uses for it and multisig itself opens up a new world for managing digital and digitized assets.³²³

The next chapter discusses a couple potential uses-cases and where an ever increasing amount of bitcoins are born.

Chapter 5: Bitcoins made in China

Moses Lake, Northern Europe, Canada and now parts of China. What do these geographic regions have in common? Relatively cheap electrical costs and an environment that is increasingly conducive for acting as a natural exergetic heat sink. In the case of China, the issue is more complex because mining is incentivized by subsidized coal power plants – the actual costs of operating a mining farm in China are externalized by taxpayers in China.

Why are farms moving to these regions in the first place? *Guanxi*.

If you have never lived or worked in China then you are likely unaware of the all-important concept of *guanxi* (social connections). While the People's Bank of China (PBOC) has alluded to the fact that it does not want China to lead the globe in either Bitcoin volume or regulatory governance, *guanxi* – or lack thereof – is what likely doomed Bitcoin exchanges. Exchange operators did not have the right *guanxi* with the right government officials. Despite the seeming financial success of several Bitcoin exchanges, they still could not overcome the political issues as it relates to personal connections; thus the effort needed to obtain the correct *guanxi* for survival was apparently beyond the financial incentives of operating an exchange.³²⁴

In contrast, miners in China have taken a different approach and have found the right people with the right *guanxi*. One such team is working within the current system and has access to a double digit megawatt power facility. When coupled together with 3rd party chips, the production costs are less than \$0.60 / gigahash. It bears mentioning that who Bob partners with has no relation to the production price of Bob's hashing machines, but it is important in other areas. There are at least three other funded teams in China with 3rd party chips (e.g., A1 and "fried cat") with access to similar energy sources.

In terms of pooled versus solo mining, some of these teams have little experience operating and optimizing their own internal networks (to efficiently propagate blocks in and out of their hashing stations). Others are more malevolent, using denial-of-service (DoS) attacks to reduce their competition. The longer you are offline, the less time you have to hash for a target value (nonces) thus preventing you from receiving block rewards which currently account for roughly 99.8% of the miner's income.³²⁵ Yet it should be noted that since mining pools began to aggregate in late 2010 (with Slush) in early 2011, DoS attacks have occurred on a global level and are not merely a Chinese phenomenon.

Throwing a wrench into this issue is the Chinese internet itself because there are essentially just two state-owned providers, China Telecom and China Unicom and they are not exactly best friends. And the Great Firewall (金盾工程) itself could potentially affect network block propagation.³²⁶

Despite these issues, the major draw of China continues to be the land, electrical and labor

costs. This has been the case for several years as the national rate for industrial usage in both India and China have hovered at approximately 8 cents / kWh which is significantly lower than others such as Denmark at 41 cents / kWh.³²⁷ In contrast, Moses Lake in Washington State has made headlines for its 1.7 cents / kWh rates which have attracted numerous farms. There are many other parts of the state which are very low, some averaging 2.3 cents per kWh. Consequently, the individuals who helped me with this section noted that Washington has a much better infrastructure (both for electricity and internet) than China, which makes it a very competitive geographic region globally.

Yet in China, some commercial operators can get electricity for 3 cents / kWh.³²⁸ And if you have the right connections (*guanxi*), you can get it essentially for free. Now, of course it is not free. Nothing is free. Someone bears this cost and that cost is borne by Chinese taxpayers and the environment because these energy generating facilities are almost all coal-powered power plants.³²⁹ While pollution may seem to be a non-issue to most redditors and North American bitcoin holders, these subsidies act in much of the same way as botnets did two years ago, externalizing the true costs of the network, distorting the marketplace by incentivizing activity (mining) that would not exist in an actual open market. Or in other words, *ex-China*, mining operations would likely still be taking place in other regions and the collective network hashrate and therefore difficulty rating would be lower enabling other marginal miners to still compete.

Outside participants cannot unilaterally blame the Chinese for this as other similar distortions existed in the past. Botnets operated by various malware authors (especially in Eastern Europe and the former Soviet Union) did and continue to externalize the costs of hashing.³³⁰ In fact, traditionally, the Russian basis of electricity is even cheaper and “social connection power” even more skewed. As a result, there has been an overland migration of outdated gear – uncompetitive gear relative to electrical costs goes over the border from China to Russia. It happened with GPU and FPGA farms and now outdated ASICs will likely migrate as well.

Furthermore you do not have to be Zhang Xin (a real-estate magnate in Beijing) to necessarily benefit from this type of private-public arrangement: other less connected mining operations in China still have access to relatively cheap systems, that once tweaked can operate at significantly less than \$1 / gigahash and their pricing has nothing to do with electricity costs. For instance, with these sub-10% hashing farms, because virtually all ASIC chips are now being manufactured in Taiwan, costs come down to volume size and chip cost which are concluded via negotiations.

Cloud hashing

In terms of the global supply chain, 90% of ASIC chips are made in Taiwan (TSMC), others go through Singapore (Global Foundries), and the remaining parts (PCB, SMT, power, fans, integration) almost all goes through Shenzhen.³³¹ Or manufacturing will have to in the near future. One estimate explained to me by a mining operator in China is that allegedly more than 50% of all mining may be going on in China and likely more could come online due to these manufacturing cost savings and incentives.³³²

One particular enterprising Chinese individual has figured out how to do a shanzhai (山寨) form of cloud hashing. While specific commercial numbers are proprietary, the rate comes to less than \$2 per gigahash. For comparison, CEX.io (which currently operates the largest mining pool, GHash.io) is around \$2.9 per gigahash and Cloudhashing (in Austin) is around \$5-\$7 per gigahash. Even KnC, which is built its own 10 MW power plant in Sweden will unlikely be able to compete long-term at these rates unless it continues its current business practice of using customer-purchased hardware first before shipping later.³³³ In addition, even with Moses Lake competitive rates of 1.7 cents, operators in the US (and Sweden) have to deal with a variety of tax and environmental issues which at this time do not exist in China.

The same source estimates that all told there are at least 2 Western companies and another 5 Chinese companies developing and deploying mining pools in China. In addition, there are also cloned and counterfeit chips running in the wild which can impact the performance of pools (i.e., burn out boards due to fraud). Thus in his estimation, given sluggish prices in bitcoin and rapid growth rate of difficulty this could lead to an unsustainable situation in the medium-term. Or in his words, “irrational exuberance and excitement are being replaced by cold math and a few bankruptcies.” One such bankruptcy was Alydian.³³⁴

Furthermore, historically the most important factor to a miner's profitability is fast access to the latest chips. Actually, according to professional miners, the most important factor is access to a *working* system with the fastest chip. Because these chips draw so much power, it is hard to produce stable, working systems. For instance, Hashfast, purportedly had the best chip in the world, but failed to ship working systems due in part to power issues and is now in bankruptcy.³³⁵ A few days of hashing with the newest ASIC chips, when you were hashing at magnitudes faster than the competition, will more than cover the electricity costs for the lifetime of the chip.³³⁶ This is an issue that will likely need to be researched more within the next two years.

And barring changes in the incentivization framework, China will continue “exporting” coins.

Other considerations

According to the sources who helped provide information on this chapter readers should be aware that:

- The four main regions for mining are: Inner Mongolia, Dongbei (northeast China), Shanxi (all coal), Sichuan (hydroelectric)
- While certain regions in China have cheaper electricity relative to other countries, relative to Washington and Russia (with 1 to 1.2 cents per kWh) the Chinese capacity is still limited by State Grid, a large state owned enterprise (SOE) with a flat rate of 0.3 RMB kWh buying in any power station linked to it. Miners will likely be unable to go under that.

- While Alice can do some meter fiddling or go off grid power, those options are hard to find and probably will not last long.
- State Grid has likely heard of bitcoin mining, but the wattage usage is not big enough to pique their interest or oversight.
- Inner Mongolia, as part of China, has overinvested in wind farms. Yet there are large areas that are not linked to the grid yet. And due to the unstable nature of wind, as well as poor internet infrastructure, none of the mining pools has gone there yet. And it is sparsely populated which leads to potential difficulties in sourcing human capital and talent to run a pool.
- Mongolia, the country, imports roughly 10-20% of its electricity from Russia, so Bob might as well go to Russia if he is willing to set up a facility in Mongolia.

According to another Chinese source, Carol, there are a number of other moving pieces at play that are fluid.

For instance, providers such as HashRatio (similar to GHash.io and Cloudhashing) have succeeded, not by designing their own chip but by figuring out the best combination of system and power configurations. Going from chip to working system is non-trivial. The end result are systems which are not necessarily pretty to look at, but they work.

And as noted at the beginning of this chapter, one of the ongoing issues Carol thinks is hard to quantify is *guanxi*, knowing whether or not you have the best price of a particular resource (like energy) is always a lingering question. That is to say, even if Alice knows the boss of a coal mine, another competitor, Bob, may know his boss's boss which gives Bob even cheaper rates than what you thought you were receiving. Improving *guanxi* is a millennia old Herculean task.

Are there any other reasons for why China could be “exporting” coins in the near future? Rui Ma, an investor with 500 Startups in China explained at Coinsummit in July 2014, “I was under the impression that China had cheaper electricity but that’s not the case; it’s because of cheaper labour and real estate costs.”³³⁷

Other sources have confirmed that labor is still significantly cheaper such that at least half of all (50%) of ASICs are and will continue be made in China for the reason Ma suggested as well as because of cheaper real estate and not necessarily due to electricity prices (in some cases electricity is actually more expensive). At a closed door industry meeting in May 2014, fifty representatives from China’s key mining equipment manufacturers gathered.³³⁸ One estimate made was that the attendees accounted for 30% of the global Bitcoin hashrate and 100% of scrypt hashrate (scrypt is the proof-of-work function used in Litecoin and Dogecoin). Barring changes in the labor cost structure this trend is likely to hold in at least the short-run.

What is another incentive to set up a mining farm in China? In April 2014 a rail cargo line between Europe and China was “relaunched” the travel time of which is one month faster than traveling by sea. And it costs 20% the price of air cargo.

What is the motivation for restarting this potential time plus cost savings? According to *China Daily*:³³⁹

In a month, the export value of one consignment of electronic products might devalue by about two percent, about several tens of thousands of dollars.

This actually relates to Bitcoin mining as well. Again, most ASICs today have less than a 6 month profitably window before they need to be dumped or pointed to another profitable altcoin. The sooner you ship a batch, the quicker the receivers can recoup the costs. And in some cases, it is just more effective to install them in China to cut down on logistical downtime. Yet even with this time savings, the time sensitivity of new mining gear is high enough to warrant taking the plane which is what professionals do today.

Lastly, one area of opportunity is lending bitcoin through sites like Jua.com – but not to short bitcoin as other lending platforms are frequently used but to lend to miners instead (i.e., lending platforms like BTCJam are sometimes used by short sellers).

As a consequence, Shenzhen-based investors who were traditionally only working on the manufacturing side are also investing in mining operations too, with one recent investment of ¥350 million RMB (\$56 million) for a 15 petahash farm. For instance, as of this writing, the mining costs of a larger, professional operation is roughly 2,700 RMB (\$435) per bitcoin. Yet now it takes 3 months to profit whereas previously it was as little as one week. This could fluctuate too as up to several hundred more petahash are expected to end up on the market by the end of the year (up to 500 petahash globally), squeezing profit margins.

A bird's-eye view

In July I had an email exchange with Zennon Kapron, founder and managing director of Kapronasia, a Shanghai-based independent research consultancy focusing on the Asian financial services industry.³⁴⁰ He is also the author of the forthcoming book, *Chomping at the Bitcoin: The Past, Present and Future of Bitcoin in China*.³⁴¹ According to him:

Mining is and will continue to be relevant in the country. As hosting mining / pooling develops though, their business models could be at risk. If you could buy enough hash such that the output in BTC at least matches the input, it does open the door for evading China's capital controls. In other words, if you are a rich individual and have say 1 billion RMB that you want to get out of the country, you could, in theory, if there was enough capacity, use that to money to buy hosted hashing and then take the return as BTC, which you could then shuttle out of the country. Although, similar to actually using the exchanges, this would be more expensive than using some of the more established grey-market methods to move money out (cost ~0.5%), it does open a loophole that the government may not be happy about. The chance for masses of Chinese consumers to lose their money through a speculative investment however is unlikely, so that worry

likely wouldn't be there.

For perspective, there are common ways to use UnionPay, art auctions and pawn shops in Macau to avoid capital controls, bitcoin could be used but probably is not frequently at this time.³⁴²

Continuing he explains that:

Commerce was never a factor in China. There were a few bitcoin mining equipment shops on Taobao as well as some non-Taobao shops that accepted bitcoin, but acceptance was never high and most of those have either shutdown or no longer advertise their relationship with bitcoin.

The same social engineering risks exist in the Bitcoin sector that exist in many other sectors. At least once a week, I get a spam text that says something along the lines of: 'Dear, your mother is in the hospital. Please send 1000 RMB to this account: XXX'. To a certain extent the Chinese have seen just about every unsophisticated social engineering attempt possible, so they are very aware, yet Bitcoin is new, so there are new possibilities.

I don't believe that we will see any additional formal regulations come out of China on Bitcoin in 2014, but I believe we will see some informal movements. One element in particular: I don't think that the ATMs in China can survive, especially if the number in operation expands rapidly. I would believe that the government would shut these down.

At the July 2014 Coinsummit in London, the panelists covering China all thought that despite a variety of startups trying to expand its ecosystem (e.g., ATMs, exchanges, wallets), there are not many use-cases today beyond the speculative asset portion.³⁴³

As explained by Kapron above and confirmed at the panel, startups like *YesBTC* attempted to build a merchant processing platform, but they have pivoted to selling mining gear, and none of the large e-commerce platforms like those of Alibaba currently allow merchant integration with digital currencies.³⁴⁴ I discuss the viability of ATMs later in this chapter.

Utility or day trading

Just how many bitcoin holders – or 'players' (玩家) as they are referred to – are there in China? Between 50,000-100,000, however it is not growing due to restrictive policies discussed below.

A vocal minority of English-speaking Bitcoin adopters on reddit and Bitcoin Talk are, for lack of better terminology: proverbial bandwagon fans. In November, when Chinese consumers exploded onto the Bitcoin scene, many commentators cheered them on, welcoming them into the big leagues.

Ever since bitcoin prices peaked in early December (corresponding with the December 5th notice from the PBOC), many of these same users have collectively thrown all of China under the bus.³⁴⁵

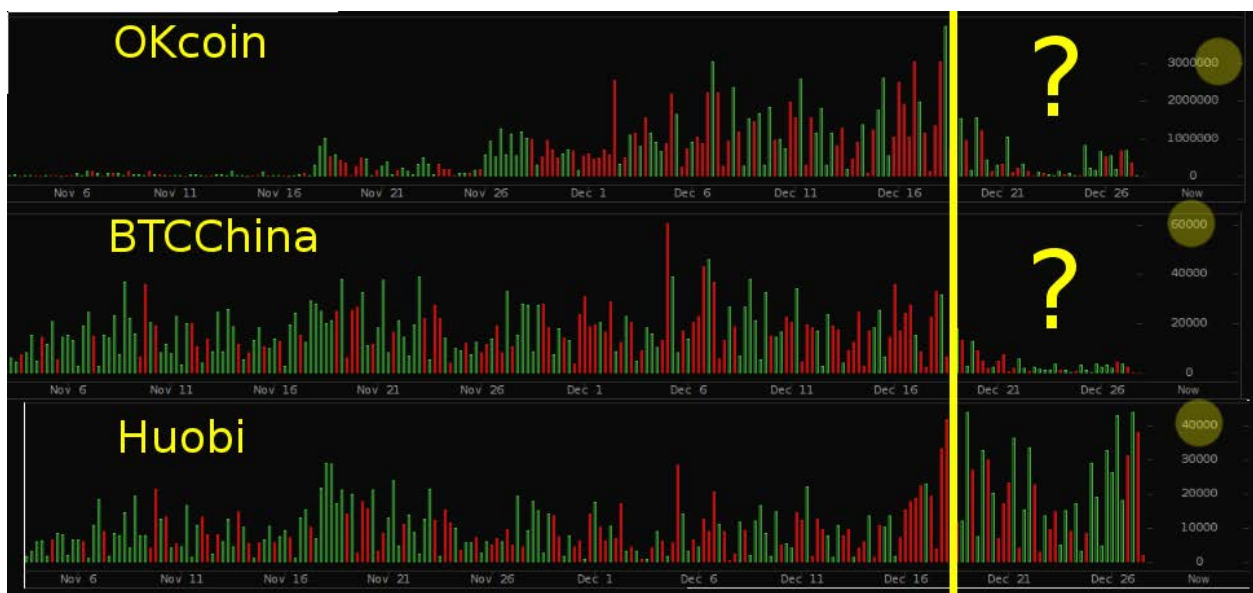
For instance, in early May *CoinDesk* published a story about FXTBTC (a Chinese bitcoin exchange) closing down. The very first comment was the following:³⁴⁶

The rest of the world would be better to ignore these PBOC reports. Bitcoin will go stronger once that happens.

Throughout each week similar such comments are posted on reddit and Bitcoin Talk.³⁴⁷ The truth is, Chinese consumers created enormous demand that drove up the prices in late November and early December. And the price has fallen measurably since the peak eight months ago, a peak which corresponded with the first “crack down” on December 5th, when the PBOC issued a notice to “protect the status of the renminbi as the statutory currency, prevent risks of money laundering, and protect financial stability.”³⁴⁸

What stability could they be referring to? All the ways to cheat and/or manipulate the stock market can be observed on bitcoin exchanges.³⁴⁹ While some claim that Chinese exchanges were fudging their volume and liquidity, extraordinary claims require extraordinary evidence.

The charts below, which were circulated in social media, illustrate the impact one specific date had on the domestic market: December 16, 2014, when the PBOC ordered 3rd party payment processing companies, such as AliPay and TenPay, to halt transactions in digital currency by January 31, 2014.





There are several ways to purportedly fake the volume:

- Because of a lack of overall transparency, exchanges self-report whatever they want to, although this kind of fakery is easy to spot if an exchange publicly exposes their market depth.
- Exchange operators can run their own bots which arbitrage (and front run) to make extra profit yet their bots do not pay any fees. Whether that is actually fake is arguable, however since the trades are actually conducted this kind of activity is typically not practiced in many “real” securities exchanges (e.g., akin to NASDAQ operating the exchange and yet maintaining an internal trading desk whereupon it does not have to pay fees).
- And another way is to simply mirror other exchanges and if an exchange is mirroring, you may be fudging the numbers to disguise it, or not. You might execute the mirrored trades or just have them for show.

How can exchanges ameliorate this loss of confidence going forward?

- Create an easy to read, publicly accessible series of charts on a permanent site such as <https://www.nyse.com/indices>
- Tell users whether or not there is any proprietary trading
- Add a real-time section about if bots are active, approximate amount of bots and how many customer bots are active each day; range if you cannot give exact numbers
- With volume numbers include:
 - daily active non-bot users
 - average trade per user
 - all unique trades
 - a running count of order depth

Yet before charging exchanges with conspiracy and shenanigans for this observable drop in volume, can there be other explanations? For instance, in mid-December both BTC China and OKCoin reinstated fees and according to this narrative, traders left to Huobi which has no trading fees.³⁵⁰ Unless these sites provide access to their databases, we may never know. But in all likelihood, correlation is causation: the PBOC is a force to be reckoned with, they enacted (caused) new regulations and guidance which scared both smart money and Chinese day traders away which correlates with the continual drop in prices.

Can large holders also move the market? One reviewer of this book noted that the relatively illiquidity of bitcoin prevents large scale exits for “whales” which could be resolved as more OTC providers merge liquidity pools:

This all requires the presumption of a highly developed exchange market that is highly liquid. That is definitely not the case. To give you a sense for it, the average daily turnover of Fx trading was in excess of \$2 trillion USD in 2006.³⁵¹

Similarly, Fx trades of \$20 million USD are routine. In Fx lingo, “Buy a dollar” means buying \$1MM USD worth. Not until the establishment of web-accessible systems was it reasonable for ordinary folks to get into Fx. Call up UBS and ask to buy \$10,000 and it wasn’t worth the time you wasted picking up the phone. Today it is possible through new e-exchange market makers.

A serious problem with bitcoin exchange is that like gold or platinum, since you can’t get interest on it because it isn’t really a currency, you can’t trade it in Fx markets. Or if you did, all forward contracts would, by necessity, be discounted by some basket of real currency interest rates. Bitcoin is 100% a “purchasing power parity” (PPP) quasi-currency. But most of Fx is driven by “interest rate parity” (CIP or UIP). PPP sort of drives long-term shifts in Fx. But there are fudge factors that keep them different ranging from culture and tariffs to wage and price controls.

To compound this issue are enthusiastic Bitcoin advocates in China, especially exchange and merchant developers who had their own public relation campaigns twist and tweak the situation, using tactics that in retrospect were wholly without merit. The fact of the matter is, there has been a cat and mouse game going on for months and while exchange operators have found temporary workarounds, for the time being, Bitcoin exchanges are *persona non grata* on the mainland.³⁵² There may be a few other loopholes and workarounds (which are quickly removed), but to believe otherwise is wishful thinking.³⁵³ No amount of marketing spins or gimmicks like ATMs will likely change that in the short-run.

ATMs

Though one should not count on Bitcoin ATMs as the saving grace in other locations either as Kapron mentioned above.

For instance, contrary to the headline that stated Bitcoin remittances were “4,000x cheaper than Western Union,” it is not, as transmission costs are trivial for money transfer operators (MTO).³⁵⁴ What does the breakdown of costs actually look like for a MTO? According to their 2012 paper, Cognizant found that:³⁵⁵

MTOs derive their revenues primarily through fees (70% to 75%), exchange rate arbitrage (20% to 25%) and other value-added services (0% to 5%). They have a high fixed cost (35% to 45%), which largely comprises expenses to cover salaries, rent,

compliance, IT and marketing. The variable cost (55% to 65%) is mostly attributable to agent commissions.

MTOs spend approximately 3% of their revenue on regulatory compliance. Market leader Western Union reportedly employs 600 full-time compliance staff and spends \$60 million annually to monitor its money transfer operations.

This issue was relayed to *CoinDesk* by Andrew Brown, head of compliance at cross-border payments specialist Earthport, stating that:³⁵⁶

“By the time all those obligations have been applied, I don’t think any apparent advantage [for bitcoin] will be left.”

While startups such as San Francisco-based ZipZap could squeeze the margins from incumbent MTO providers, Brown’s prediction also impacts other areas of the ecosystem.³⁵⁷ For instance, in addition to paying for compliance costs in the jurisdiction they operate in, Bitcoin ATM operators need to generate a profit to recoup their investment and compete against other ATMs nearby. Most, typically charge a 5% usage fee on top of the exchange spread.³⁵⁸ And eventually they too will need a permanent physical location staffed by agents. Again, transmitting is non-trivial for incumbent remittance firms nor are the funds stolen from the wire, instead, most of the fees involve operating a physical network of agents. In the long-run Bitcoin-based remittance and ATM operators will probably be unable to avoid such costs and fees.³⁵⁹

Edge use-cases

It is also important to distinguish what a blockchain can do in a developing country like China and what it probably will be used for as detailed above. For instance, in terms of property ownership — no one really owns property in China, only the state does.³⁶⁰ And the state sells parcels of land typically as 70 year leases. Yet because of how some Deng-era liberalizations took place, numerous leases (and subleases) may only be valid for another 40-50 years, and in many cases, if Bob does not have the right *guanxi* it may be invalidated altogether. This happens today with so-called “nail houses” (*dingzihu*) because there is no Lockean labor theory of property.³⁶¹

One might think that a blockchain, with its ability to manage and track deeds, titles and registries, would be the low-fruit to this quandary, especially in remote areas, but ultimately it is a political issue and decision. Even if all residents hashed or stamped their leases onto a blockchain, without enforcement or recognition from the court system, they will be unable to defend their ownership claims. This could change overtime and in cities like Shanghai, as there is a lot less ambiguity today than in other rural areas.

If the political apparatus in China does find a competitive use-case for blockchains, it is difficult to predict whether or not it would be used like the Great Firewall to protect its self-interests or allow it to percolate in some organic, decentralized manner.

Yet as seen in the previous chapters, a blockchain is not nearly as efficient or cost-effective as a centralized database in a data center tracking property titles. In most cities, there are departments that handle this. For instance, the Shanghai Real Estate Trading Center (Fangdi) is in charge of this matter.³⁶² Thus this niche may have few use-cases since most towns and villages — even remote ones in Xinjiang — will eventually be connected via a centralized solution.

In terms of the ramifications of what smart contracts and smart property could be used for in China (which is touched on in chapter 17 as well), it is important to distinguish between what smart property and smart contracts are.³⁶³ In short, a smart contract is computer code that self-enforces the terms of the contract. Smart property, in most examples are physical property, such as a house, car or boat, whose ownership can be controlled with a smart contract.

Currently, there are no known working examples of a physical asset (such as a car ignition system) whose ownership is remotely controlled by a smart contract residing on a cryptoledger. Again, for the most part the community is collectively playing catch-up with the West. For instance, there is no Perkins Coie of China yet, and very few of these companies even engage in legal counsel thus it is unlikely that these types of contracts or notary services will be developed for mainland users in the near-future.³⁶⁴

Perhaps this will change, and there may be an explosion of innovation in China, though at the moment virtually all of the activity involves day trading on exchanges. One notable exception is YBEX, which is a voting-based crowdfunding platform that accepts bitcoins (and ybexcoins) to fund certain projects.³⁶⁵ Lightspeed Ventures China, 500 Startups, Sequoia Capital China (ZhenFund) and IDG-ACCEL are active investment teams in China looking at entrepreneurs in this area.

Without the Middle Kingdom

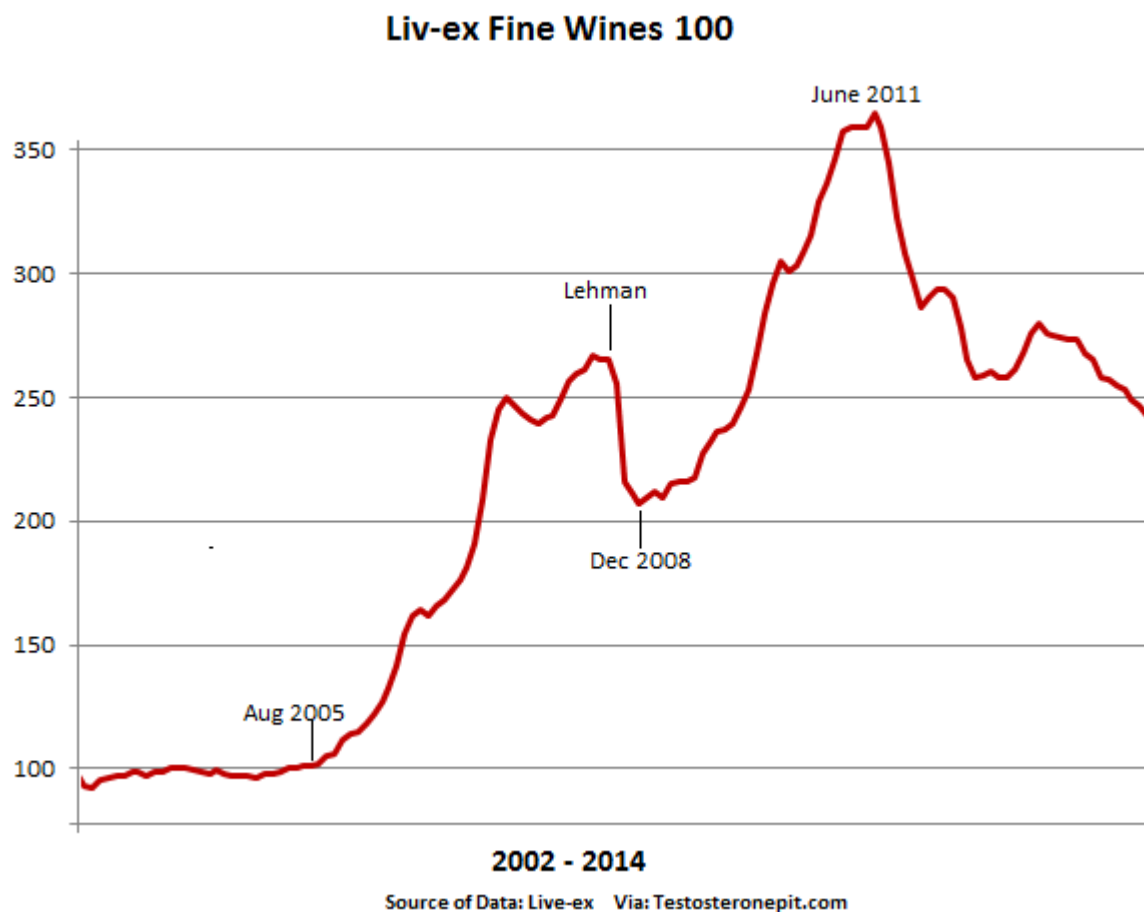
This was not the first fad in China to have attracted obsession and craving, as Weiwu Zhang recently explained about China's long history of enthusiasm for "scarce" goods, big and small:³⁶⁶

The crowd's mind changes, and the 'scarce resource' is often randomly chosen, too. A given resource is hoarded, and when a tipping point is reached, usually accomplished by a signal event, it suddenly becomes popular. Perhaps the most memorable example is the 2010 garlic bubble. It started as a small bubble, but when people realised that garlic was what everyone wanted to hoard, they hoarded it too. Reports have it that the price of garlic peaked at 30 times the pre-bubble price. This garlic is not a special onion, like

the precious tulip root that was mistaken as an onion and consumed for breakfast during the Dutch tulipomania. It is the most common daily food variety. The mung bean bubble is worth a mention too. These were both before Bitcoin.

The Chinese garlic boom was fed by claims that it would “help ward off the swine flu.”³⁶⁷ Similarly, as *Reuters* explained, “[m]ung beans got their start from Zhang Wuben, a self-proclaimed expert in Chinese medicine, who said that daily consumption of green bean juice and raw eggplant would stave off all kinds of diseases. The health ministry took the highly unusual step last week of denying that Zhang was an expert.”

Similar bubbles have occurred in a variety of areas, including most notably wine.



The chart above illustrates the boom in wine sales and how the post-Olympic boom from high net worth individuals from China contributed to its subsequent rise.^{368 369}

While some of the consumption is met by domestic supply, Australia vineyards are the second largest exporter to the mainland, France still dominates as the largest wine exporter to China, followed by Australia and is the 5th largest export market for US wineries (Hong Kong is 3rd).³⁷⁰

China is also the largest importer of cognac (by value) and is expected to surpass the US as the largest consumer of the brandy by 2020.³⁷¹

A large bulk of purchases were actually not for consumption purchases, as one analyst noted that:³⁷²

Investors should have been drinking their investments instead. But in China, that's exactly what they fear the most. Not only because it would destroy their investment, but also because that's when they'd find out that their cherished but plunging investment stored in their refrigerated vault might be counterfeit.

After a series of investigations, some of which are still ongoing – this bubble had been fed in part by fake wine:³⁷³

China's CTV has reported that 50 per cent of wine sold in China could be fake but many in the industry believe the true figure for high-profile brands - such as Bordeaux's Chateau Latour and Chateau Lafite, as well as premium Australian names such as Penfolds Grange - is as much as 90 per cent.

Perhaps Bitcoin will be different in the long-run, but in the short-run, speculation appears to have been the spirit and outlook for many purchasers. The topic of bubbles is further explored in chapter 13.

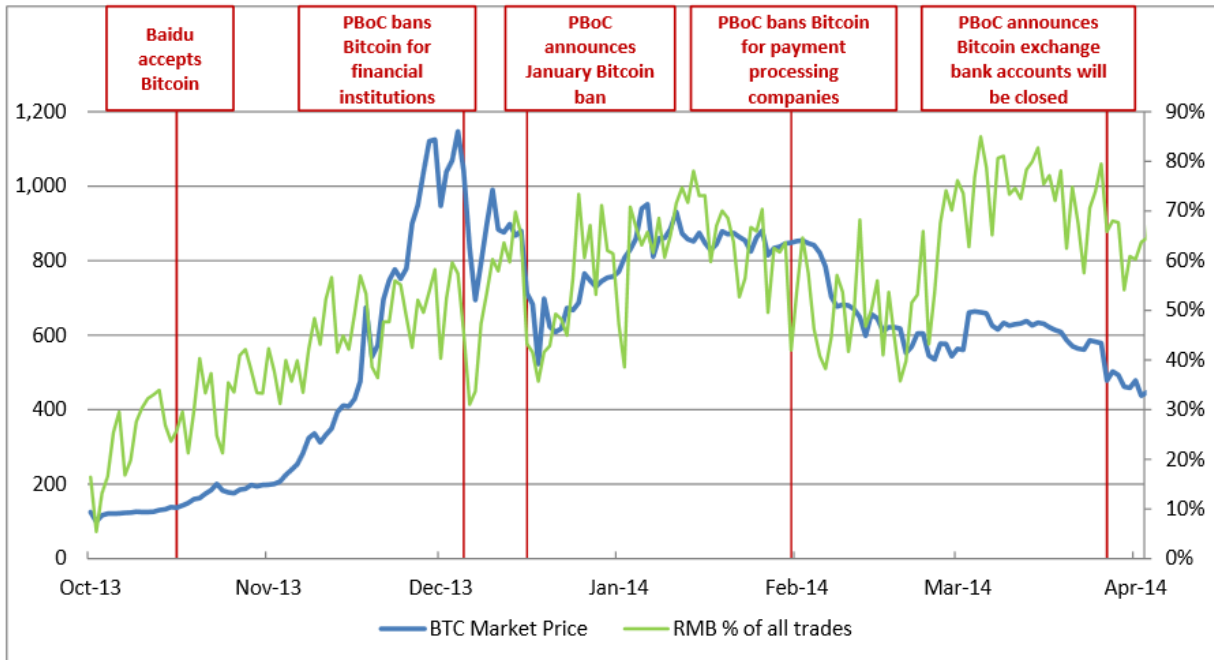
Perchance the types of inflammatory comments mentioned earlier targeted towards Chinese participants and the mainland marketplace only represents a vocal minority of users. But based on the fact that most popular news stories in Bitcoin-related media center around price levels, it may be the case that these social media denizens do not care about developing a trustless consensus mechanism to empower the underbanked in developing countries such as China.

Whatever the case may be, policy makers in China may appear opaque, but they could always block websites or arrest entrepreneurs although, as of this writing, they have not.

Consequently, most Chinese operations now have accounts in Hong Kong but they cannot operate as bitcoin businesses; the Hong Kong Monetary Authority (HKMA) has asked Hong Kong banks to report any account related to cryptocurrencies so most of the accounts are usually not open about the true nature of the operations. Some are still openly related to bitcoin but for mining investments (hardware purchases) or merchant investments and there is still pressure on those.

In her May 2014 report, Bitcoin's Uncertain Future in China, Lauren Gloudeman attempted to correlate the policy mandates in China with the local bitcoin prices as shown below in Figure 4:³⁷⁴

Figure 4: Effects of China's Bitcoin Policy on Price (USD)



Source: Bitcoinity.org, CoinDesk

One of the key points that she noted was that “[c]ontinued suppression of the Bitcoin market in China may severely impact global trading volumes, price levels, and perceived legitimacy.”

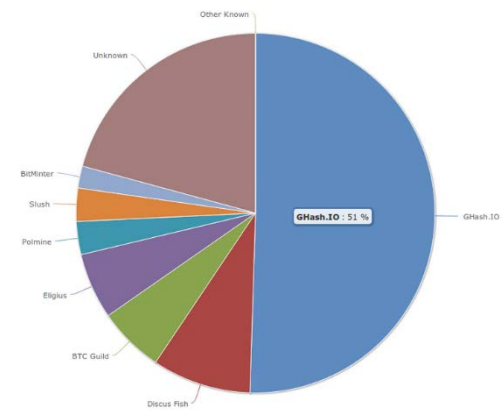
Thus despite claims to the contrary, Chinese demand, and its subsequent absence, did impact prices. Who will replace the Chinese whale? Perhaps in a bit of irony, funds from BitLicensed Wall Street could end up driving up the price once again, effectively bailing out some of the vocal bitcoin holders who are now underwater.

Chapter 6: Living in a trusted, post-51% world

This chapter explores the motivations for why mining centralization has occurred and why this trend will continue to remain so in the future.

While its hashrate has increased by many orders of magnitude, the Bitcoin network is qualitatively less secure today than it was two years ago. This is in large part due to the centralizing of the mining process within ASIC and ASIC farms (due to economies of scale).

For example, the most recent episode of the ongoing series of bad cop/good cop involving the largest pool, Ghash.io should put to rest the belief that only state actors can brute force the network.³⁷⁵ While some measurements differ, late on June 12, 2014, GHash.io reached approximately 51% for a multi-hour time span.³⁷⁶



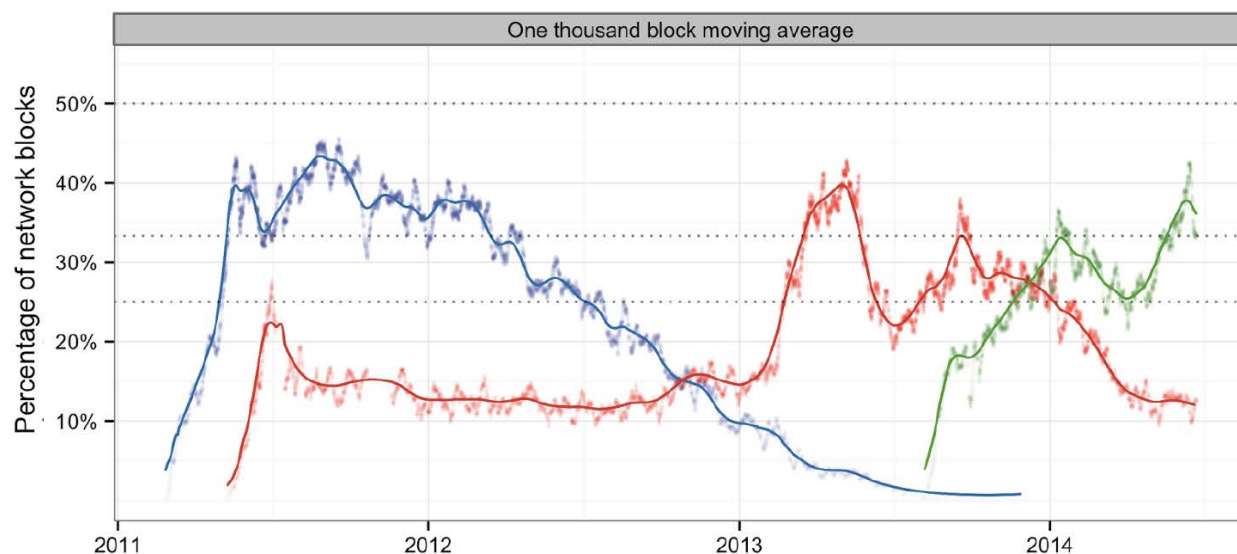
Data source: Blockchain.info

In July 2014 Coinometrics published an analysis of the blockchain based on three pools: DeepBit, BTCGuild and GHash.io. Each of these historically were the largest at one point. Yet despite their size, Coinometrics found that, “There has never been a pool or identifiable solo miner that has solved more than 50% of the network blocks for any week.”³⁷⁷

Does that mean Bitcoin is free and clear?

No, because “[a] miner with 48% can reverse 10 confirmations with an 85% success rate. Even at the chosen 40% self-imposed cap, the mining pool could overturn six confirmations with 50% probability.”

The chart below visualizes a one thousand block moving average which is roughly the amount of blocks mined in one week:



Source: *Coinometrics*

The blue line represents DeepBit, the red line represents BTC Guild and the green line represents GHash.io. According to Coinometrics:

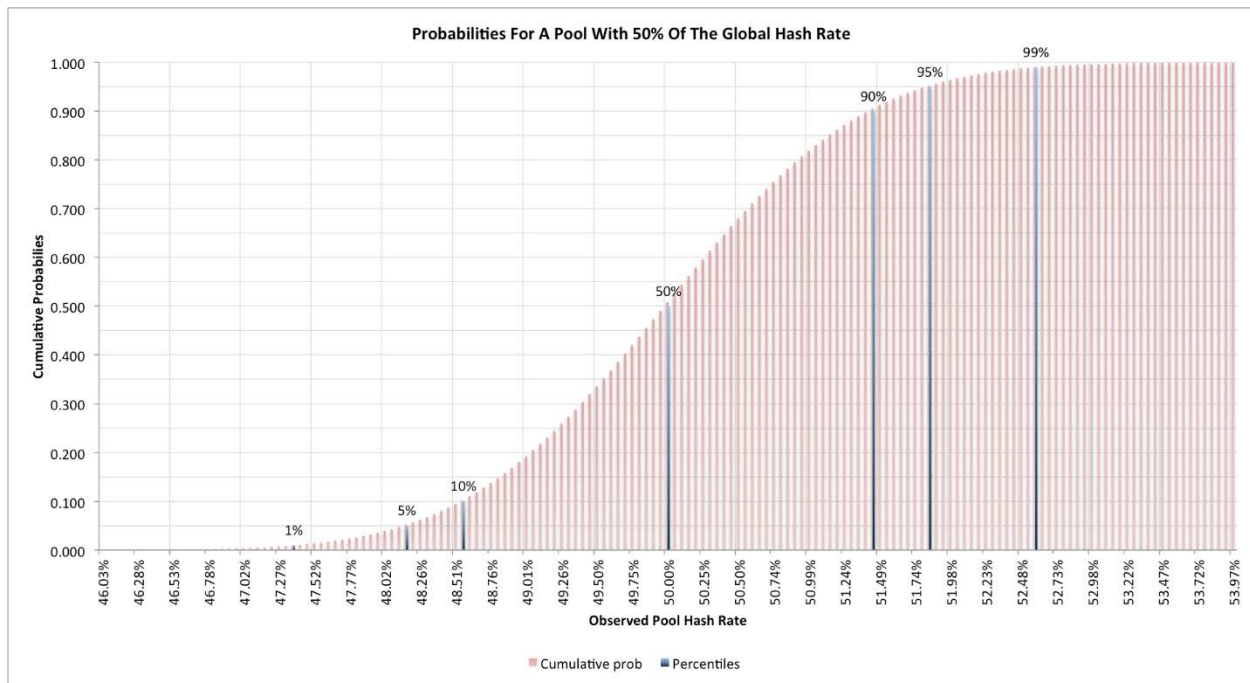
Even when the estimate of the intensity function (the smooth lines in Figure 2 [above]) is only approaching 45% of the network, the stochastic nature of the block solving process means that a block solver could easily have a hashrate above 50% for a short while. This needs to be considered when deciding the tolerance level of market concentration. The three members of the 50% club have in the past had a sufficient proportion of the network to successfully mine selfishly, or perform double spends with a good probability of success for significant periods of time. As more complex and valuable services are built on the blockchain calculating the risk of these events occurring is still in its infancy.

It is also worth noting that Coinotron, the largest Litecoin mining pool, held more than 50% for several days in May 2014, yet at this time no one has discovered any double-spending attacks by them.³⁷⁸

For perspective, I spoke with Dave Hudson. He ran a Monte Carlo simulation 10 million times to see what happens when a Bitcoin mining pool has 50% of the actual global hash rate and found that:³⁷⁹

As with many of the Bitcoin statistics we've seen, things are rarely as clear-cut as they first appear. We really need to see more than 55%, and probably close to 60%, of the hash rate being assigned to a pool within any 24 hour period before that alone is sufficient to say that the pool has achieved 50% of the network hash rate.

This is visualized in the chart below:



Source: Dave Hudson

Yet, in practice, because CAPEX still dominates OPEX, at roughly \$2 / gigahash it would cost roughly \$90 million in early June 2014 to obtain 51% of the network hashrate (not necessarily conduct an attack) – which is significantly lower than military budgets or other Hollywoodesque scenarios and conditions that some advocates claim such an event would require.

Peter Todd, another Bitcoin core developer, following the GHash.io incident, noted that:³⁸⁰

GHash.IO shows that the economic incentives behind Bitcoin are probably very flawed, it might take a disaster to get the consensus to fix it, and if that happens I want to make sure I can pay my rent and buy food while we're fixing it. I made a promise to myself a while back that I'd sell 50% of my bitcoins if a pool hit 50%, and it's happened. I've known for awhile now that the incentives Bitcoin is based on are flawed for many reasons and seeing a 50% pool even with only a few of those reasons mattering is worrying to say the least.

In his June 2014 interview with *IamSatoshi Networks*, Todd further explored the issue of block size increases.³⁸¹ As noted in chapter 2, in order to make the Bitcoin network more competitive as a payments and transportation network, there have been many proposals to increase the hard cap of 1 MB block sizes by several orders of magnitude. To date however, the average block size is around 350 KB, with an average of 0.7 transactions per second — thus the current need to increase it is low (primarily because few people actually use the chain for much activity such as commerce). If block sizes are increased using the existing method (and not using store-only unspent transaction outputs), without the use of something like tree chains, then centralization will occur because miners (and fully validating nodes) will need to pay for larger

bandwidth options or larger hard drives which squeezes out marginal players. This is a known issue and Todd highlights this as a hurdle for hashers wanting to move to another pool.

However there is a logistical problem with trying to move.

For instance, following a Bitcoin mining “summit” in July 2014, GHash.io announced that it would try to limit their share of the bitcoin share hashrate to 39.99%.³⁸² They would do this in part by publicly asking miners to point their hashing power to other pools. The problem is for the users without any of their own hardware, they are reliant on renting servers owned and controlled by CEX.io (the parent company of GHash.io); these users cannot move the mining equipment elsewhere so it is not fully clear how this jawboning will work.

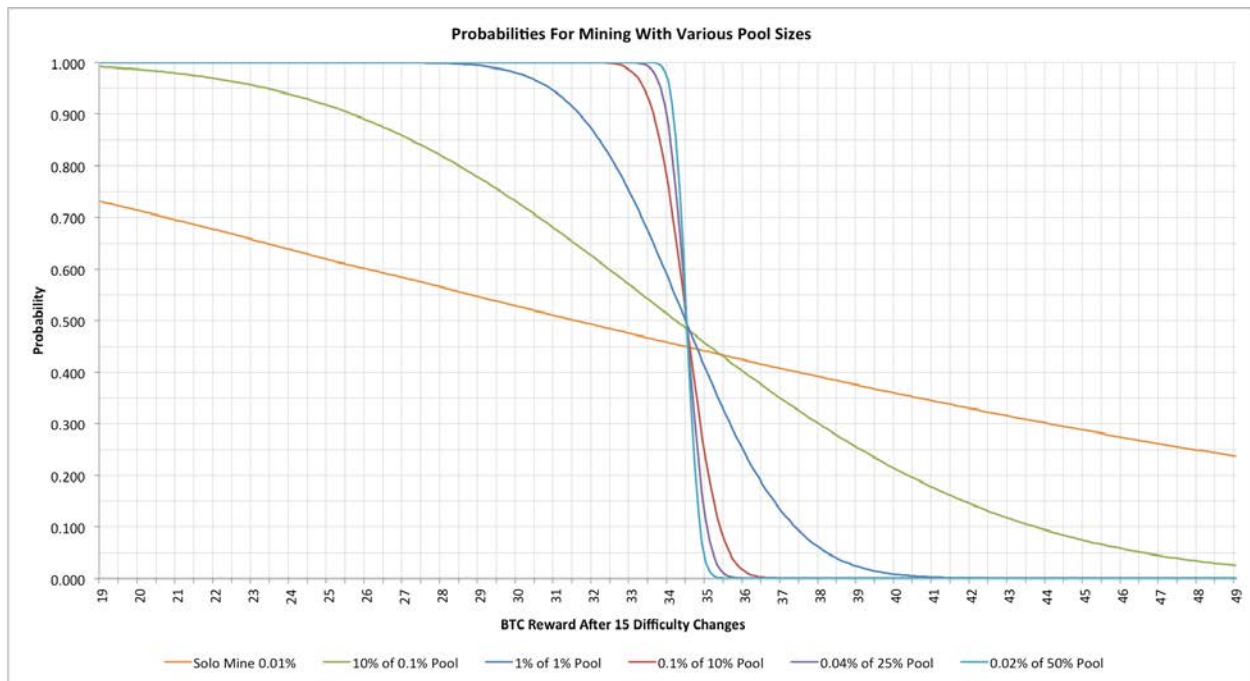
Because of its footprint, what this means is that the network moved from trustless, to trusted. The community has to trust (through vigilance) that pools like GHash.io will not double-spend, censor transactions or conduct a Finney attack (attacking a 0-confirmation spend).³⁸³ It is doubtful that GHash.io would do so, but it technically can.³⁸⁴ And even if GHash.io somehow broke apart, someone else will fill the void.³⁸⁵

This is because mining is essentially a statistical Poisson process (technically an inhomogeneous Poisson process), as the hashrate and hence difficulty is not constant over time. Thus there is too much variance to be left to small pools and therefore eventually someone else will eventually capitalize off the economies of scale.³⁸⁶

What does this mean specifically in terms of mining on Bitcoin? According to Dave Hudson:³⁸⁷

The first thing to look at is the way mining operates. The use of the SHA256 hash is intended to make it effectively impossible to predict what will or won't give a particular hash result without actually computing the hash and seeing if it solved a block. Essentially each minor change in the an attempt to solve a block gives a totally random effect, so trying one hash means that the next attempt is neither no more likely, or no less likely, to succeed! This highly random nature means that mining is a Poisson Process. As each attempt to solve a block is unpredictable then in theory everyone might mine all day and never solve a block. Similarly it's also possible that a single miner might find 6 blocks in a succession. Both outcomes are possible, but both are staggeringly unlikely!

So then, what does randomization in payouts lead to in terms of incentives and motivations? What is the incentive for pooling as seen with GHash.io?



Source: Dave Hudson

The chart above was published in June 2014 by Hudson.³⁸⁸ This chart shows the net results of running a different Monte Carlo simulation 10 million times. The key finding is that there is an incentive for miners to all use large pools to smooth out their variance or in Hudson's words, "The larger pools are definitely more attractive to anyone seeking predictable returns." Thus, investors with expected return on investments would rather be safe than sorry as anything less than a large pool is effectively gambling on lower probabilities. This is essentially the same thing as office pools or investment pools for state-run lotteries.³⁸⁹

In an exchange to clarify what this means, according to Hudson:³⁹⁰

There are a lot of incentives for centralized mining. One of my favourite stats at the moment is Bitcoin Stats Data Propagation.³⁹¹ It is taking > 3 seconds for a block to propagate to 50% of the network and > 10 seconds to hit 90%. That is a lot of time where miners are potentially working on the wrong problem! With better data I want to calculate those stats properly because this has a couple of effects:

- 1) Distant miners end up disadvantaged because they're essentially doing incrementally useless work for the first few seconds after a block is found.
- 2) Centralized pool schemes can disseminate blocks much faster - in fact they could prioritize disseminating new work over announcing the new block or have the systems in place to enable those blocks to be broadcast by dedicated systems that aren't involved in mining activities.

Concluding, Hudson notes the irony in which, “What's been somewhat amusing me all day is to see everyone arguing about GHash.IO not acting ethically within a system that is intrinsically designed with an assumption that no parties are trustworthy.” Consequently, readers may be interested in Jonathan Levin’s paper, *Creating a decentralised payment network: A study of Bitcoin*, which discusses this issue in more detail.³⁹²

Zero-sum mining

As noted in chapter 6, on the mining side, aside from chronic scammers, there are essentially only three consistently profitable entities:

- TSMC (Taiwan Semiconductor Manufacturing Company)
- Utility companies
- Large mining farms with access to the newest ASIC batches reducing overall operating costs relative to marginal players

Perversely, the roughly \$1 billion worth of capital spent on mining the past 12 months primarily went towards electrical companies and hardware manufacturers, not into the ecosystem itself. And because of these upfront costs, it is difficult to say what solutions will incentivize the re-on ramping of the mining process by more than a few circles of professionals including malware authors.

As Bitcoin core developers have pointed out on numerous occasions: the idea that miners and mining pools (the labor force) would abandon pools like GHash.io is continually disproven (and more than likely CEX.io, the parent company of GHash.io simply moves hashrate over to “unknown pools” until calm has been restored). Instead, miners understandably pay attention solely to the hashrate arms race. And their motivation to do so is prudent: they are economically rational actors (*homo economicus*) because the seigniorage subsidy accounts for (as of this writing) roughly 99.8% of the laborers income (seigniorage minus transaction fee).³⁹³

Thus, as Dave Hudson adroitly pointed out above, it is puzzling why the community would be vexed that a pool would want to provide services (low variance, merge mining, multi-language support, DDoS protection, contract trading, and *purportedly* even coin mixing) in the most efficient manner within a system where trust is taboo.³⁹⁴ Or as Jonathan Levin notes in his paper, “Mining pools offer a revenue smoothing service at a fee.” Why would rational participants with revenue expectations move away from certainty and gravitate towards uncertainty?

Again, only one miner can win, there is no silver place finish for second. Thus the more hashrate (lottery tickets) pool operators can get their labor force to throw towards obtaining the winning lottery number, the more revenue they can earn for their company whose physical capital stock is always depreciating. As a consequence, anything that is not working towards that end is marginalized. Hence, as noted in my previous article, most mining pools and farms

have not upgraded to the latest version of the Bitcoin core software because it offers no new useful features for most miners.

Taking a haircut and solutions

Consequently, because it costs real money and investors want to recoup their costs, mining will gravitate towards solutions that provide a reliable rate of return and this ultimately leads to industrial scale mining in centralized geographic regions.

Again what miners are faced with is the following: the more lottery tickets (or scratch-off puzzles) that they can obtain, the more chances at winning a block as miners are continuously incrementing the nonce in hopes to get the “lucky number.” In his new book, Nicolas Wenker, creatively describes this process as baseball swings: “In other words, mining occurs as miners in a pool leverage as much computer processing power as possible to take “swings” at the nonce as quickly as possible in a furious race to “strike gold” by being the first mining team to get their block’s nonce value below their block’s hash value.”³⁹⁵

What is this lucky number or value? Meni Rosenfeld described it thusly, “The miner plays with the nonce to get a block, up to a point. Since nonce is a 32-bit integer which only allows for 4B values, eventually it will need to ask the server (whether locally or on a pool) for a new merkle root to work on (where things like the extra nonce have been changed).”³⁹⁶

Thus as meticulously described in chapter 3, there is an incentive to throw as much hashrate as possible to obtain the block reward before your competition does the same because it is a winner-takes-all system. Below are several solutions:

- Peter Todd previously discussed this issue in a lengthy thread about “How a floating blocksize limit inevitably leads towards centralization.” His solution is “Tree Chains.”³⁹⁷
- Two Phase Proof of Work (2P-PoW) by Ittay Eyal and Emin Sirer³⁹⁸
- Proof of Activity: Extending Bitcoin’s Proof of Work via Proof of Stake by Charlie Lee, Alex Mizrahi, Meni Rosenfeld and Iddo Bentov³⁹⁹
- Andrew Miller is a graduate student at the University of Maryland has at least one quasi solution called Permacoin⁴⁰⁰
- Bitcoin Cooperative Proof-of-Stake by Stephen Reed⁴⁰¹
- Delegated Proof of Stake by Daniel Larimer⁴⁰²
- Blockpad: Improved Proof-of-work function with decentralization incentives by Sergio Lerner⁴⁰³
- Vitalik Buterin has some mining solutions related to Ethereum, but will likely not be implemented for Bitcoin⁴⁰⁴
- Greg Maxwell, a Bitcoin core developer ,has been discussing integrating a unique private key for each piece of hardware, soldered onto the physical hardware that is tamper resistant (not tamper proof) making it costly if destroyed. Bob could have all mining machines in one facility but according to this design, they machines could be viewed as potentially decentralized with this quasi-TPM (Trusted Platform Module) device.

- Andrew Poelstra (andytoshi), has a paper on ASICs and decentralization noting that once you hit the thermodynamic limit of chip fabrication, the technology becomes commoditized and proliferates, potentially leading to decentralization.⁴⁰⁵ However this actually leads to global energy arbitrage, where miners move to the location with the cheapest energy and reliable internet access.
- Perhaps the most novel approach is Proof-of-Idle by Tadge Dyrja⁴⁰⁶

However, irrespective of what solution is chosen it always boils down to this: what incentive do miners have to actually implement these? There is currently no incentive to implement new unprofitable code that removes the seigniorage subsidy because miners have sunk costs that have to be paid for. And there is no immediate incentive to upgrade to new software (one-third of all nodes are running 0.8.x code) so even if it was implemented in code, why upgrade when there is no financial benefit to do so? Similarly, even if proof-of-stake works (and thus far, all have led to centralization), there is no incentive for miners to use it (due to a lack of the subsidy) leading to a hard fork.⁴⁰⁷

Is a hard fork the end of the world? L.M. Goodman, in the Tezos position paper argues that it is not:

The argument that there can never be more than 21 million bitcoin because if a fork raised the cap, then it wouldn't be Bitcoin anymore" isn't very substantive, for Bitcoin is what the consensus says it is.

Thus while the prevailing “social contract” that most adopters agree to would dissolve, Bitcoin itself would technically survive. But this is a vulnerability: hard forks are an actual weakness as they rely on some centralization authority to arbitrarily decide the course of action; protocol forks act as a type of social attack on a protocol. This is a topic ripe for future research.

To compound this issue, there are vocal, influential members of the community effectively stonewalling efforts to discuss it – this includes those who are *not* involved in core development (the 10-15 guys consistently in #wizard IRC room), those whom have never mined before, and the largest segment: the ideological adopters who purge the community of skeptical discourse.

In fact, bringing up criticism or skeptical points of view are continually met with vocal threats of “public shaming” by ideological groups – which stymies a free flowing dialogue of ideas.

Again, it cost GHash.io roughly \$90 million in hardware to achieve that level in June 2014. A clever attacker would not need to brute force the ecosystem, but instead compromise network gear (with 0-day exploits), DDOS pools or as XKCD aptly illustrated: “use a wrench.”⁴⁰⁸

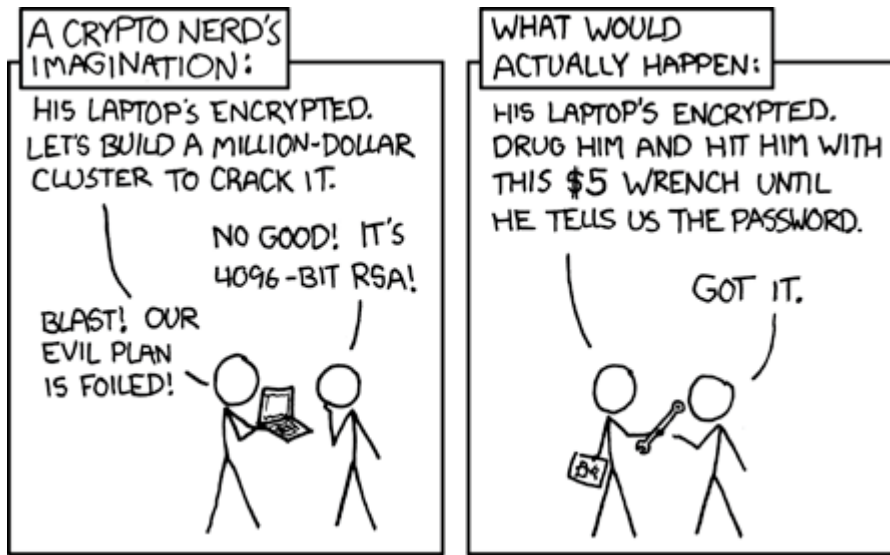


Image source: XKCD "Security"

Other solutions and hurdles

- Change the hashing algorithm from SHA256. However script (which is used in Litecoin and Dogecoin) is no longer a deterrent as shown with the large supply of script-based ASICs now available for commercial purchase. Other choices include: Script-N, Script Jane, Groestel (Grøestl), Keccak, Quark, X11, X13. It bears mentioning that X11 and X13 are a cauldron of hashing algorithms.
- Getblocktemplate BIP 23 from Luke-Jr (which Hearn discussed as well), however there is no straight forward incentive mechanism for mining pools to use this today because it actually increases the costs to mine.⁴⁰⁹
- Blacklisting, whitelisting and redlisting of pools that propagate certain blocks. This is a controversial issue that was debated back in April because of BitUndo (double spend as a service).⁴¹⁰
- P2Pool, however as Mike Hearn pointed out: it is difficult to install for most people, website difficult to find, feels "clunky" compared to centralized pools and has an increasingly high share difficulty.⁴¹¹ It also increases costs for miners.
- Change the inhomogeneous Poisson process in the code, but then it is no longer random, see Dave Hudson's article: "Hash Rate Headaches"⁴¹²
- Change the difficulty reset period to another arbitrary time (instead of every 2016 blocks). The automatically readjusting difficulty rating reinforces the zero-sum of hashing (e.g., exergy is consumed linearly, $MV=MC$) yet any other time period would likely lead to similar result, albeit protracted (or contracted).
- Lastly, who is going to pay for and test the code? This is a public goods problem. Jeremy Allaire CEO of Circle recently challenged the developers to "step up" and create a more inclusive process for development and simultaneously explains how investors (venture funding) will secure the network.⁴¹³ Yet investors understandably desire consistent reliable return-on-investment, this creates an

incentive to mine at the large pool – to cut down on variance and orphan rates. However this still does not answer the question: who will pay for all of the code?

Is centralization a real issue?

I spoke to several other experts and below are their insights on this matter.

Robert Sams, co-founder of Swiss Coin Group and Cryptonomics:

Choose-your-own-difficulty which goes something like this. A miner can choose what difficulty he mines at, and the reward is some non-linear function of difficulty chosen. This will allow people with inferior hardware to mine some coins, even though they'll be paying more in electricity for them than the market rate. I think people will do that, as virgin coins have anonymity value. This scheme would likely lead to $MC > MV$, which is good... mining will no longer be profitable (you can't "sell" virgin coins and retain their anonymity value).

To my knowledge, this approach hasn't been explored in detail by anyone (including myself). But I have a gut feeling that it's promising. The essence of the idea is that the coinbase is actually more valuable than coins with a history, but it's a value that isn't tradable. If you make it feasible for people to mine some coin in a reasonable period of time, people will even if the mining costs are greater than the market value of the coin. So if, for example, all the guys buying drugs and naughty stuff acquire their coin by mining under this scheme (feasible... your commodity hardware may get you .1 coin in a couple of weeks), you could have mining economics that make it unfeasible for anyone to mine on scale, anyone who has to sell coin to pay for electricity bills."

Jonathan Levin, co-founder of Coinometrics:

One really important point is to ensure that any new solution does not make things too botnet friendly.

Another simple thing about this is that it is unsurprising that the bitcoin network got into this mess as it is economically rational to join the biggest pool. Minimises variance and ceteris paribus reduce orphans increasing expected return per hash. The other point is that there is still hardware bottlenecks so designing the theoretically most robust system may fail due to market imperfections. Implicitly in many arguments I hear about mining people assume perfect competition. Do we need to remind people what are the necessary conditions for perfect competition? Perfect information, equal access to markets, zero transportation costs, many players this is clearly not going to be a perfectly competitive decentralised market but it certainly should not favour inherently the big players.

Dave Babbitt, a Predictive Analytics graduate student at Northwestern University:⁴¹⁴

Centralization wouldn't have been a surprise if the Bitcoin economy was simulated before it was launched. (As I keep on saying to myself while looking at the huge number of hours required to get it done.) Efforts to formally model the Bitcoin economy didn't start picking up steam until February of 2014. Yet certain equation-based models would've validly predicted the centralization problems we are having with Bitcoin. Even the cross-disciplinary field of Agent-Based Modeling (ABM) was mature enough in 2007 to do just that. The whole crypto-economy could have been simulated with readily-available software and clusters. Devs are using phrases like "you don't need to model the web to design TCP/IP" to justify not worrying about the economic aspects of their design. But just as Kleinrock, Baran, Davies, and Licklider modeled the packet net before Kahn and Cerf designed TCP/IP, so core developers should have simulated the currency and banking aspects of their design before they decided on the fundamentals.

Sergio Lerner, an independent security researcher at Certimix:⁴¹⁵

The only way to give a theoretical solution to the mining centralization problem is by forcing miners to use real identities, and people vote/trust on those. This is because with anonymous mining all miners could be controlled by a single party. Having real identities implies legal liabilities and users trust, which in turn implies centralization (institutions, pool, companies) to reduce personal risks and provide higher trust. So it's a paradox. Decentralization looks more like Ripple paradigm than Bitcoin paradigm.

Some argue proof-of-stake of hybrid system can have better decentralization incentives. All methods I've analyzed are inherently more complex and have many security problems than simple proof-of-work. So I expect decentralization comes on the form of a proof-of-work mining that practically (not theoretically) has deterrents against centralization; script with a high memory footprint does it. Also see my LIMIO protocol as an innovative way of decentralization in addition to the Blockpad proof-of-work already mentioned.⁴¹⁶

There will likely be dozens, perhaps hundreds of other proposals and experiments in the coming months and years, each with their own pros and cons. For instance, one potential issue highlighted by Sams' proposed approach is that the block reward is programmed to decrease and get smaller. Simultaneously it cannot be known as to whether or not that the dollar value of the reward is going to get larger (the two are not causally linked). If mining moves to individuals who do not mind mining at a loss in the quest for an anonymous, "virgin" coinbase that does not have a history, then perhaps this loss-bearing activity can continue for years.

Another potential issue could be botnets that Levin mentioned. In the beginning Satoshi Nakamoto assumed that botnets were actually a good thing because they might reduce spam oriented botnets – yet it is clear that they simply externalize the costs onto other parts of the economy and squeeze out marginal participants. In his words:⁴¹⁷

I didn't really make that statement as strong as I could have. The requirement is that the good guys collectively have more CPU power than any single attacker.

There would be many smaller zombie farms that are not big enough to overpower the network, and they could still make money by generating bitcoins. The smaller farms are then the "honest nodes". (I need a better term than "honest") The more smaller farms resort to generating bitcoins, the higher the bar gets to overpower the network, making larger farms also too small to overpower it so that they may as well generate bitcoins too. According to the "long tail" theory, the small, medium and merely large farms put together should add up to a lot more than the biggest zombie farm.

Even if a bad guy does overpower the network, it's not like he's instantly rich. All he can accomplish is to take back money he himself spent, like bouncing a check. To exploit it, he would have to buy something from a merchant, wait till it ships, then overpower the network and try to take his money back. I don't think he could make as much money trying to pull a carding scheme like that as he could by generating bitcoins. With a zombie farm that big, he could generate more bitcoins than everyone else combined.

The Bitcoin network might actually reduce spam by diverting zombie farms to generating bitcoins instead.

In the end, despite the multitude of avenues presented above, proof-of-work may simply not be a viable solution as a trustless means for arriving at a consensus in a distributed manner.

Chapter 7: Network effects

At the end of the book, I describe several next-generation platforms which are marketed as “2.0” systems. These were created for a variety of reasons including to side-step the technical and functional limitations of the current Bitcoin protocol. Yet before delving in those, even if the developers of these 2.0 protocols built the best, most 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.⁴¹⁸

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 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 new 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?).⁴¹⁹ 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. 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.

Protocols

Yet people confuse network effect with protocol. The protocol is what confers the monopoly the network effect does not. The reason there is no competing email is because eventually everyone agreed on a protocol. Online shopping is a network effect, but it is not a protocol effect, anyone can replicate it. Microsoft Windows is like a protocol, users are locked in. For any organization to have longevity, they need to create barriers to lock users in. These could be artificial (patents, legal compliance, taxi medallions) or some type of competitive advantage.

For instance, in the long-run asset-light companies such as Netflix will likely have trouble competing with Amazon Prime because up until recently with its Open Connect Appliances, Netflix did not really own all the servers they rely on to move the data. They are open to competitors who can use the same logistical and transportation network.⁴²⁰ On the other hand, Amazon has a monopoly they can leverage because they raised and built a competitive advantage through infrastructure (warehouses, algorithms, a supply chain, physical storage for customers). For anyone to replicate that it is much more difficult as they need increasingly larger amounts of capital. Similarly Uber could run into issues as they do not own a fleet and other competitors can provide a similar function, relying on arbitrage to stay ahead in marketshare. For instance, on July 13, 2014, Uber announced a \$1,000 bonus to “woo” Lyft drivers to switch and drive for Uber instead (Lyft is a large competitor to Uber).⁴²¹ In fact Uber loses money (5%) on every fare aside from surge pricing (it pays drivers more than customers pay).⁴²² Uber’s lack of fleet and physical capital is frequently highlighted as one of its core strengths. However, Uber would not have to woo anyone if they owned the fleet: asset-light also means expense and cash flow volatility.

In an open market, with none of these hurdles, first movers even with early adopters are not necessarily set for life. Diners Club, WebCrawler, Palm, Atari and Friendster are notable examples of this failure, in fact three out of five of these were later acquired by their own competition (Discover, AOL and HP respectively).

For example, Diners Club was founded in 1950 and was the first charge card company. It laid the foundation, both with spearheading acceptance and in dealing with legal challenges of this segment. However within a decade it faced competition from American Express and later Visa and MasterCard, all of whom had to recreate some forms of physical infrastructure. Yet despite this competition the charge card segment did not spiral into dereliction, but instead flourished.

In fact, nearly five decades after it was founded, Diners Club was acquired by one of its competitors, Discover. And despite technological similarities all of these competitors continued to grow and expand globally. Thus, in a competitive marketplace with no barriers to entry, it is unlikely that altcoins will either completely die or lead to failure of cryptocurrencies as an experiment in peer-to-peer payments. Similarly, TiVo commercialized the concept of a digital video recording (DVR) device and yet today it is merely one of many companies in the space it created.

And perhaps preeminent of all first-movers, despite inventing and patenting the internal combustion engine, Karl Benz and the modern automobile line that carries his marquis today, are just one of many competitors in the entire automobile industry. In fact, while the information on the site has been litigated via copyright (see *Craigslist v. 3Taps*), a site like Craigslist that has been seemingly dominant for years, likely generates most of its revenue from employment advertisements.⁴²³ If this is the case then LinkedIn and TaskRabbit are probably eroding its revenues (e.g., if revenue is flat, then it is being eroded). Dominance does not necessarily mean permanence and even the vaunted “network effects” that the US Postal Service had (through a monopoly on First Class mail) did not save it from increased obsolescence.

Prior to the enactment of several BitLicense requirements that create a barrier to entry for altcoins and altledgers, no one is locked into Bitcoin, its code is easily reproducible.⁴²⁴ Any number of large banks has a significantly larger customer base than Bitcoin. For example, Bank of America could fork the code, email all of its 50 million customers a Javascript widget (like BitMinter uses), tell them it makes “magic internet money” and immediately leap-frog the entire cryptocurrency user base with BOAcoin.⁴²⁵ This may be one of the reasons alternative value transfer systems such as Ripple or a few of the exotic altcoins will likely always exist in this ecosystem. In the long-run, technology oriented organizations have to have some capital requirements or specific trade secrets to survive, they cannot outsource everything as IBM has tried to do with diminishing success.

With Bitcoin, the security has been outsourced to a labor force comprised of non-proprietary equipment which allows any similarly-coded competition to catch up. On the other hand, firms like Ripple Labs (and its partners) essentially own the hardware. Some adopters may dislike this, but Bitcoin is not immune to the economic laws that govern adoption and incumbency.

As noted by David Evans, the miners in this system are providing a costly service to outside participants:⁴²⁶

The public ledger laborers, however, spend significant effort. They also incur significant costs in particular for computational resources. They are not contributing to a software project that will benefit themselves or their employers. Instead, they are providing a service services to individuals and businesses that are engaging in financial transactions.

This also is a unique set of conditions that may not work according to the plan proposed by many adopters. Evans continues:

The CNPE [constrained non-profit entity, Bitcoin] could not manage the public ledger platform efficiently under these constraints. It needs to manage a globally distributed workforce and the provision of resources to the platform. It also needs to decide on the optimal release of containers [blocks] into the system. But it has few tools for performing either of these tasks. This would therefore appear to be a rather rickety

structure for operating any sort of substantial remittance network or other financial services platform.

In fact, the approach towards managing the standard public ledger platform is so novel that we do not have any comparisons for assessing whether this approach could support an efficient or even viable platform in the long run. The public ledger platform model deviates significantly from open source models because the public ledger has to hire significant resources. Indeed, I do not know of any open source projects that manage markets that supply outputs and hire inputs in this manner. The public ledger platform also differs from proprietary models involving for-profit and not-for profit businesses because the platform protocol cedes almost all control over output and input prices to mechanistic rules that cannot adjust to market circumstances.

Containers are the semantic term for blocks. As noted in chapter 2, blocks are private goods provided by miners. Their size is limited and therefore capacity is scarce.

Forks

In a recent article on platform monopolies, Fred Wilson, a venture capitalist and founder of Union Square Ventures, notes that Bitcoin has the same disruptive potential on par with Google and Amazon. Stating, “But maybe most importantly, we are investing in bitcoin and the blockchain, which is the foundation for truly distributed peer to peer marketplaces without the Internet middleman.”⁴²⁷

The problem however is that since it is open-source and easily forkable – and the overseeing entity, Bitcoin, does not actually own any hardware – in the long run it will be probably unable to have a defensible position as a platform monopoly. After all, irrespective of laws, it is hard to compete with MasterCard when they spent \$299 million in capital expenditures alone last year just as it would be hard to compete with incumbent semiconductor firms such as Intel or TSMC when the cost of building a new fab plant is \$3-\$5 billion.⁴²⁸

Monopolies however do not last even with high capital expenditures. For example when vacuum tubes went out of favor, all the capex in plant property and equipment could not save those fully invested from emerging semiconductor fabs.⁴²⁹ So something has to change. Only if there is better way to transact outside of existing payment systems like MasterCard or AliPay will their existing network come under threat. The problem with Bitcoin is its entirely virtual; it owns no real estate on either machines or user end points that cannot be easily replaced. The proprietary nature of the protocol does not exclude formation of competing networks no more than Slackware Linux could not ultimately exclude other distributions on the server market (nor could Microsoft ultimately stymie Linux itself from the same thing).

During a fireside chat two years ago, Peter Thiel explained how differentiation and monopoly worked for PayPal (which he was a co-founder of):⁴³⁰

I think PayPal was successful as a business because it was dramatically better than the next best. It was better by a very big margin, had it only been better by a small margin it would not have been a great business. The payments, there was an enormous fraud problem, we figured out how to solve it, our competitors had no idea how to solve it. We figured, there were one or two other things like that that were very radically differentiated. If we had been no different from our competitors maybe it would have made sense for eBay to acquire us but would have been a really modest acquisition could bought any other number of companies that would have been just the same. Monopoly is always a loaded word. You want to do something that is unique, you do not want to do something that is just a commodity.

While the debate over how much better other competing altcoins and altprotocols actually are, Bitcoin at the time of this writing, may not be able to retain its market leading position without being able to create some kind of monopoly – some kind of barrier to entry or fundamental functional difference. It was first, yes; but unique, no.

Incidentally, with the New York Financial Services BitLicense requirements, startups will likely need to raise an increasing amount of capital to afford compliance costs.⁴³¹ As a consequence, this could act as an artificial barrier to entry that will probably help and protect incumbent wallets, exchanges and ATM providers from new competition.⁴³² Similarly, one section in the BitLicense (200.2n5) may make it cost prohibitive from starting or launching a new altcoin, metacoins or altledger, insulating Bitcoin itself from outside competition and creating for the moment, a type of monopoly.⁴³³

While the exact rules are still in public comment phase, if other countries adopt similar guidelines, in order to launch a new altcoin or altplatform developers may have to pay the legal costs for amenability there as well. Furthermore, since most venture funded digital currency businesses are being built around Bitcoin and a handful of other alt platforms, the legal costs of switching or supporting new alternatives could be cost prohibitive and non-trivial. The exception may be existing chartered financial institutions (as noted by Matt Levine in chapter 9) but this licensing process (a “taxi medallion” or “bit medallion”) may be the monopoly creating provision that allows Bitcoin to thrive despite its technical and economic limitations.

The following chapter will look at whether or not the TCP/IP protocol is an appropriate analogy to describe this system.

Chapter 8: TCIPcoin and User Adoption

One of the most common analogies used by adopters and investors in the digital currency space is that Bitcoin's evolutionary state is roughly equivalent to the internet in 1995. And continuing, that Bitcoin itself is a new type of protocol capable of transferring value like TCP/IP transferred data. This chapter explores this analogy and why it is incorrect.

Imagine an alternative history, a Mirror World, in which Robert Kahn and Vint Cerf created TCP/IP and only 21 million packets were allowed to exist. Under this paradigm users were expected to "mine" network packets. The amount of packets that could be mined on any given day were fixed and set on a static release schedule of 50 packets per every 10 minutes. Miners could then sell them to a demand side of the market. And because users could only use the internet if they had a packet, people (early adopters) might hoard packets with the hopes that they could resell them to others for increasingly higher prices. As a consequence, you might end up with the same kind of behavior we observe today with cryptocurrencies: of early adopters hoping for a world in which at some point these packets could be used to buy a yacht or island or both and therefore very little packet usage actually takes place on the network. An internet without any activity.

Similarly, what would happen if the fixed revenue an internet service provider (ISP) received spit in half every 4 years? In some ways, this could result in lower utility across the network. In our world, in order to be profitable the revenue generated from the internet traffic necessarily has to exceed the costs of running the equipment. Yet in the Mirror World, the cost of maintaining the equipment rises and falls in proportional to the value of the packets; and the amount of packets rewarded for maintaining the network decreases by 50% every four years eventually leading to an exodus of ISPs.

Eventually in this universe, someone, Alice, would see the futility in this, that this artificial supply constraint could be lifted by creating an unlimited amount of packets – packets which are created dynamically on demand, are no longer scarce and thus have little to no marginal value themselves yet collectively provide utility in the form of larger, bulkier forms of data that can be formed into images, videos, music, books and the web as we know it.

While this may not be the best example, as an infinite amount of credit could in some instances spurs deleterious inflation, but it shows that the TCP/IP analogy and specifically TCIPcoin is an inaccurate analogy. In fact, it is unknown what the "right" amount of bitcoins there should or should not be, yet on-going projects from Ferdinando Ametrano and Morini Massimo are attempting to devise one that may be. However, today, if these units were to actually be used as a medium of exchange, there may be a way to model how the supply could dynamically change to correspond with increased demand. Future ledger designers may be able to model these issues and incentives as described by Dave Babbitt in chapter 6.

Sluggish maturation

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

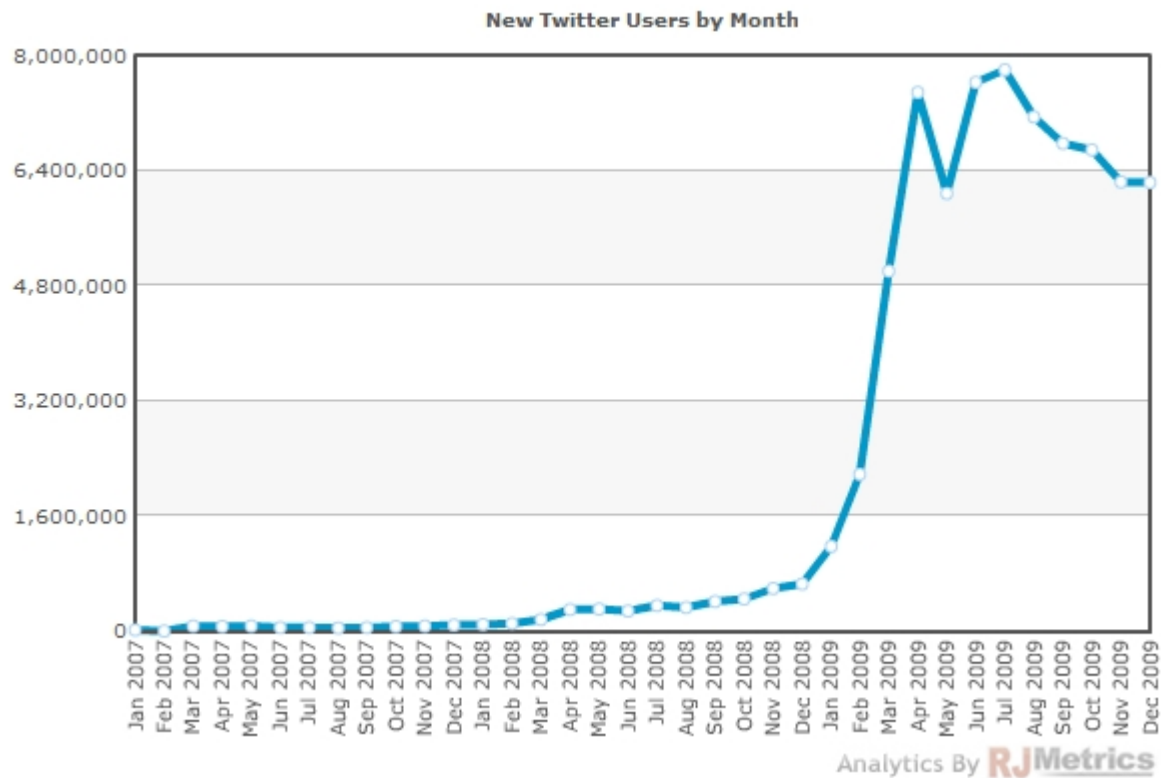
It could be the latter. That Bitcoin could be seen as a small developing economy that is capital-starved, has an underdeveloped industrial base and contains a glut of underemployed human residents.⁴³⁴ In short, it suffers from many of the same ailments of a poor, developing country. And over time, with investment, education and improvements in protocol (infrastructural) capabilities, the ecosystem may flourish.

If the purpose of Bitcoin is to create a trustless bilateral consensus mechanism to empower the underbanked and simultaneously provide incentives to bootstrap the economy throughout its germination stage, then at some point its users, entrepreneurs and ecosystem will necessarily need to create enterprises that provide real genuine economic engines of growth. Today however, this is not the case and may be one of the reasons for why there is no visible “Hockey Stick” growth curve that takes hold with many other viral applications. As illustrated below, despite the enormous amount of free publicity it has had, that other platforms like Square or Stripe would love to have, there is arguably no pain point that Bitcoin solves (yet) for the developed world.⁴³⁵

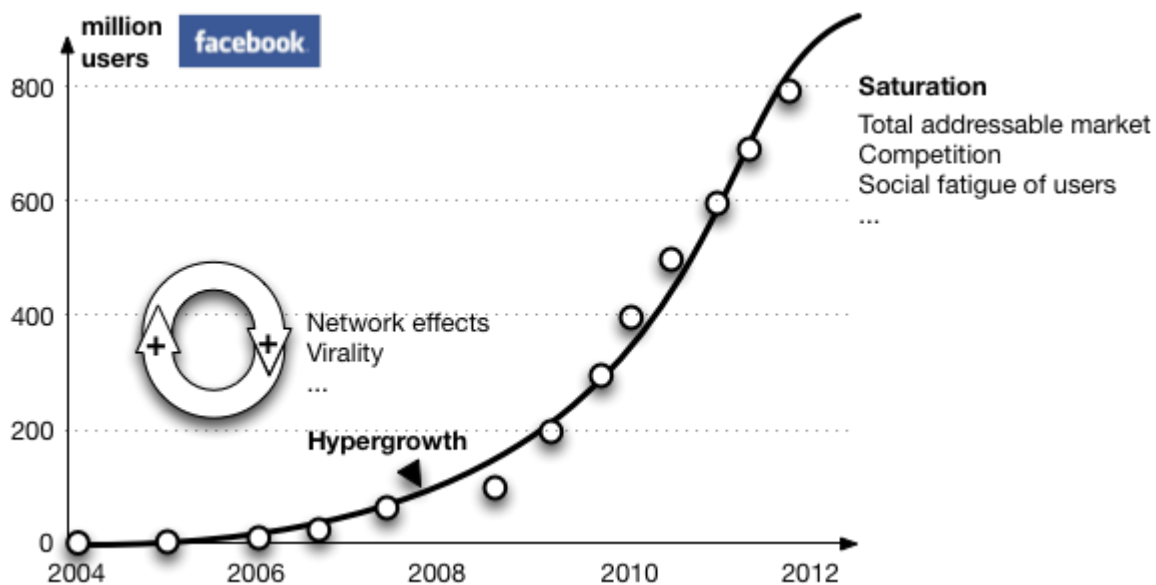
If the stated goal by adopters in the developed world is to supplant the financial functions of Wall Street (which likely will not happen) or compete with the payment rails of Visa (which will also likely not happen) then investors, developers and entrepreneurs need to build replacement businesses and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

What does a successful adoption rate curve look like?

For instance, this chart from RJMetrics illustrates the Hockey Stick of Twitter:⁴³⁶

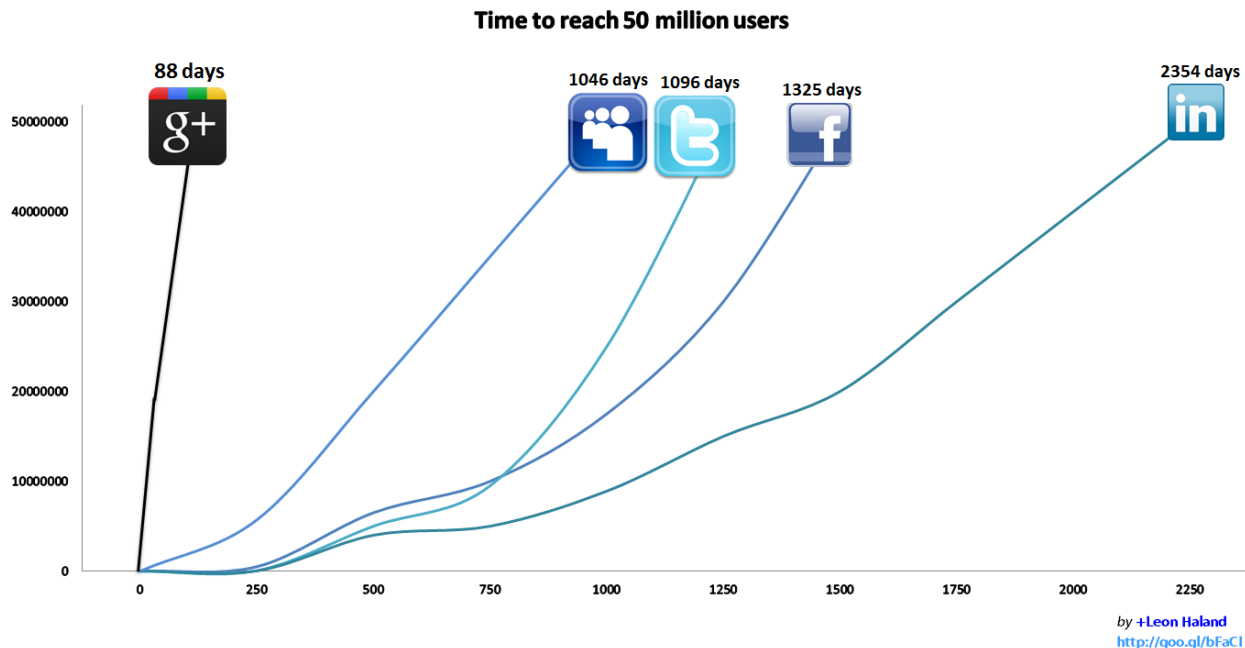


And this was what Facebook's S-curve looked like:⁴³⁷



Source: *Harvard Business Review*

What time frame did the large social media platforms reach 50 million users? Below is a chart illustrating this:⁴³⁸



I spoke with Mark DeWeaver, who is the author of one of the first books to chronicle China's post-1949 financial history and cofounder of the Quantriarian fund.⁴³⁹ According to him,

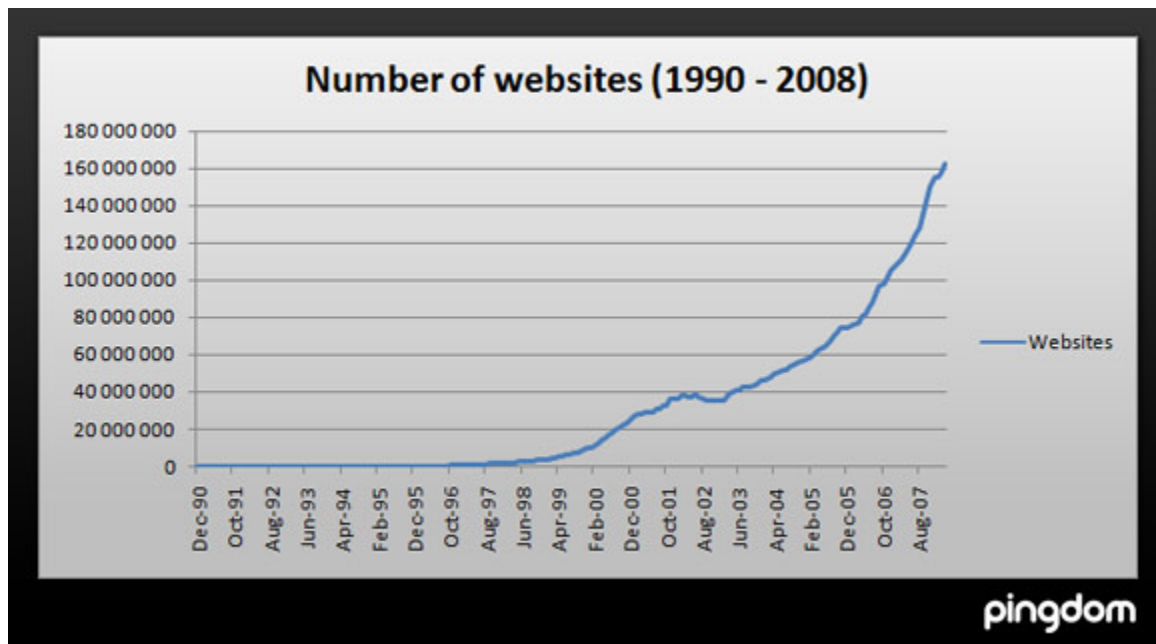
“The thing about developing economies is that they usually seem to be held hostage by special interest groups that insist that development must proceed along a path that doesn’t threaten their interests. So they tend to end up with what the political scientist Fred Riggs called “prismatic development”— a Potemkin version of the development seen in advanced countries. If it’s like a developing country, it could be stuck where it is now pretty much forever.”

While this issue will likely fill volumes in the coming years, as noted above, there are several special interest groups in the Bitcoin ecosystem, one of which exists as a form of *regulatory capture*: miners. Miners (transaction processors) are the sole labor force and will only hash and protect code that is profitable to them. The proof-of-work security mechanism at the heart of the protocol will likely never be switched to something less capital intensive like proof-of-stake or even tree chains.⁴⁴⁰ Thus, even though there have been several proposed improvements to the protocol to alleviate and mitigate some of the long-term technological and economic challenges (such as block reward halving), these might not be incorporated because the labor force could simply fork the code and carry on with the *status quo*.

However perhaps these are unfair comparisons. Bitcoin, the network, might not be a developing economy. The definition of a developing economy may apply to Bitcoin just as little as saying it is simply a currency. It could merely be a money-like informational commodity (or perhaps “factum” money as Vitalik Buterin and Max Kaye have proposed), which we still have to figure out how to use; like cavemen discovering fire and burning their fingers – we may be

currently in the burning fingers stage.⁴⁴¹⁴⁴² The charts above showed that Bitcoin does not follow the hockey stick curve compared to companies built on the internet.

However, if Bitcoin compares to the internet itself, as many proponents liken it, then future usage charts may end up comparing more with internet traffic from the late 1960s and early 1970s with Bitcoin “traffic” starting in 2009.



The chart above illustrates the number of websites from December 1990 to March 2008.⁴⁴³ Nevertheless, it is unknown at this time what the growth curve could look like in the future as consumer tastes may change.

Furthermore, let us assume that Bitcoin is a company and we compare it to Facebook. When Facebook was born, the legal environment it operated in was more or less well defined. This is not the case with Bitcoin as it faces many uncertainties in various jurisdictions which could be preventing wider adoption.⁴⁴⁴ Therefore a more fair comparison could be in the future, starting at the point when the regulatory framework of Bitcoin and other cryptoprotocols are less nebulous and more concrete by each member of the G-20 (or some other arbitrarily large percentage of the world economy).

Probability of adoption

What can the history of Facebook teach the Bitcoin community?

In his paper, *Achieving critical mass in social networks*, Chris Geddes explores what the tipping point for achieving critical mass is for social networking platforms such as Facebook.⁴⁴⁵

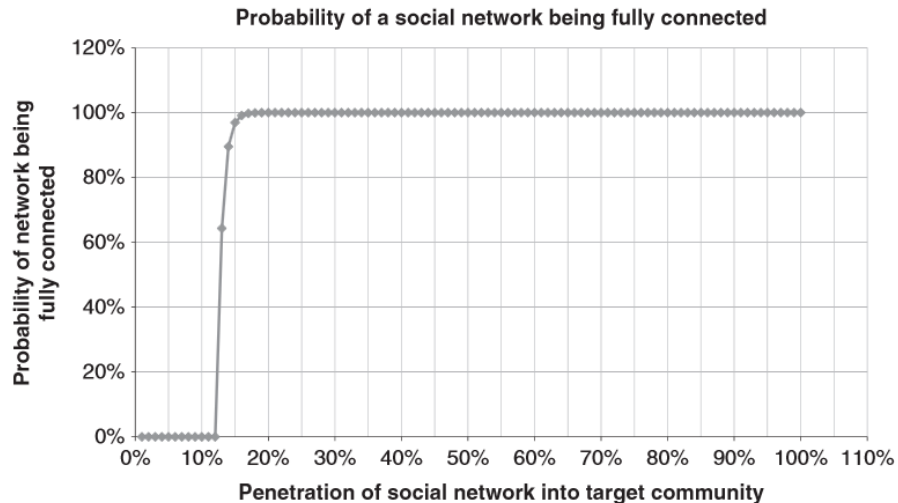


Figure 1: How community penetration determines interconnectedness of social networks.

Source: Chris Geddes

In his analysis there is a magic number to achieve critical mass, 15%, as visualized in Figure 1 (above). In his words:

Comparisons across network theory, graph theory and real-life examples of technology adoption show that after around 15 per cent of a community has been penetrated, the rate of acceleration of adoption dramatically increases until it plateaus at a saturation point.

Despite the tens of millions of people who have heard of and exposed to Bitcoin throughout the OECD, why has there not been a similar uptake and adoption for what is heralded and hyped as “the most important invention since the internet?”⁴⁴⁶

Again, it may not be a fair comparison, perhaps the adoption and usage rates for all new currencies or commodities or ledgers start out shallow, in small niches and that therefore the social media analogy is incorrect.

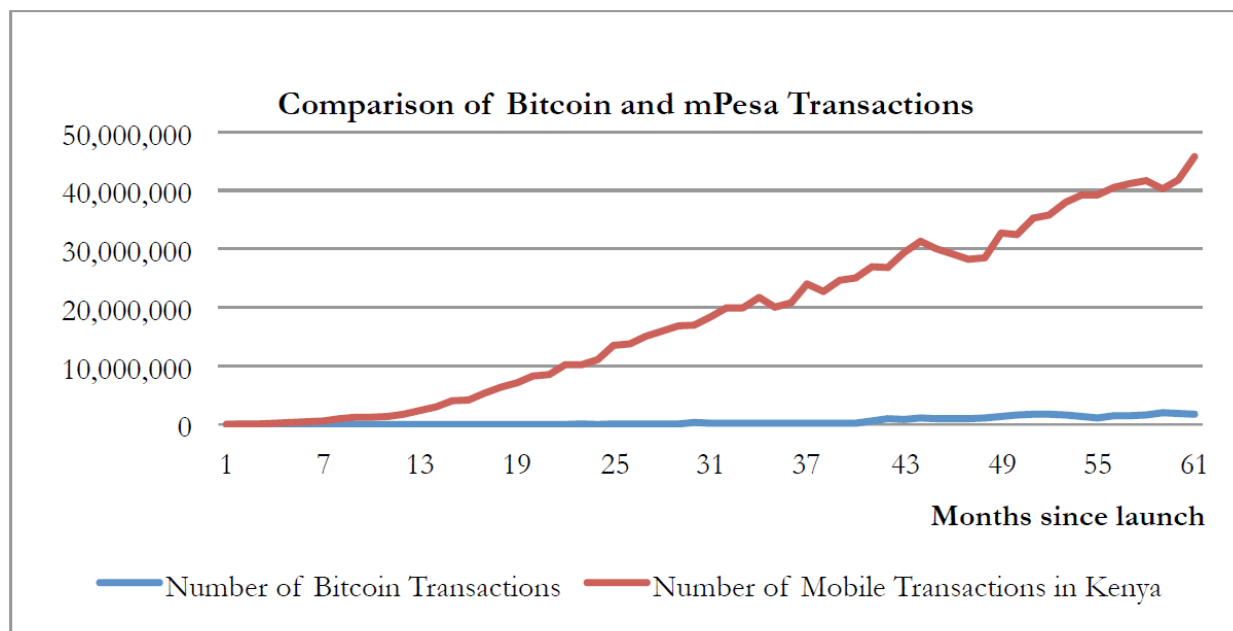
Yet there may be another reason and Geddes notes this in his conclusion:

Success is, however, absolutely reliant on getting it right first time. Users are fickle and are significantly less likely to log in a second time if, for whatever reason, their first time experience fails to meet their expectations.

Despite the hard work of improving user interfaces and moving the complexity to the background, perhaps many of these millions of people who have heard of Bitcoin, attempted to learn more about it and even use it. Perhaps in the process they found out it was too difficult or they were scammed and as a consequence, they are no longer interested in it as it failed to meet their expectations. Maybe mass awareness has taken place but the audience was

unconvinced of its purported merits. Perhaps this is another fulfilment of Amara's Law: overestimating the effect of a technology in the short run and underestimate the effect in the long run. Therefore the question for the community now is: how can passionate Bitcoin adopters inspire what is otherwise, to use sales parlance, a "dead lead?"⁴⁴⁷

One last comparison is with another payment platform which started at roughly the same time, below is Bitcoin (blue) versus M-PESA (red) from David Evans.⁴⁴⁸ M-PESA is a popular mobile payment system which launched in 2007 and is operated by Safaricom and Vodacom. It serves more than 30 million users in East Africa (Kenya and Tanzania), the Middle East and India. ⁴⁴⁹⁴⁵⁰ It is used by tens of millions (67%) of adult residents daily and 43% of Kenya's GDP flows through the M-PESA system.⁴⁵¹



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

As we can see, there is no real competition, though in fairness, this may not be apples to apples. Perhaps MPESA is a money substitute instead of the money-like informational commodity that bitcoin currently is.

Using similar data, Venmo, a payment application for smartphones that allows Bob, a user, to share and exchange payments with his friends and people in his social circle is also gaining traction faster than Bitcoin.⁴⁵² Similarly, while an imperfect facsimile, Square, CloudFlare, Stripe and MakerBot each were founded in 2009 or 2010 yet their uptake and adoption relative to the amount of direct media attention and ecosystem investment, is significantly higher than Bitcoin.⁴⁵³ Although the decentralized character of Bitcoin means that these corporate analogies are imperfect, there may be tangential explanations.

How many users?

The actual amount of bitcoin users is relatively difficult to accurately know (due to its pseudonymous nature) yet a rough estimate of 250,000 – 500,000 is probably a valid range. Despite the hype there are *not* millions of on-chain users (yet). For instance, as of block 310,000, according to the Bitcoin Distribution Chart approximately 321,680 addresses contain 99.1% of all bitcoins (UTXOs).⁴⁵⁴ While some individuals and companies control multiple addresses, this likely means that less than half a million people have funds on the Bitcoin network; a figure that Jonathan Levin of Coinometrics mentioned at CoinSummit in March 2014 as well.⁴⁵⁵

Some of these addresses are invariably controlled by firms like Circle and Coinbase (which create ease-of-use and utility for the network), however because they are off-chain this creates a trusted third party vulnerability negating the primary purpose of a blockchain. All in all, what this means is that there is likely an upper bound of no more than 10 million people who have ever handled a digital key controlling bitcoin, and the actual figure is likely significantly less. And despite the growth in hosted wallets, actual active bitcoin users – those who currently have more than 1 bitcoin and have sent a fraction of a bitcoin to another address in the past 6 months – may be as low as 500,000 individuals or less.⁴⁵⁶

For perspective, according to a January 2014 notice from Steve Englander, Head of G10 FX Strategy at Citibank:⁴⁵⁷

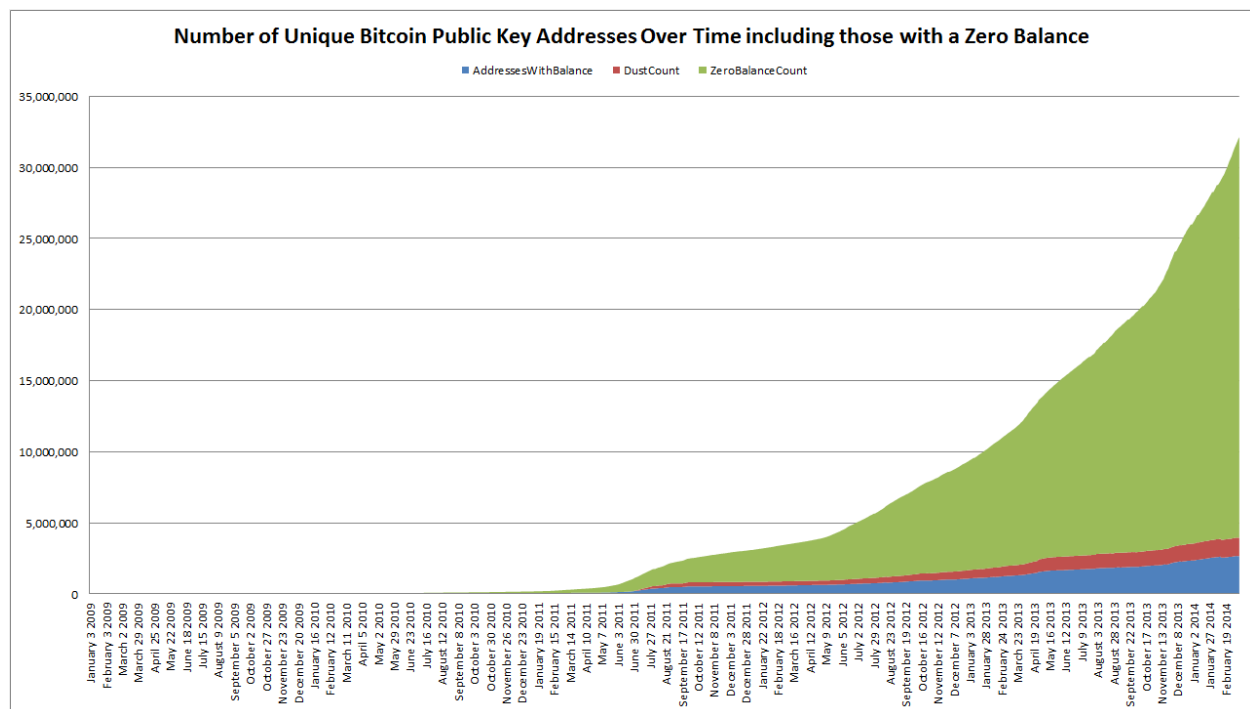
Best estimates are that there are about one million holders of Bitcoin; 47 individuals hold about 30 percent, another 900 hold a further 20 percent, the next 10,000 about 25% and another million about 20%, with 5% being lost. So 1/10th of one percent represent about half the holdings of Bitcoin and 1 percent close to 80 percent. The concentration of Litecoin ownership is similar.

Most of the big wallets have been in place from early on, so sitting back and watching your capital grow has been a very successful strategy. The distribution of Bitcoin holdings looks much like the distribution of wealth in North Korea and makes China's and even the US' wealth distribution look like that of a workers' paradise. There are estimates of a Gini coefficient of 0.88 for Bitcoin, but if anything the estimates are low if big holders own multiple wallets and the overall concentration of Bitcoin wealth is greater than in the sample used to estimate the coefficients. The most recent estimate of Gini coefficients of wealth concentration does not show any country above 0.85, but this sample did not include North Korea.

The Gini coefficient, named after Corrado Gini, is a statistical measure intended to represent the income distribution or income equality in a region or country. The coefficient varies between 0 and 1, with 0 representing complete equality and 1, the opposite. One estimate published in December 2013 was that roughly 1,000 addresses (or perhaps, individuals) owned half of all mined bitcoins; though it is unclear if those addresses are linked or controlled by

companies serving a multitude of other customers (such as Coinbase) or by a fund such as Pantera.⁴⁵⁸

Furthermore, comparisons with price level increases and address growth are not the same as user growth.



Source: John Ratcliff

This chart (above), compiled by John Ratcliff, shows the aggregate number of addresses ever used on the Bitcoin network between January 2009 through February 2014.⁴⁵⁹ Ratcliff is a principal engineer at NVIDIA who has a unique hobby, using 3D tools to visualize blockchain analytics. Over the past several months he has created visual aids for the community, in part to help visualize trends and even highlight uncertainty.

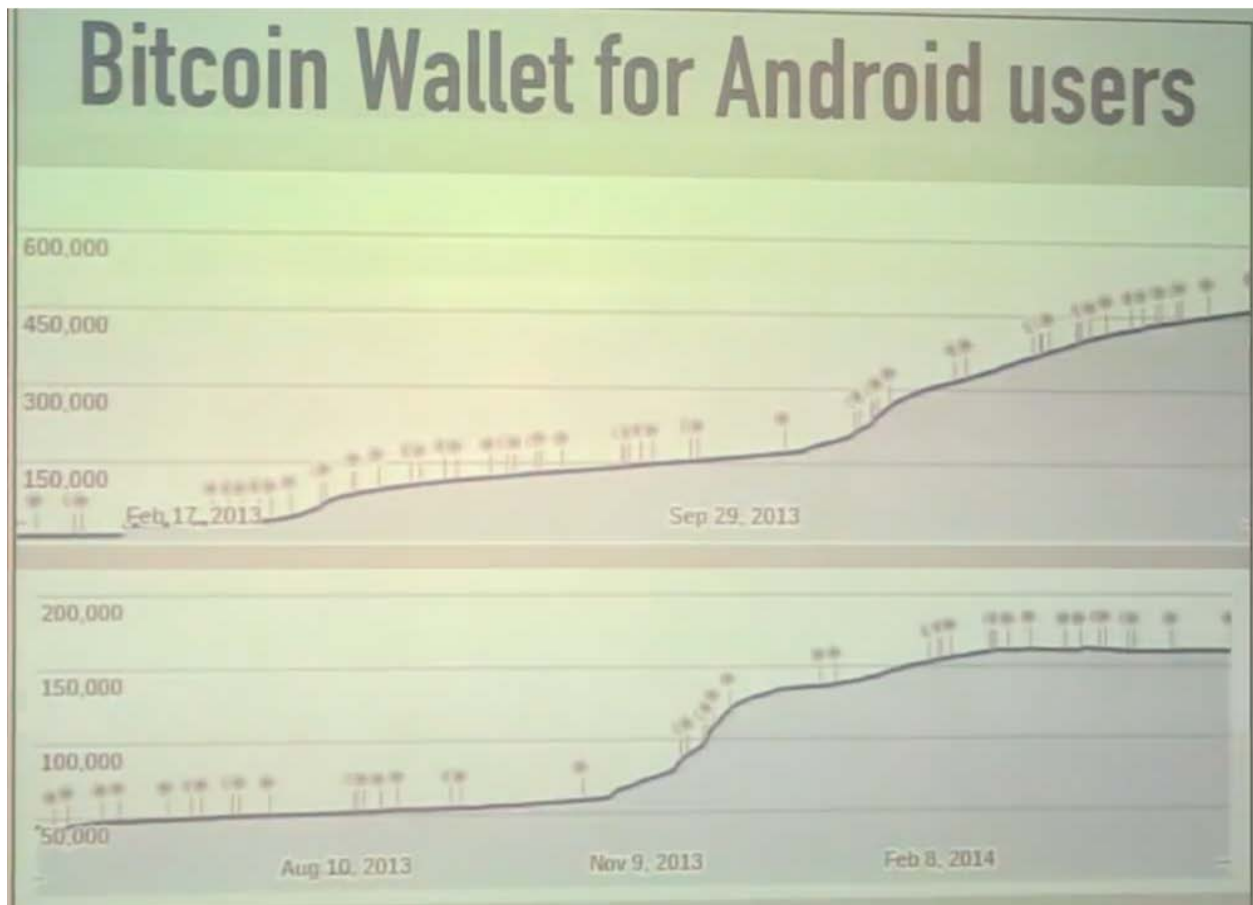
The blue line represents what are essentially spent addresses – addresses used as “intermediate steps” (i.e., using a new address per transaction, or to identify amounts received from particular payers). The red line illustrates addresses with bitcoins (UTXOs): that there are roughly only 2.5 million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

It should also be noted that addresses themselves do not “contain bitcoin,” they correspond to signing keys which can be used to redeem unspent transaction outputs (UTXOs). There is a conflated, semantic meaning used in non-technical publications yet from a technical

perspective, it is more accurate to use UTXO rather than addresses as “payment buckets,” since addresses are essentially just UTXO labels.⁴⁶⁰

Permanent beta mode

Many proponents claim that Bitcoin is still in beta mode, that it is too early for a real comparison because infrastructure is still being laid. This may be the case, perhaps the hockey stick will come later. Or maybe, as Mike Hearn (a Bitcoin core developer) hypothesized in May 2014, perhaps it will remain a niche (akin to desktop Linux).⁴⁶¹



Source: Mike Hearn and Andreas Schildbach

The top graph (from Hearn’s presentation) shows the total amount of Android Bitcoin wallet installations.⁴⁶² The bottom graph is the total active installations of Bitcoin wallets (first graph minus uninstalls).

According to Hearn, “At the end of February Bitcoin stops growing and I argue that this app is a very good proxy for Bitcoin usage overall because the top graph up here matches very well with Blockchain.info and other wallet providers that have been released. It correlates very well with other data that we have. The bottom graph what it shows is that at this point we are losing users as fast as we are adding them.”

I contacted Andreas Schildbach, the lead developer of the project in mid-July 2014 and he explained that while installations have risen and crossed the 500,000 mark, the active usage remains horizontal (with a recent uptick).⁴⁶³

Patterns or not

The following visual aid (below) shows corresponding interest over time: that Bitcoin usage and demand of bitcoins follows the media cycle (they reinforce one another as Mike Hearn mentioned above).

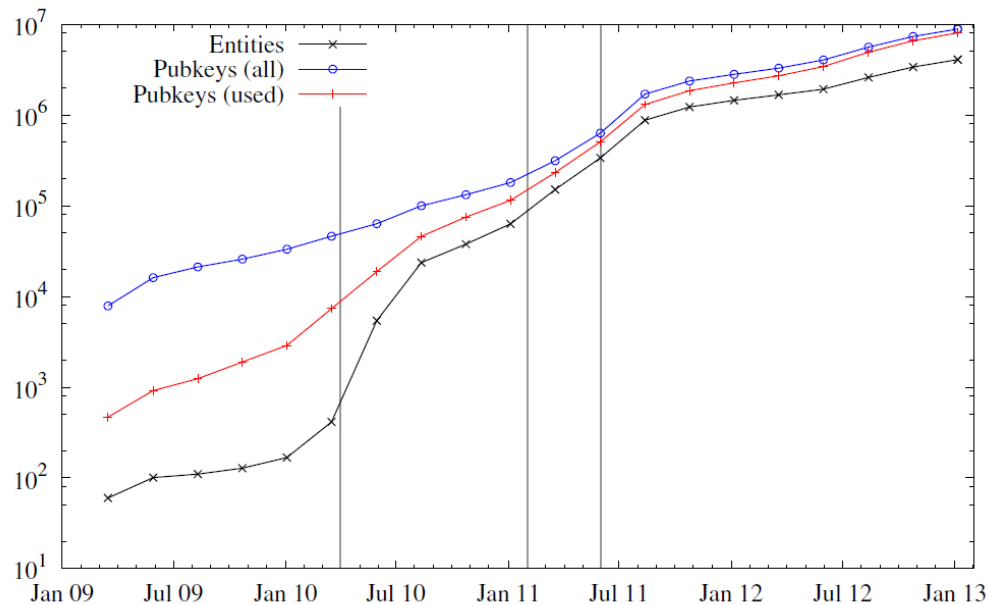
This chart compares Bitcoin, M-PESA and PayPal from January 2009 – July 2014 from Google Trends:⁴⁶⁴



As illustrated above, the interest over time for Bitcoin measured by search queries on Google looks nearly identical to the market price of bitcoin – the two likely reinforce one another during a boom which Hearn discussed in his presentation above.

Similarly, in May 2013 a team of researchers, Ober *et. al.*, exploring the structure and anonymity of the Bitcoin transaction graph published the following chart:⁴⁶⁵

Figure 1. Number of all public keys, used public keys and entities. The three vertical gray bars indicate three important events in the history of Bitcoin: start of public trading (leftmost), a post on Slashdot (middle) and an article on Gawker (rightmost).



Source: *Structure and Anonymity of the Bitcoin Transaction Graph*

In their words:

Figure 1 shows the number of public keys, used public keys, and entities over time. We can see a huge increase in the number of entities in April 2010. The reason for the increased interest in Bitcoin is most likely the fact that around this time (late April 2010) public trading of bitcoins began at an exchange rate of 0.003 USD per one bitcoin (in batches of 1000). More publications on Slashdot (for “reaching dollar parity”), Forbes and Gawker have created further interest in Bitcoin, which can be seen by a fast-increasing number of entities. After all, a hype was created and found its peak in June/July 2011, where the exchange rate reached about 30 USD. After the latter article, the exchange rate dropped below 2 USD. Despite this bubble, Bitcoin was still popular enough that a sustainable user base exists and still new users are recruited. The ratio of public keys (used or unused) to the number of entities seems to be stationary at a factor of about two, which means on average two public keys can be assigned to one entity solely based on the Bitcoin block chain.

While it is difficult to estimate or link “entities” to a single individual, company or organization, the researchers used a similar methodology as John Ratcliff independently did in his own approach cited in several chapters of this book.

In addition, the research team views this “entity” as an upper bound estimate for actual users, stating:

We first consider the number of public keys and try to estimate the number of active entities within the Bitcoin system. The number of all public keys (or addresses) is the number of public keys present in any transaction, whereas the notion of used public keys corresponds to those public keys that were used as input to any transaction at least once. Such used public keys belong to an actor who has control over these bitcoins. Therefore, we regard this as an economically active entity. Addresses used together as input for a single transaction belong to the same entity, because, in order to use an address as an input, one must be in possession of the corresponding private key for that address (this observation was already made by Reid and Harrigan). It is of course possible that some entity has never used two or more addresses together, but is still in possession of both private keys. In such a case both addresses would be perceived as belonging to two different entities by an adversary (and our experimental analysis) due to lack of data. Thus, the number of entities reported here serves as an upper bound.

While the pseudonymous nature of the blockchain makes it difficult to know exactly how many users there may be, the study above serves as a jump-off point for future researchers.

Alts and apophenia

How do the patterns Ober’s team saw correlate with the apophenia used by many Bitcoin adopters and altcoin creators on reddit and Twitter?

Currently it appears that Bitcoin has turned a segment of geeks into underwater day traders some of whom are suffering from a Type 1 error, the gambler's fallacy; believing that a certain outcome (i.e., a bull market) is necessarily “due” after a long streak of another outcome (i.e., a bear market). And who spend enormous amounts of time and energy creating sock puppets (fake accounts) to pump-and-dump get-rich-quick alts and bitcoin in an effort to compensate for their historically poor trading strategies.

And while most alts have a one-dimensional *modus operandi*, some alts provide an excellent method for experimenting with new features, new economic models and new ways of thinking that cannot be conducted with Bitcoin main due to the risk of disrupting several billion in assets.⁴⁶⁶

In January 2014, Steven Englander, Head of G10 FX Strategy at Citibank explored this financial incentive to make alts:⁴⁶⁷

Seignorage generates strong incentives for holders of the original Bitcoin to encourage its use, but it also generates incentives to create many alternative currencies, and mine them early and often. The hope is that one or several of these currencies will either a) take hold as a store of value or b) become so fashionable that the early miners can cash out. One element of the tulip bubble that is always ignored is that it was a boon to tulip

farmers in addition to speculators. Given how specialized mining has become, the seignorage gains to Bitcoin follow-ons will accrue heavily to a narrow swatch of tulip farmers technology mavenes who are in a position to mine each successive alternative currency while the going is good and cheap.

Another problem with apophenia relates to S-curves and adoption. S-curves are commonly used to illustrate the diffusion of innovations via adoption. Creating an S-curve using price levels is an incorrect way to measure adoption. Price levels of bitcoins are a function of supply and demand, which as noted throughout this study are largely a function of speculation and not economic demand of the token.

The type of volatility we see today is related to demand volatility, the changes in demand for bitcoin as an asset. Yet nothing has changed in the actual asset; a bitcoin (a UTXO) today is fundamentally no different than it was in late November 2013, yet its market price is 30% less. If the underlying conditions of an asset have not changed (such as the economic demand for it in commercial activity), yet the demand for it has sharply changes, this may be an indication of “animal spirits.”

For instance, in a November 2013 presentation, James D’Angelo, an educator, conflated price growth with user growth.⁴⁶⁸ Stating,

When people say that Bitcoin’s curve and growth is unnatural all they have to do is think about is bacteria, rats, Twitter, Google. And you start to see that sure, Bitcoin could die tomorrow. I don’t know what could kill it, but something could kill it. Some crazy stock manipulation or some government regulation. If you really understand how Bitcoin works it seems unlikely that it is going to be killed tomorrow by some simple thing. It is a network based thing, the more people use it the more value it has.

[...]

The world seems to be getting it, the numbers of people is going up every year. It’s got an exponential adoption curve. So just like rats on the island, just like Twitter, just like Google, just like Facebook, Bitcoin is doing that, it’s going up and down daily.

Actually, it does not. It is a *non sequitur* to suggest that 1,000% growth in market value of a token D’Angelo cites is the same as a user growth. In fact, there is a public data resource, the blockchain, that shows that there has not been a 1,000% growth in either users or in usage of bitcoins during these booms or busts. This could change in the future but it is not the case today or for his presentation last fall.

Niches

We cannot know for certain whether it will remain a niche *a priori*, this is an empirical matter. Instead we can only look back on what we have used it for, what needs it solves today – and for most people who have knowledge of a private key, they use it for speculation and hoarding.

One way to illustrate and view this phenomenon is through token movement on the blockchain which is described at length in chapter 8.

As explored later in chapter 12, while it is unknown what the exact motivation for these token holders are, it is clear that only a small fraction is liquid, most is illiquid. Perhaps these tokens were lost, stolen or seized. Maybe the users have psychologically moved beyond merely “saving” tokens to “hoarding” them.⁴⁶⁹ While this topic is explored more in the following chapters, “hoarding” does not grow economies either – only savings do because savings are lent out entrepreneurs who attempt to build and create utility. Hoarders may claim that they are providing some kind of reserve demand that creates price pressure thus incentivizing others to come into the market, yet again, this issue raises challenges that intersect with the Prisoner’s Dilemma (like someone has to eventually build the museums for hoarders relics) and is also discussed later.⁴⁷⁰

The next chapter will discuss the issues of volatility and deflation in more detail.

Chapter 9: Deflation in theory and practice

One of the core advantages over traditional paper money, so the story goes, is that bitcoins supply was fixed from day one, making it the perfect form of non-debaseable (sic) money. This chapter explores the problems of using an inelastic money supply to compete with elastic money supplies.

Teunis Brosens, an economist with ING, explained in a July 2014 video report that if they are accepted more widely, cryptocurrencies such as bitcoin could become a medium of exchange but that because the value of bitcoin was very volatile it would be problematic as a store of value or unit of account.⁴⁷¹ Stating:

Bitcoin's value increased tenfold in 2013 but it has also had several speculative crises in its short history. With real currencies, central banks dampen these fluctuations by regulating money supply and prices through interest rates. But it is an explicit goal of bitcoin and other cryptocurrencies to do away with central authorities. The supply of bitcoins increases at a predetermined rate by mining. But demand for bitcoin varies, so its price and the exchange rate with currencies, such as the dollar and the euro, fluctuate. These fluctuations could be bitcoin's undoing as they complicate its adoption as real money.

There is a way out: a bitcoin algorithm that smoothly matches money supply and demand. It is not impossible, but the inventors of that successful algorithm would make such a momentous step forward that they would surely qualify for the Nobel Prize in Economics.

To be fair, volatility is not the same as deflation. A currency can be volatile without being deflationary (notably such as the Korean Won, ₩, during 2008) and vice-versa. And a currency can be elastic without being volatile.

Yet what are the problems with deflation and inelasticity in Bitcoin?

Many Bitcoin adopters point to these two attributes as positive features. Yet as this chapter will show, they are bugs. For example, Dan Kervick explains why the latter is a drawback:⁴⁷²

Deflation might appear to be an attractive thing at first look. Wouldn't it be nice for our money to appreciate in value as the prices for goods and services continually fall? But economists associate deflation with two negative phenomena: First, if prices are falling then the incentive to hoard the currency increases, since anybody who possesses that currency is seeing its value increase each day. Thus, the currency itself becomes an appreciating investment vehicle for its owner, so long as it isn't spent. Hoarding by an individual agent is no big deal, but it is clearly bad news for the economy when hoarding is widespread, since if people stop buying things, then producers stop producing things

and stop paying workers to produce things. That's one reason why downturns are often associated with deflation, and growth is usually associated with modest inflation.

In its July 2014 report, Congressional Research Service came to similar conclusion:⁴⁷³

Because the supply is capped in the long run, widespread use of Bitcoin would mean that the demand for Bitcoin would likely outstrip supply, causing Bitcoin's price to steadily increase. The corollary of that increase is that the Bitcoin price of goods and services would steadily fall causing deflation. Faced with deflation, there is a strong incentive to hoard Bitcoins and not spend them, causing the current level of transactions to fall.

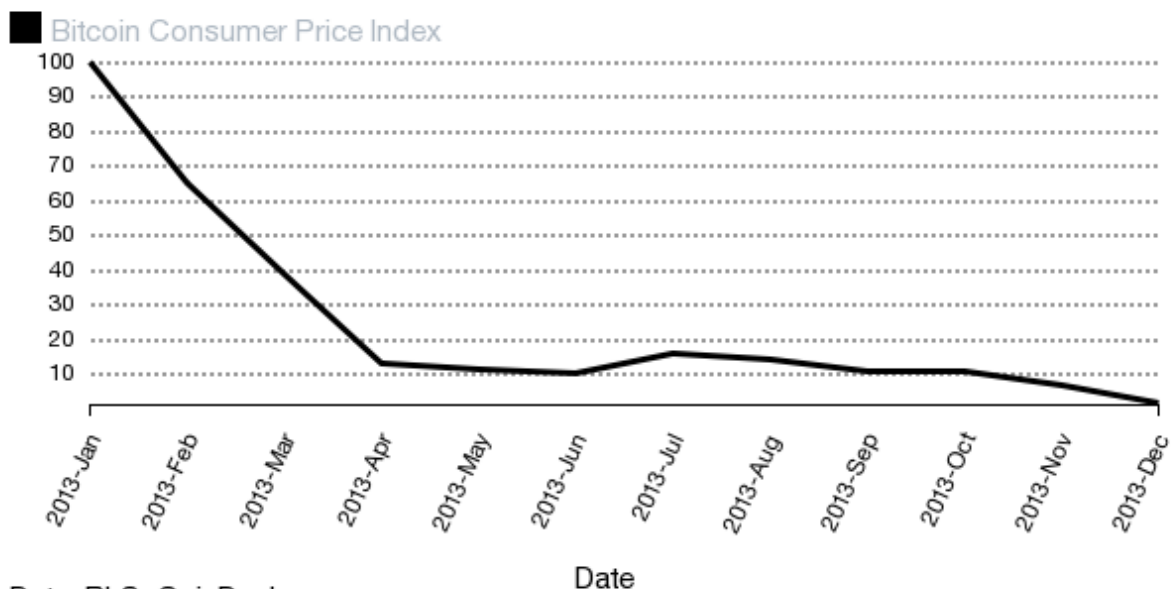
As has been established, Bitcoin (the network) is not a banking system because banking is a cornucopia of financial services including lending, payments processing, safe-keeping, notary, interest rate setting, underwriting debt and equity and an assortment of other services.⁴⁷⁴ Incidentally, one popular method for large holders of bitcoin to secure the bitcoins is to create a "paper wallet" and in turn store the piece of paper in a bank safe deposit box.

Customers depositing savings in a bank is semantically an investment, as those funds are then lent to others. In contrast, there is no mechanism within the Bitcoin network to provide such functionality, in essence these funds are inert.

What does this look like in practice?

Bitcoin Consumer Price Index

January 2013=100



The chart (above) was created by Peter Coy.⁴⁷⁵ He created a Bitcoin Consumer Price Index which is modeled on the US Bureau of Labor Statistics CPI. During the time span, January 2013 through early December 2013, the market price in US dollars of a bitcoin increased 64x. However prices measured in Bitcoin were down 98.5% during the same period. What does this mean? This is deflation, the mirror reflection illustrating the aforementioned volatility in purchasing power. As a consequence, when the price of Bitcoin goes up, why would Bob use his bitcoins to buy things when those bitcoins might double in value in a week, a day—or an hour?⁴⁷⁶

As Coy notes:

Two bad things happen in a deflation. First, people tend to postpone purchases as they wait for prices to get lower. That slows the economy to a crawl. Second, debts get more and more burdensome because they don't shrink the way everything else does. If you owed 1,000 Bitcoins before the deflation, you still owe 1,000 Bitcoins after it, only now your paycheck has shrunk by 98.5 percent. The only solution is to default. That's what happened on a massive scale in the Great Depression.

One frequently used argument against this line of reasoning regularly cited by some Bitcoin advocates is that technological improvements are deflationary. For instance, the nominal cost of an Apple II in 1977 was \$1298 and adjusted for inflation it would be \$5,095 today.⁴⁷⁷ And in the following 37 years not only has the nominal price dropped for contemporary systems but the technological performance as measured by hard drive, CPU, RAM and other attributes increased by many orders of magnitude. Yet people still buy them, why do they buy despite what seems to be “deflation” (e.g., a decline in prices)?

This misses two points. The first is, bitcoin (the token) is not a “technology,” the blockchain / protocol is. The second is that a product such as a laptop is not divisible into smaller units while simultaneously being able to still function as a laptop (e.g., Bob cannot cut up a laptop into 100 smaller units and expect it to work as a computational device). Or in short, laptops are not money. Bitcoins (the token), on the other hand, are divisible and consequently many of the adopters have attempted to shoe-horn it into a role of what effectively is (in the long-run) a deflationary currency.

Deflationary currencies historically absorb the purchasing power of the real economy and incentivize users not to actually spend them. They can – but not always do – make a potential store of value or unit of account but sometimes not an effective medium of exchange. Notable exceptions include the US dollar in the 1930's, the yen and, at times the yuan.⁴⁷⁸

What about the investing example mentioned by Coy?

In practice, an investment is not worth doing unless it generates a higher return than the risk free rate (the theoretical rate of return of an investment with no risk of financial loss).⁴⁷⁹

Every investment has a minimum acceptable rate of return (MARR) or “hurdle rate” which is the rate of return that it has to “jump over” to be alluring and viable to outside investors. For instance, if Bob can get 2% a year from a government bond then a minimum return on a competing investment has to be at least over 2% (and much higher), because Bob also needs to factor in the chance, the risk that the investment could stall or fail. In a deflationary environment such as Bitcoin, this is exacerbated by the fact that there is a disincentive to invest bitcoins in other asset classes.

Or more precisely, if a risk free interest rate did exist for Bitcoin, it would probably be either zero or negative. For instance, let us assume that Bitcoin appreciates at 20% a year. When Bitcoin is used to make an investment, this project would need to generate at least a 20% real return to merely break even with the alternative of just holding the currency. Nonetheless, we need to factor in the risk premium of this project so the MARR would be greater than 20%. This would mean that only the safest and most desirable projects would ever go forward, while the majority of projects would be discarded and consequently productive resources would lie idle. In essence, deflation would lead to non-allocation of capital that could otherwise have been efficient.

What this illustrates then is that bitcoins are not currently fulfilling the role of both a store of value and a medium of exchange. Again, this is a lengthy topic that is probably best discussed by Robert Sams “growthcoin” and Ferdinando Ametrano’s “stablecoin” publications which also describe how volatility is a factor; yet implementing either solution would likely fork the community, dividing them into one group who wants to spend coins and another who wants to hold.⁴⁸⁰

Does the deflation in bitcoin prices really delay purchases? Earlier this year Edward Hadas, the economic editor for *Reuters Breakingviews* made the comparison that it was noting that:⁴⁸¹

Deflation is an obvious issue. Price declines are inevitable when a finite supply of Bitcoin money, a feature of the software, meets an expanding supply of purchased goods and services. That would be uncomfortable. Consumers might delay purchases as they wait for prices to fall, workers might chafe at regular annual wage cuts, and creditors would be even worse off.

Hadas concluded that the situation Bitcoin as an economy faces is akin to the paradox of thrift, a downward spiral in economic activity (i.e., a depression).

Volatility

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

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

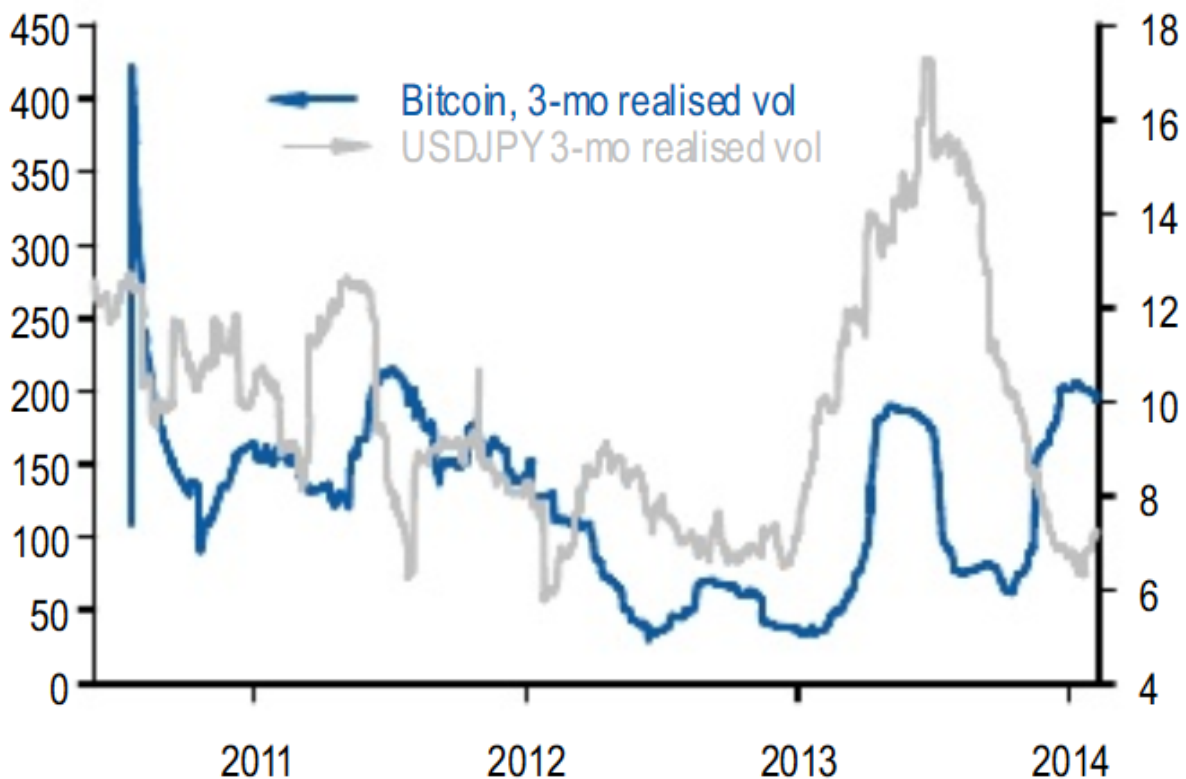
Source: Compilation with data from quandl.com, coinplorer.com, oanda.com

In practice, volatility is a poor property for a medium of exchange to have – bitcoin values were eighteen times (18x) more volatile than the euro in the first quarter of 2014 (see Table 1 from David Evans above).⁴⁸² Furthermore, it is the implication of wanting to hold cash for the transaction motive. In practice, people are risk adverse, and the existence of transactions costs mean more costly rebalancing of the medium of exchange that balance the more volatile the medium of exchange. Perhaps as some have suggested, when BitLicenses are issued later in 2014, new institutional participants will provide larger amounts of volume and liquidity, subduing some of the volatility.⁴⁸³

Or maybe not.

Chart 2: Bitcoin is over 20 times more volatile than USD/JPY

3-mo realised volatility; note difference in scales



Source: J.P. Morgan

The chart above comes from a February 2014 report by John Normand at Global FX Strategy with JP Morgan.⁴⁸⁴ As visualized over a four year period, bitcoins are 20 times more volatile than the dollar/yen trading pair.

Normand also notes that:

A virtual currency's transactional use will always be limited unless it performs the other two functions of money better than a fiat currency. As a unit of account and store of value, bitcoin also falls well short of fiat currencies given its extreme volatility. As highlighted earlier in chart 2, bitcoin's realised volatility has averaged 120% over the past three years, with a range of 50% to 400%. By comparison, typical G10 currency volatility is 8% with a range of 7% to 16% over the past three years. Typical emerging markets FX volatility is about 9% with a range of 7% to 20% over the past three years. Even during periods of extreme financial market stress such as the Asian Crisis of 1997/98 and the Argentine Default of 2002, currency volatility reached levels closer to 50% (Asia) or 120% (Argentina), and then only persisted for a few weeks.

True, these swings may represent simply normal volatility for a start-up currency just like the fluctuations of start-up companies' share prices during the 1990s. Even by dot-com standards, however, these moves are brutal. The Nasdaq only quintupled in value in three years (1997-2000), while bitcoin's price has risen 50-fold in the past year (charts 5 and 6). Such price fluctuations make it impossible to seriously consider bitcoin as a unit of account or store of value for an material amount of corporate or investor exposure.

Could this change with time and more liquidity? Perhaps, but maybe not.

There is also a chance that when BitLicenses are issued later this fall, it will likely bring new professional traders into this market, and traders are largely interested in volatility for arbitrage opportunities. Thus, the smoothing out volatility that some predict could happen might not; the phrase "be careful what you wish for" might be apt here. The armchair day traders on reddit could very well get cleaned out if and when real professionals with actual HFT experience come online. In addition, there is a very real incentive to also create artificial arbitrage opportunities such as a denial-of-service on exchanges or pools and impact the market just a little bit but this cannot be known *a priori* either.

Stalled and at a stand still

The discussion of inflation versus deflation with respect to Bitcoin has gone on since at least November 2008, with Ray Dillinger explaining to the same listserve Bitcoin was originally announced on that:⁴⁸⁵

I know the same (lack of intrinsic value) can be said of fiat currencies, but an artificial demand for fiat currencies is created by (among other things) taxation and legal-tender laws. Also, even a fiat currency can be an inflation hedge against another fiat currency's higher rate of inflation. But in the case of bitcoins the inflation rate of 35% is almost guaranteed by the technology, there are no supporting mechanisms for taxation, and no legal-tender laws. People will not hold assets in this highly-inflationary currency if they can help it.

One common refrain from some adopters is that even if the value fluctuates, bitcoin holders have to spend to buy food and satiate the lower tier of Maslow's hierarchy. This could be the case in a few instances (those who converted all their savings into bitcoins), but in practice most holders of bitcoin (or rather, most individuals with the knowledge of the private key) typically are diversified and live in a developed country and consequently have other means to purchase such necessities. So while it may be difficult to delay purchases indefinitely (no one besides Kevin Kelly regularly uses a 1980s Panasonic dial-pad), the economy as a whole is depressed because no activity is taking place (e.g., few spend, few lend).⁴⁸⁶ Why, as a lender would you lend if the price measured in bitcoin could decrease?⁴⁸⁷⁴⁸⁸

For instance, in the Coy example noted above, if Bob loaned a friend, Alice, 100 bitcoins on December 31, 2012, Alice might not have had the ability to pay it back a year later. She would, at the time, be taking out roughly \$1,350 (\$13.50 per bitcoin) but by the end of the year in December 2013 would owe 64 times that or roughly \$86,400. Faced with such decisions, few borrowers would bother taking out loans and most would simply default. In general, with deflation, the lender gets paid back an amount that is worth more than what he originally lent. However when deflation is as extreme as the example above, the default rate will be high.

Facing such a possibility as seen with bitcoin in 2013, few lenders might be interested in lending, but would rather just hold onto the asset and await for its appreciation; especially considering how the rest of the bitcoin ecosystem (e.g., credit ratings) is non-existent, which makes the risk of default higher than it otherwise would be.⁴⁸⁹ After all, what kind of business could Alice realistically create, get off the ground and produce a profitable return of 64x in one year?⁴⁹⁰

Or to use another example: Bob's barbeque business. The revenue of the business would be the same in real terms but the nominal amount of currency units from sales would go down due to deflation. What happens in this case is that if Bob had a debt that is pre-set in terms of nominal currency units, he ends up having an increasingly harder time to pay because he would have to deliver more real value with each succeeding payment. This is why deflation is bad for businesses. It makes their debt burden in real value higher and higher every year. If the currency is deflationary, theoretically the interest rates would be much lower, offsetting this cost. However, that is only if deflation levels are predictable and built into the interest cost – which according to Brian Hanley's analysis, is essentially impossible with Bitcoin since there's no central clearing house or method of coordination to provide Bob and market participant's inflation targets while adjusting the money supply to hit those targets.⁴⁹¹ In effect, Bob ends up with a much less predictable investment environment and the bane of business is lack of stability and future predictability. Consequently, Bob's decisions are no longer accounting-based but are simply gambles.

In an exchange with Massimo Morini, author of the earlier cited paper *Inv and Sav Wallets*, came to similar conclusions:⁴⁹²

This is essentially a syllogistic paradox: for Bitcoin to grow in economic relevance, people need to spend bitcoins for transactions. But if people anticipate that Bitcoin will grow in economic relevance, they know bitcoins will also grow in value so people will be motivated not to spend them but to hoard them. Thus bitcoins will not grow in economic relevance, and in this case they will also stop growing in terms of value. We may not be so far away from seeing this happen.

Non-flexible supply or demand is one crucial curse of bitcoins. This is one of the things I try to address in this paper: dividing the players who have an incentive to hoard because they get the gains from growth of the currency, from the normal player that want stable

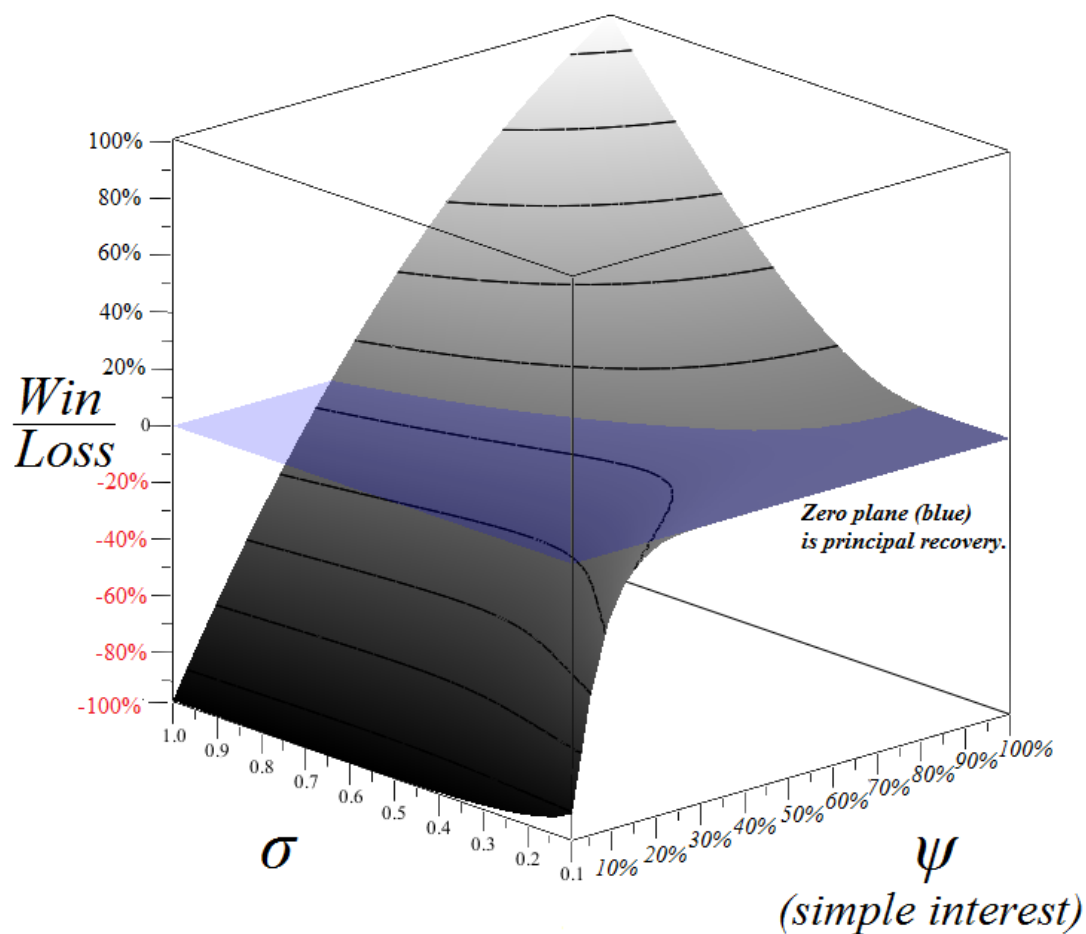
prices and wallets and like the currency for its transactional abilities. Unfortunately, even the idea proposed by Ferdinando, to transform the growth of bitcoin value into a proportional growth of wallet amount for everyone, there remains a distorted incentive to hoard.

In the real economy, saving money with financial institutions is beneficial because it does not “sit on the sidelines.” Bob deposits it in a bank and they in turn lend it out for productive purposes (e.g., loaned out to Alice who then builds a factory). Hoarding a medium of exchange does not do anything or create value; it has no productive input on the economy because it simply sits and remains stagnant.

According to Brian Hanley, one of the core hurdles that Bitcoin as start-up economy faces:⁴⁹³

You can't expand a money supply by deflation, this is deadly to an economy. Reserve banking is impossible with bitcoin; it has unified the unit of account and the unit of exchange. Because you can't do banking, the only thing that can be done with bitcoin is hoarding, which is not saving. In a bank, money saved is kept in circulation, it is used. When a medium of exchange is hoarded, it is useless to anyone. There is little meaningful difference between hoarded bitcoin and lost bitcoins.

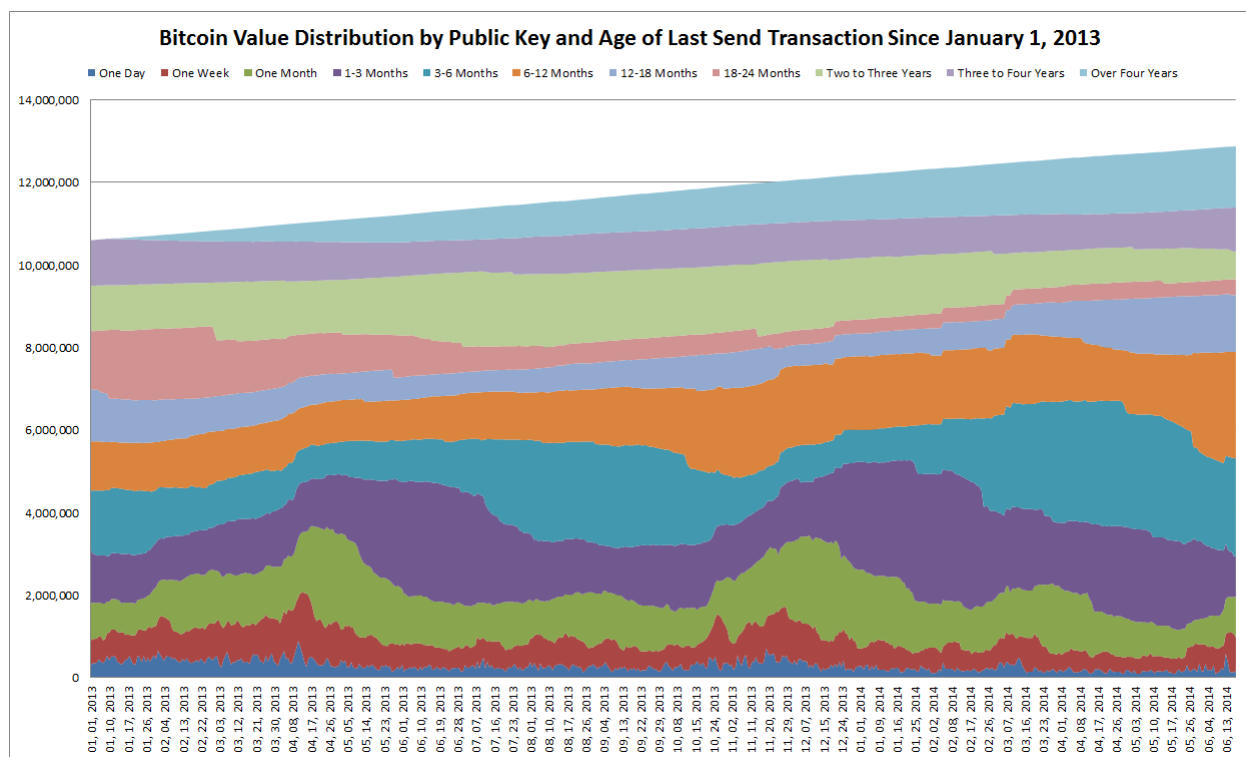
Bitcoin creators misunderstand wealth creation. Wealth is created by loans. Loans are money in the present given with the promise to do useful work for society in the future. Similarly, virtually all money in existence is debt money. It exists because it is owed to someone else. Society uses money as a circulatory system for distribution of goods and services to individuals. Any hard-currency monetary system that cannot create new money as needed (through loans or minting it to meet requirements) is a zero-sum game. Zero sum games have interesting characteristics. They force all loans to get loanshark interest rates or on average investors lose.



Source: Brian Hanley

Modern money is supposed to be a medium of exchange and consequently money needs to change many hands to create a vibrant economy. With hoarding, velocity is zero. Again, there is a difference between saving and hoarding. If Bob is saving funds in a bank, he is essentially saying he does not have a need for it right now (e.g., low time preference) and instead will lend it to someone who does have a productive need (i.e., lend it to the capital markets, to Apple or Tesla who can then build and create additional value and wealth). If Bob put it under the mattress, which is how the Bitcoin protocol treats ledger entries (a “bitmattress”), the value of the money could increase yet there is no overall economic productive gain because there is less to go around the economy.⁴⁹⁴ In fact, as Hanley has noted, it removes it from circulation.⁴⁹⁵ So it exacerbates the problem of attempting to make interest on any investment. The game outcomes shown above, assume all players are spending their money without hoarding.

And we see this behavior on the blockchain today.

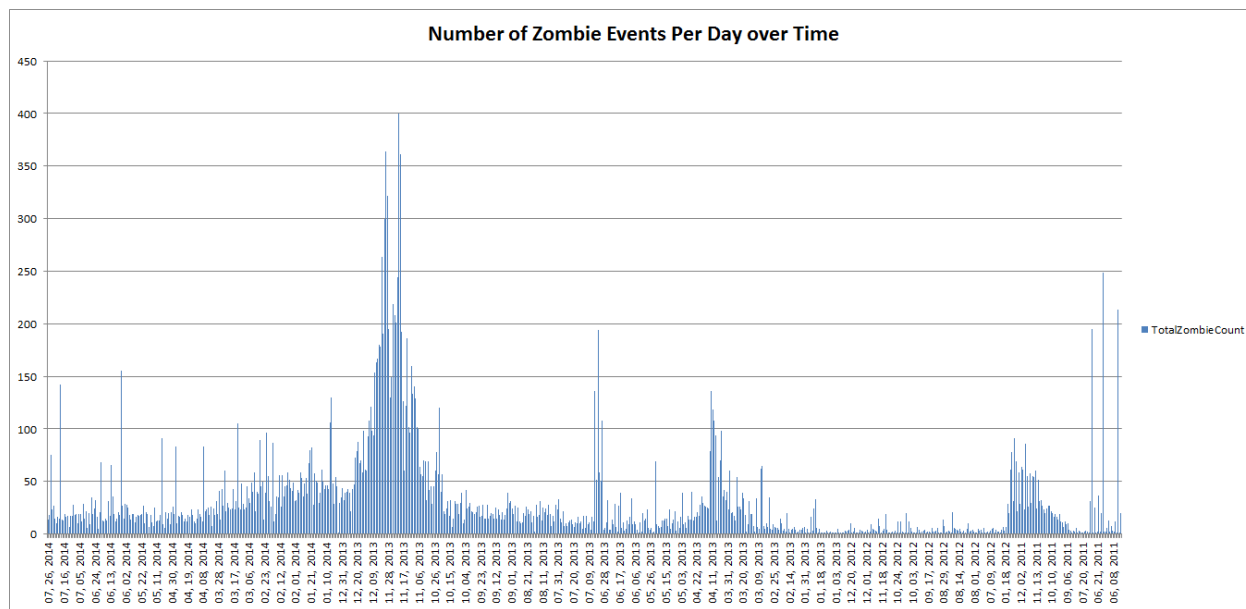


Source: John Ratcliff

In June 2014 John Ratcliff published an explanation about “zombie bitcoins” (coins, or rather UTXOs, that have not been active in more than 18 months) which is where the chart above comes from.⁴⁹⁶ Each color band represents the last time a private key corresponding to these UTXOs was used.

Thus, one take-away from this chart is that liquidity – as shown by the One Day, One Week and perhaps One Month bands – represents between 100,000 to 2,000,000 bitcoins. What is the actual number? Without a full traffic analysis we probably will never know. And as Hanley pointed out, what we do know is that there is no way to distinguish between hoarded coins and lost coins; and consequently neither is actively able to create economic value by remaining comatose.

The following month, Ratcliff further explored the “zombie coins”:



Source: John Ratcliff

In his words the chart above shows, “the number of zombie events that occur daily over time. As you can see, during periods when the bitcoin price is going up, the number of zombie events (indicating people cashing in and moving old bitcoin public keys) goes up substantially. Note that this is just a total count of events. It does not graph value.”⁴⁹⁷ Note that the x-axis is in reverse chronological order, from July 2014 through June 2011.

Two years ago, Dorit Ron and Adi Shamir of The Weizmann Institute of Science published a paper, observing a similar pattern of dormant coins:⁴⁹⁸

Here is our first surprising discovery, which is related to the question of whether most bitcoins are stored or spent. The total number of BTC’s in the system is linear in the number of blocks. Each block is associated with the generation of 50 new BTC’s and thus there are 9,000,050 BTC’s in our address graph (generated from the 180,001 blocks between block number zero and block number 180,000). If we sum up the amounts accumulated at the 609,270 addresses which only receive and never send any BTC’s, we see that they contain 7,019,100 BTC’s, which are almost 78% of all existing BTC’s.

However, 76.5% of these 78% (i.e., 59.7% of all the coins in the system) are “old coins”, defined as bitcoins received at some address more than three months before the cut off date (May 13th 2012), which were not followed by any outgoing transactions from that address after they were received... This is strong evidence that the majority of bitcoins are not circulating in the system... Note that the total number of bitcoins participating in all the transactions since the establishment of the system (except for the actual minting operations) is 423,287,950 BTC’s, and thus each coin which is in circulation had to be moved a large number of times to account for this total flow.

At the time, in fall of 2012, the fact that 59.7% of all mined bitcoins were stagnant was met with a non-plussed response: there was very little to buy, sell or trade them for. Has that changed since then?

What we can tell from the spikes in Ratcliff's chart that the largest movements take place during volatile time periods, specifically during price run-ups. So, for instance, in the spring of 2013 there was enormous Western media attention and a subsequent boom that peaked in mid-April when Mt. Gox, the largest exchange, had to temporarily shut down. Similarly, November and early December 2013 corresponds with additional global media coverage and Chinese adopters coming online – with prices peaking on December 4th. Or in other words, transactional volume rises and falls with price levels – the bulk of on-chain activity corresponds primarily to day trading and speculation. This, despite the fact that Ratcliff notes that prices during this 18 month time span increased 4,000%. If money increases in value isn't it, so goes the narrative, intuitive that users would spend more of it?

That is to say, even though there are now more than 63,000 merchants (and perhaps as many as 100,000) that accept bitcoin and even though token valuation has risen logarithmically, UTXO holders as a whole prefer speculating over conducting actual commercial activity. What could change this behavior?

Maybe nothing will because Bitcoin is a recreation of a medieval agrarian economy; few people spend, in part because the network codifies what is essentially negative time value of money.⁴⁹⁹

Or as Dan Kervick independently surmised:⁵⁰⁰

So you can see why you would very much like to be a miner in a thriving Bitcoin economy and why early adopters of Bitcoin are so fanatical about keeping the system going. Those who manage to accumulate bitcoins in the earlier stages when the pace of bitcoin creation is high, could profit handsomely when the deflationary phase kicks in. These miners would, if the world-conquering dreams of the Bitcoiners ever came to pass, be something like the descendants of medieval vassals who acquired some poor land from their lords in an early era when there was still much land to be claimed and settled, and who then became fabulously wealthy over time by hanging onto their holdings as the finite stock of land was all brought into private ownership and production while the population continued to increase.

What about wages?

In April 2014, *The Economist* wrote a response to Mike Hearn, a developer who works on the Bitcoin core team (whom I have cited several times), regarding how Bitcoin-denominated wages have problems endemic to this deflationary environment.⁵⁰¹

I think Mr Hearn may have misunderstood the piece's argument. It was not that deflation would kill Bitcoin. Rather, it is that deflation will prevent Bitcoin from becoming a unit of account, and that, in turn, will keep it from displacing traditional

currencies. But Bitcoin could survive and indeed thrive without becoming the coin of the realm.

The issue, as the piece explains, is that deflation in the unit of account leads to unemployment, thanks to the fact that wages generally don't adjust downward. Mr Hearn suggests that the idea that deflation might be costly is controversial among economists. I must disagree; it really isn't. Economists would love it if he were right that deflation didn't matter—that money, in economists' parlance, is neutral. If wages adjusted quickly and cleanly then they could go back to applying really straightforward classical economic models and everyone's life would be simpler. But the data are very clear on this point; wages are "sticky", and so deflation in the currency in which wages are set is costly.

A unit of account is one of the core attributes of money, providing a unit of measurement for defining, recording, and comparing value. A “sticky wage” (also called nominal rigidity) is one that is not flexible, that does not respond to macroeconomic shocks. What this means is that because of how relatively volatile Bitcoin-denominated prices are, that participants (both employee and employer) would continue using a unit of account such as dollars and euros; real economic calculation would be done in fiat instead of bitcoin.

In his paper, *Hayek Money*, Ferdinando Ametrano sees a similar problem with wages and loans:⁵⁰²

The unfeasibility of a bitcoin loan is similar to that of a bitcoin salary: neither a borrower nor an employer would want to face the risk of seeing her debt or salary liabilities growing a hundredfold in a few years. A manufacturing firm cannot accept an order in bitcoin with the risk of its value doubling or halving on a single bad day. Even the development of a derivative market could only hedge these risks with an implausibly high price. This is the cryptocurrency paradox: arguably the best ever kind of money by any metrics, marred by the severe inability to serve as reliable unit of account.

Money and credit

There is an endless stream of papers and books on the topic of what constitutes the attributes of money. Arguably one of the most thorough explanations of what money is and how it arose is, *The Ascent of Money* by Niall Ferguson which was later turned into a series on PBS.⁵⁰³

Despite what some Bitcoin advocates claim, gold itself was not used on a large scale since time immemorial. In practice, there were numerous types of physical assets ranging from metals to Rai stones and seashells and to cigarettes.⁵⁰⁴ England even used a system of money known as tally sticks for several hundred years.⁵⁰⁵ And the reality is that prior to the birth of civilizations, many tribes and villages operated with barter and gift systems with themselves and one another. Some never even created something akin to “money.”

In her book review of David Graeber's book, *Debt: The First 5,000 Years*, Gillian Tett explains this further:⁵⁰⁶

Still, Graeber's book is not just thought-provoking, but also exceedingly timely. His sweeping narrative history essentially argues that many of our existing ideas about money and credit are limited, if not wrong. Take how we think that money evolved. In modern society, Graeber argues, economists often assume that money emerged as a medium of exchange to replace barter, while virtual credit developed after that. After all, gold is easier to carry around than sacks of potatoes or cows – and credit cards are a very recent invention.

However, Graeber asserts this sequencing is wrong: his reading of history suggests that complex debt relations, in the widest sense, emerged before coins circulated (and before complex systems of barter, too). Back in 3,000BC in Mesopotamia, people were keeping records of who owed what to whom – but were barely using coins. And today, numerous non-western societies operate with fiendishly complex debt systems, which blur social and economic obligations, even if they barely use "currency". Indeed, anthropologists spend a considerable amount of time looking at how these "debts" bind groups together. "There is nothing new about virtual money. Actually this was the original form of money," Graeber argues. "Credit systems were interspersed with a period of bullion, but credit came first."

As noted by Ferguson, up until the Renaissance, there were no real financial instruments or professionalized banking or hedging methods in the West. Bonds, joint-stock corporations and insurance companies evolved throughout time (all post-Fibonacci).⁵⁰⁷ And consequently, this is reflected in the dearth of economic output at the time. That without a way to expand credit – to create loans to start businesses – the pie cannot be enlarged. In his words, "Credit and debt, in short are among the essential building blocks of economic development, as vital to creating the wealth of nations as mining, manufacturing or mobile technology." In contrast, poverty (subsistence) more often, "has more to do with a lack of financial institutions, with the absence of banks, not their presence."

Or in other words, the expansion of credit through fractional reserve banking was a key disruptive technology, a real innovation in finance.⁵⁰⁸

Fractional reserve banking

Another issue that is somewhat related to the lack of a fractional deposit mechanism in Bitcoin that perhaps goes under-addressed is the dynamic by which cryptocurrencies are inextricably linked with prevailing fiat currencies.

This is a point addressed by Marc Pilkington in his paper, *Complexity theory and Bitcoin*.⁵⁰⁹ In it, he contends the existence theorem that Bitcoin's viability can only be initially measured by

the quantity of fiat currency that it can buy (i.e., its exchangeability therewith) implying that Bitcoin cannot exist without fiat currency at a point in time.

In his words:

Furthermore, the epistemological stance of the researcher investigating Bitcoin, a market-driven currency, vis-à-vis traditional fiat currencies, is complex. Ironically, while Bitcoin, a twenty-first century digital claim of wealth, is touted in libertarian circles and by proponents of alternative (non-mainstream) frameworks, as an alternative to fiat currency, its viability can only be initially measured by the quantity of fiat money it can buy (i.e its exchangeability therewith). In an international monetary system dominated by fiat currencies, we call this result the Bitcoin existence theorem. In classical logic, the law of excluded middle states that, for any proposition, either that proposition is true, or its negation is true.

For instance, let us consider the following propositions.

(1) Bitcoin can exist without Fiat Money

(2) Bitcoin cannot exist without Fiat Money

It follows that (1) and (2) cannot be true simultaneously. According to the Bitcoin existence theorem, proposition (2) is true for fiat currencies exist

Given that the fiat system will continue to be subject to state seigniorage, it would seem that the existence theorem has bearing on how an eventual system of lending would evolve within Bitcoin if it ever should.⁵¹⁰ Namely, in the flavor that makes it difficult for the interest rate regime governing lending and borrowing within a cryptocurrency context could ever be truly divested from such regimes that prevailed in the primary fiat currencies “defining” value within the cryptocurrency context in an exchangeability sense.

More simply, this may suggest that should Bitcoin ever gain true “moneyness” whether it would not be forever subject to Gresham's Law in a way that makes gold impractical as true replacement for fiat for purposes of mass-transaction. Even assuming a stable system of lending could be implemented in Bitcoin, the rates of lending would likely be at least in some sense derivative of fiat rates. In such a system of *de facto* “competing” currencies, the temptation to hoard would still be present, albeit originating now more centrally on the basis of Gresham's Law as opposed to deflation.

Coinbase could turn into a fully-fledged bank, providing interest to bitcoin holders to be able to loan out bitcoins (much like BTCJam and Bitbond do). And they could do this through a fractional reserve banking (FRB) process. While many early adopters are ideologically opposed to FRB, Huobi’s new Hong Kong branch (BitVC) may be heading in that direction already: users can lend funds to Huobi for interest and Huobi will then lend it out to users to trade on

margin.⁵¹¹⁵¹²⁵¹³ Contrary to what many Bitcoin adopters contend, fractional reserve banking itself is not inherently a bad thing.

Yet according to Matt Levine with *Bloomberg View*, the proposed BitLicense regulations in New York state mean that startups (e.g., non-chartered institutions) are not allowed to implement fractional reserve lending:⁵¹⁴

What this means is that if you're in the business of bitcoinery -- "receiving Virtual Currency for transmission or transmitting the same; securing, storing, holding, or maintaining custody or control of Virtual Currency on behalf of others; buying and selling Virtual Currency as a customer business; performing retail conversion service ... or controlling, administering, or issuing a Virtual Currency" -- and you owe bitcoins to customers, then you need to have 100 percent of those bitcoins sitting in your bitcoin vault. *And* you can't borrow against them. *And* you need to have some extra cash in dollars, just in case (in case what?). *And* you need to have however much capital Ben Lawskey decides you should have.

[...]

But, obviously, there is one sort of business that doesn't run on this model. *Financial* companies basically take your money and put it in places where it makes money for them while you're not looking. Banks, in particular, take deposits and lend or invest them back out. If I put \$100 in the bank, the bank does not just put a crisp \$100 bill in an envelope labeled "For Matt, whenever." The bank takes my \$100 and buys credit derivatives or whatever with it, and relies on the well-understood magic of banking -- maturity transformation, diversification, deposit insurance, etc. -- to answer the question, "what happens if I want my \$100 back?" That's why, instead of charging me a fee to hold on to my money, my bank can pay me a very teeny amount of interest.

Other financial intermediaries don't do exactly this, but there is a general theme of making money by using the customers' stuff when the customers aren't using it. This will not fly with Ben Lawskey, though, when it comes to bitcoin businesses. Bitcoin businesses, in New York, will have to be far more conservative than regular financial businesses.

While these regulations will not be finalized and enforced until later this fall it looks like you have to be a bank, to be a bank.⁵¹⁵

However, prior to BitLicenses, competition from other cryptocommodities had the potential to make the total monetary stock more elastic and decentralized – effectively creating a type of FRB (though it is debatable if it would have worked without massive counterparty risk).

With his permission, I have reprinted several relevant portions of Brian Hanley's paper, *The False Premises and Promises of Bitcoin*, which help describe fractional reserve banking with respect to bitcoin.⁵¹⁶

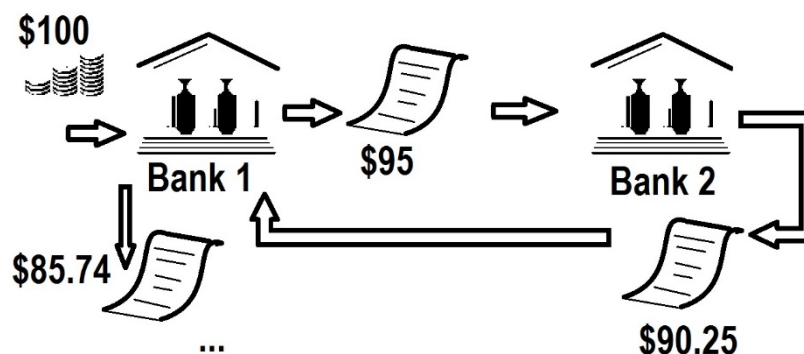
In terms of banking:

The core of the issue is that since bitcoins are unique and cannot be duplicated, bitcoin can only exist as an electronic analog kind of physical coin. Ergo no money can be created by making a loan.

In the long past, enough gold or silver was, at least in principle, required to cover reserve requirements at a bank. The need for more gold to act as the core for banking reserves was once a major matter of concern for nations. Physical currency transactions in economies began to dwindle in the 14th century with the establishment of banks in Europe⁵¹⁷. Gold and silver backed currency standards came and went versus fiat money in the 19th century. This continued until the formal ending of the gold standard in the USA in 1971, and in 2000 the formal end to the 40% backing of the Swiss Franc by gold.

Since all bitcoins are actual coin, the amount of bitcoin is limited, and bitcoins cannot be created on demand, it is impossible for bitcoins to be used to make loans since every loan would need to be made in actual bitcoins. To clarify this let's review a classical toy banking model based on 5% gold reserves as shown in figures 3 and 4.

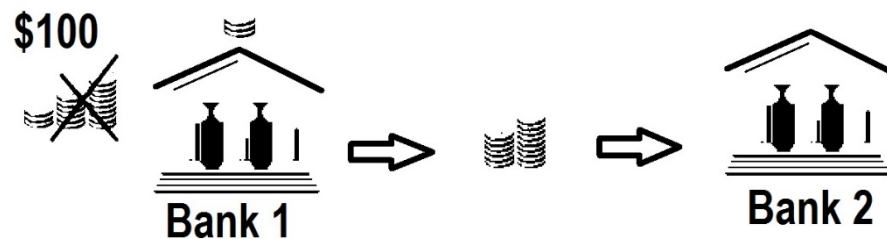
Figure 3: Three iterations of loans in a 5% reserve banking system.



An initial hard currency (gold) deposit is entered into the books of Bank 1. Loan paper is created of 95% of the reserve. This is "virtual money" deposited into Bank

2. Bank 2 credits this virtual money and makes a new loan, of 95% loan which is deposited into Bank 1, and that in turn is accepted on Bank 1's books, a new loan is made, etc. The result is $\$95 + \$90.25 + \$85.74 = \189.49 . And that money creation can continue to the theoretical $1/r$ limit, where r is the reserve fraction required.

Figure 4: Physical coin system.



An initial gold deposit is placed in Bank 1 and logged into its books. Loan paper is created of 95% of the deposit. But this time the loan must be redeemed inside Bank 1 for the \$95 in physical coin, and is carried out of bank 1 to deposit into Bank 2. When it is done, Bank 1 has \$5 in coin and Bank 2 has \$95 in coin. There is no change in the amount of money in the system, because no new money has been created by credit.

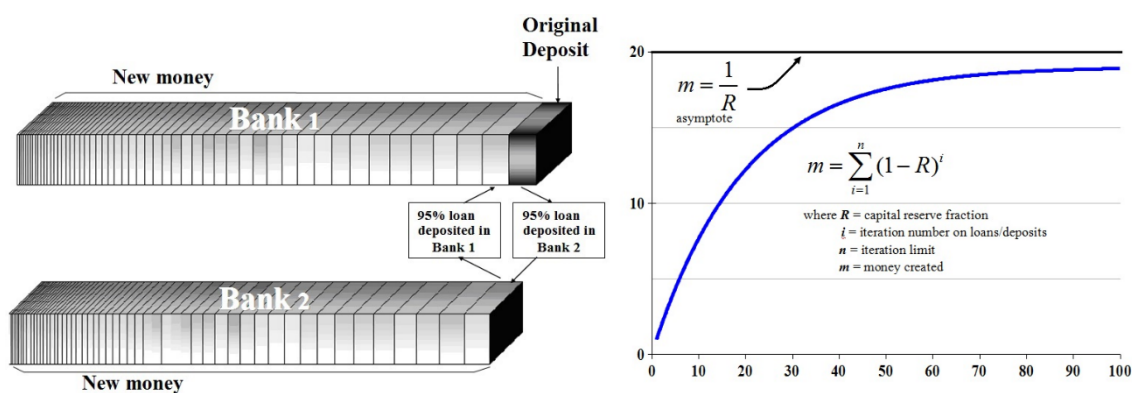
We have one of two choices here. We can allocate a new *virtual-bitcoin* to the depositor for 95% of the value of his deposit. Or, we can allocate the loan to as *virtual-bitcoin*, usable as if it were bitcoin, but not actually real bitcoin. *Virtual-bitcoin* is precisely the kind of money that bitcoin was designed to prevent, because bitcoin's designers did not think the problem through.

Figures 3 and 4 are schematics for a classical toy banking system based on a single gold deposit. In the real world, even for a gold-backed currency, things were more complex than shown. In the time of gold-backed currency, banks had capital reserves (today tier 1 and tier 2 capital, per Basel accords⁵¹⁸) and those reserves were provided

by the bank's partners or stockholders, not regular depositors. The diagrams here don't differentiate this.

Capital reserves ensured bankers had "skin in the game" that they would lose if their loans went bad. Their capital regulated how much deposited money could be loaned out. But records indicate that reserves in the old system varied widely. Even as long ago as the 1840's and before, in the heyday of gold-backed currency, a bank might operate at times with practically non-existent reserves, and this was fine for the economy⁵¹⁹. Thus, the difference between gold-standard and fiat money of today is less clear from evidence than it is in theory.

Figure 5: Graphical representation of banking multiplier



Each time a loan is made, it becomes a new deposit of a bank. The width of each brick in the above diagram is proportional to its size. The size of each loan declines because of reserve requirements. Equations of the banking multiplier are on the right. In practice, there are usually temporal limits to the banking multiplier, because originating a loan takes significant time. Also, loans are demand driven, which is why strategies like quantitative easing (QE) have trouble – QE is metaphorically pushing a rope.

Additionally, unlike the toy model, money from a loan would not necessarily come onto the books of a bank until it was spent. With gold and silver certificate paper notes,

bank letters of credit, and bank cheques used to spend money, the net effect was similar to what is shown in figures 3, 4 and 5, but considerably messier. However, this classical toy model of banking has been good enough to educate beginning students for a long time, and is the basis for the mathematical derivation of the money multiplier asymptotic limit, so it is acceptable here.

Figures 3 and 4 make clear that creating loans based on bitcoin would require a new entity, the *virtual-bitcoin*, which would be backed by bitcoin, but not actually be bitcoin, just as gold-backed currency is backed by gold but not actually itself gold.

In this *virtual-bitcoin* scenario, bitcoin banks would keep bitcoin on reserve and redeem the *virtual-bitcoin* for real bitcoin in transfers, payments, etc. Such *virtual-bitcoins* would no longer be specific bitcoins that were deposited into an account, but instead be a *note* allowing the bearer the right to use it as if it were real bitcoin. This would correspond to a time in America many years ago when banks issued their own gold-backed currency, and the value of a bank's currency tended to vary with distance from the issuing bank.

No provision for *virtual-bitcoin* to exist in order to expand credit has been made in its design, and such ideas as paper currencies or accounting credits are anathema to the bitcoin community. The whole point of bitcoin is to force electronic transactions to only use these tokens that cannot be duplicated. To make *virtual-bitcoin* work would require a central clearinghouse to authorize the transactions, and then bitcoin would have come full circle – implementing the central clearinghouse accounting authority it was created to put an end to. Even if the objection of the bitcoin community to the idea of *virtual-bitcoin* could be overcome, it has other serious problems.

Primarily, why would a holder of a *virtual-bitcoin* note ever do anything except immediately present it for redemption in real bitcoin? We are not living in the naïve era of the Medici bankers, who could implement reserve banking without anyone being the wiser. Consequently the account holder would want to take possession of the underlying asset to prevent loss. I suppose some might prefer the *virtual-bitcoin* if enough interest

was paid. But that would be certain to end in a bank run, and the result would look very similar to a Ponzi scheme.

Physical coin (gold, silver, etc.) is heavy, bulky and inconvenient. Bitcoin is not bulky – bitcoin has indeed solved that problem gold and silver have. All the bitcoins ever made could be held in a digital ‘wallet’ on a thumb drive. So the ancient motive of depositors to have a safe place to store their inconvenient, hard to safeguard money does not exist with bitcoin – except that bitcoin can be stolen⁵²⁰. But is the problem of potential theft large enough? And an even better question is, does risk of theft go up because of depositing bitcoins, or even trading them on an exchange? Evidence indicates it does⁵²¹⁵²².

With the invention of secondary markets for derivatives and contracts (for swaps, forwards and options) which in turn could be collateralized, FRB may have been a possibility in the long-run; though as Hanley noted, this would likely require a centralized counterparty to track these assets.⁵²³⁵²⁴ Either way, BitLicenses may limit these possibilities going forward.

And even if FRB was allowed, Coinbase and others – while on-ramping a lot of new users and providing utility through ease-of-use functionality – have a long way to go before this could occur. For instance, in June 2014 Coinbase announced instant buyback – once you spend bitcoins, you can immediately buy more with one mouse click.⁵²⁵ Yet, the reddit comment below sums up actually what happens:⁵²⁶

The optics of this from the outside are terrible.

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

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

This is a classic example of using technology for technologies sake (e.g., overengineered solutions) as illustrated in the following example. By replacing the word “bitcoin” with “RMB” the outside observer can see that no fundamental benefit or value was added for consumers. To them, the transportation is invisible. Instead what matters is holding RMB and counterparties settling trade obligations in RMB – or in this case bitcoin, which merchants do not as they immediately convert it to fiat.

In his paper, Evans explains this negative-sum game:⁵²⁷

Consider the second case where the consumer and the merchant are both insured. In that case the transaction makes no sense. The consumer uses dollars to buy coins from the wallet provider for a transaction, the wallet provider buys coins from an exchange, then the wallet provider sells the coins back to the exchange since it needs to pay the merchant in dollars, then wallet provider pays the merchant in dollars, and the consumer gets their purchase. Of course the wallet provider could dispense with coins entirely and simply take dollars from the consumer and pay the merchant.

In the real world, of course, people could also use unstable currencies to transact in and hedge their transactions with various foreign exchange products. But unless they have some legal or regulatory obligation to do this they would simply standardize their transactions using a stable currency.

Again, for the perspective of the consumer, bitcoin provided no value-added service in this scenario. If there is fraud or something happens with the merchandise on the other end of the purchase, Coinbase (or an entity like it) would still need to provide customer service. Furthermore, as noted by Evans, both merchants and consumers like stability – most do not have the time to analyze exchange prices each day to find the “sweet spot” to buy or sell. What if there is no “sweet spot?” And aside from immediate liquidation, Coinbase does not provide a hedging mechanism right now.

Consequently, Chris Dixon, a venture capitalist at Andreessen Horowitz which is an investor in Coinbase made a similar error in stating:⁵²⁸

For example, one of the most common criticisms of Bitcoin is that it is too volatile and speculative to be used as a payment system. Merchants want the stability of government-backed currencies. Buyers don’t want their Bitcoin exposure to fluctuate whenever they transact in Bitcoin. Coinbase has solved this problem. Merchants can instantly convert any Bitcoin they receive into dollars. Buyers can automatically replenish any Bitcoin they spend. Transactions that use Coinbase this way create zero net Bitcoin exposure for either party. Volatility is no longer an issue.

It could be worthwhile to use bitcoins to transact international business, assuming that the spread plus fee charged by the clearing house (bank, credit card company, or the party converting the currencies) is greater than whatever fee Coinbase charges.

But, in practice, this is untrue for transactions in the same country, the regular day-to-day transactions which a currency is supposed to facilitate. Anyone holding bitcoins is the one exposed to its volatility. In the scenario above, if merchants simply convert bitcoins immediately, this defeats the purpose of using bitcoins in the first place as David Evans has explained. Or in other words Coinbase just becomes a frictionful fee tree. Why accept bitcoins if you instantly convert them, how is this any different than say, accepting the RMB? If Coinbase is holding bitcoins, then it is exposed to this volatility, potentially turning it into a foreign exchange company with few legal ways to hedge it.

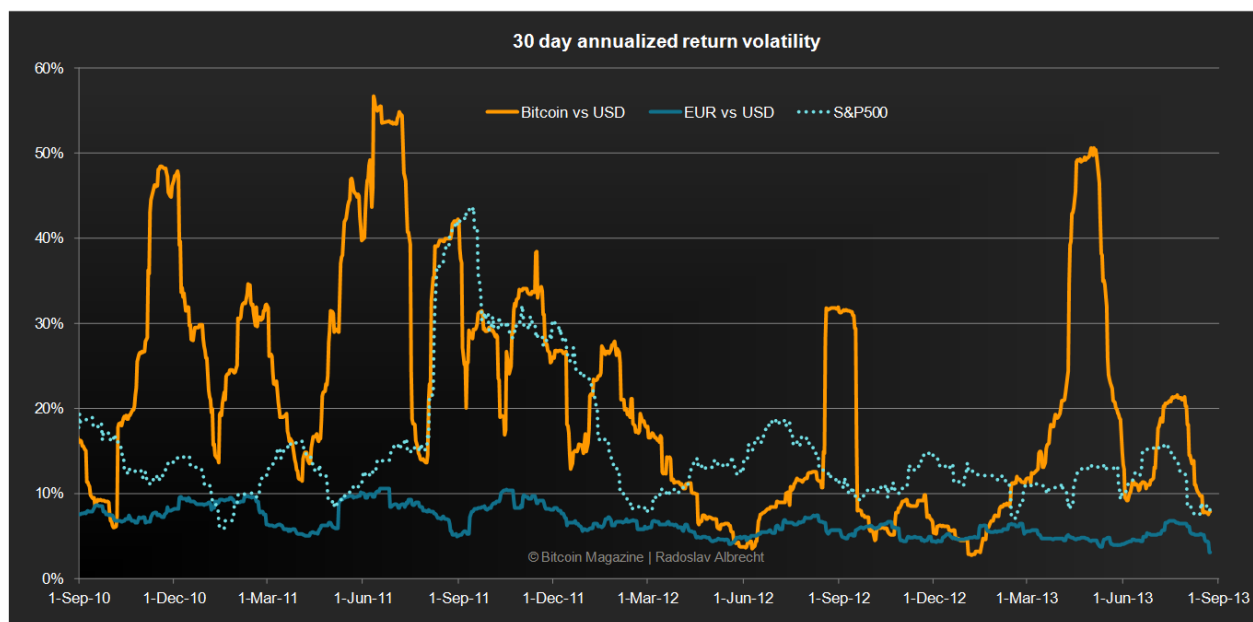
Won't the volatility eventually disappear as some proponents claim it will?

No, as Brett King, recently noted:⁵²⁹

Call it a *bubble*, call it a Ponzi scheme (if you don't understand it), or call it (as the US Treasury does) a *distributed virtual currency*, the biggest problem Bitcoin has had in the last two years has been one of volatility. While volatile commodities make for interesting investment plays for the more aggressive investors amongst us, it rarely is a good thing for a currency or a payments network. Herein lies one of the key problems for Bitcoin, to be a true force for disruption, it needs to be used by large groups of people. But most people like their currency and their bank balance to be highly *stable* — lack of stability is never going to stimulate mainstream adoption.

If you compare BTC versus the stock market, which is normally considered moderately volatile, it is clear that Bitcoin is still highly volatile — that needs to change before we fix the adoption problem. To be fair, though, it isn't significantly affecting the market for Bitcoin from a trading perspective. In fact, the volatility may have made it more attractive in the past.

The chart below, from Radoslav Albrecht, illustrates the annualized 30 day moving average volatility of Bitcoin versus the USD and S&P 500 between July 2010 and August 2013.⁵³⁰



Data sources: bitcoincharts.com; Yahoo! Finance; quandl.com; calculations from Radoslav Albrecht

During this time frame, based on calculations from Albrecht, bitcoins had a daily volatility of 7.2% and 135% annualized return volatility.

In Albrecht's words:

Comparing Bitcoin volatility with EURUSD we can see, that the EURUSD pair has a much smaller volatility. Only very rarely it crosses the 10% line. On the other hand, the S&P500 volatility is higher and fluctuates more. In 2011 it crosses the 40% line. Back in 2008, at the peak of the financial crisis, S&P500 volatility even went beyond 80% on an annualized basis. The Bitcoin volatility graph looks more like the S&P500 graph than like the EURUSD graph. Therefore, in the last three years Bitcoin prices behaved more like an asset than like a currency.

What does this mean in the long run then? According to Brett King:

While we're trading Bitcoin for capital gains, we're treating it as a commodity. While we're doing that, we're not going to see mass adoption of Bitcoin on the payments side, nor as a day-to-day value store (a replacement for the bank account).

What we need is to get Bitcoin wallets on phones, being used everyday. For that consumers need places to spend their Bitcoin — this is good transaction volume, as opposed to *bad transaction volume* which curtails adoption growth. The only other way to go is to encourage stable growth as an asset class, so that Bitcoin outperforms the stock market on returns, while being less volatile — given Bitcoin's nature as a pseudo commodity, that is extremely unlikely. If we encourage Bitcoin as an asset class, then the dreams of supplanting the centralized banking systems of the world dies.

It is worth highlighting that this trading pattern, that users treat bitcoins as a commodity in practice, long before any legal definition or government body (such as the IRS) attempted to codify the token as property. Or in other words, bitcoins from the onset were treated as a *de facto* commodity which some advocates claim was only a temporary role when it likely is permanent.

But that does not mean this particular service is frictionless. For instance, in another article, David Evans delved into the specific transaction costs of various platforms and explained:⁵³¹

Consider Coinbase. This bitcoin wallet charges the merchant 1 percent of the transaction amount. But that doesn't include the round trip for the transaction. Coinbase also charges 1 percent of the dollars loaded into the wallet plus 15 cents. The round trip cost of a transaction that begins with the consumer buying bitcoins for the wallet is therefore 2 percent, ignoring the 15-cent fee.

This 2% + \$0.15 is roughly on par with competing systems and obviously higher than the 1 percent that is frequently cited.⁵³² Perhaps these margins will change, but the fixed income miners receive will not and that impacts the incentive structure.

Similarly Ben Edelman, an associate professor at Harvard found that consumers pay more when they pay with bitcoin.⁵³³

Usually, consumers pay the same bottom-line price no matter what payment mechanism they choose. Cash, credit, and (perhaps) Bitcoin are all the same price. Savvy consumers choose a payment mechanism based on benefits, seeking the best rebates or points. This market structure has predictable incentives: I choose a Visa Signature Preferred card with 2.2% cash back not because it's the cheapest to merchants (it's not) but because it's the best for me. (It's hard to find a card with a larger rebate.) Indeed, to a merchant, my Signature Preferred is surely the *worst* of Visa's offerings because it carries the highest interchange fees (charged to credit card processors, and in turn to merchants) of any Visa card. But a consumer has no reason to consider or care about those costs to merchants.

How does Bitcoin fit in? Suppose I wanted to buy shoes at Overstock that cost \$100. If I pay by credit card, the receipt says \$100, but my card's rebate means I actually only pay \$97.80. If I wanted to pay with Bitcoin instead, I'd need to open a Bitcoin wallet and pay \$101 to Coinbase to get \$100 of Bitcoins (at the current exchange rate). (The extra dollar covers a 1% fee to Coinbase.) If I hurry straight to Overstock, my Bitcoins should still be worth \$100. (They're as likely to go up as down in the time I have to wait.) But notice: The transaction ends up costing me \$101 by Bitcoin, versus \$97.80 by credit card. I might try it once as an experiment. But I have every incentive to stick with my credit card going forward.

To spur consumer adoption of Bitcoin, merchants should offer discounts for consumers who use it. Suppose Overstock's credit card processor charges 2.9%, a relatively standard fee. Is there a discount that makes Bitcoin preferable to credit cards both for me and for Overstock? It turns out that there is not. If Overstock reduces its price to me by 2.9% when I pay by Bitcoin, I still have to pay 1% to get the Bitcoins, which means I pay \$98.10 to get the shoes. That's still more than the \$97.80 I would pay by using my credit card.

Why would a consumer want to pay more without receiving at least the same benefits they had previously received (e.g., cash back rewards, fraud protection)? They probably do not, hence the low usage for bitcoins in this manner. And again, this is not to single out Coinbase, they are just used as an illustration and have for all intents and purposes been a good actor in this ecosystem. While not an endorsement, they are one of the more promising startups in part because they are trying to create value (and have).⁵³⁴

In conclusion, there is a difference between the money and economy Bob wants to have versus the money and economy Bob currently has. Today Bitcoin, as I have argued, is at most an emerging market akin to a pre-industrialized agrarian economy with enormous frictions (e.g., paying fees to go between fiat and bitcoin and vice-versa).

The next chapter will discuss the static reward structure wrought by the inelastic money supply.

Chapter 10: Bitcoin's command economy and knock-on effects

As noted in chapter 9, the Bitcoin network (as nearly all other cryptocurrency networks) operates very similar to a command economy. This is done through the arbitrary reward mechanism – the revenue (income) system – built into the protocol.

Internally Bitcoin is an inflexible command economy that outsources and arbitrarily rations its scarce resources (block rewards and money supply) irrespective of economic conditions (e.g., Bob, the miner, is rewarded whether or not he processes transactions). And front loading rewards the first four years without processing any transactions is an unsustainable activity.

In fact, as Jonathan Levin, co-founder of Coinometrics, notes in his new paper, *Creating a decentralised payment network*, he found that “[i]n total over the network history there have been 84,469 blocks with no transactions.”⁵³⁵ Yet because there is no one at the helm, no entrepreneur to rationally allocate block rewards or market value for those rewards the first year, ultimately as we will see below, 4.8 million bitcoins were given out for naught.

Many adopters note that this was done to help bootstrap the economy and that the initial distribution of bitcoins through the block reward is purportedly not how bitcoin will operate in the long run. And that at some point Bitcoin's internal economy will somehow be incentivized by transaction fees only – or at least that is theoretical transition (see chapter 3). But the fact that miners were rewarded irrespective and arbitrarily of their actual work is very similar to how top-down command economies work rationing wages. This is a topic that will likely be debated over the coming years.

For additional perspective I spoke with Martin Harrigan, a software developer and founder of Quantabytes, a cryptocurrency analytics start-up. In his view:⁵³⁶

The initial distribution of bitcoins is a one-time process that is distorting our understanding of the Bitcoin economy. I think that the peaks in transaction volume during the price run-ups are a form of secondary distribution: early adopters are distributing their bitcoins, for profit, to new users. This is a vital part of Bitcoin's distribution process and may continue for as long as there are periods of significant price increase. It may be that institutional investors will take-over a significant portion of this process for several years. Then, at some point, when the technology, infrastructure, regulatory frameworks, and our understanding of cryptocurrencies has matured, the price will stabilise and Bitcoin will return to individual users as a stable transactional currency in the traditional sense.

Of course, I'm speculating wildly here. My point is that we don't have a good null model. We're not seeing "hockey stick growth" but maybe that's okay. Many start-ups need this type of growth to survive -- I don't think Bitcoin does. During the Bitcoin crash of 2011 the price dropped 93% and didn't recover until 2013. The difficulty also dropped and remained stagnant for a year and half. Although I can't quantify it, the "mood" on the

Bitcointalk forums was grim. The equivalent event would have been fatal to most start-ups.

Perhaps, as Harrigan noted, this will change in the future. And perhaps those frictions are still lower than the cost of doing business in certain regions (like The Philippines).

Before we discuss that though, historically one way command economies were characterized in the 20th century is one in which a committee arbitrarily set wages irrespective of the amount, type or quality of labor involved. For example, in China, wages for doctors are still set at a flat rate by a planning commission, roughly 3,000 RMB per month (or 10,000 RMB per month in some cities) irrespective of the amount of patients you see (sometimes up to 100 a day) or quality of care you provide.⁵³⁷ Coupled with an explicit profit-sharing agreement with pharmaceutical companies through drug prescriptions, this has led to a number of perverse incentives for *underpaid* doctors to overprescribe medicines (which they receive commissions from) to compensate for their relatively meager salaries.⁵³⁸ For comparison, according to a 2013 report from the Bureau of Labor Statistics, the mean annual wage for physicians was \$187,200 in the US.⁵³⁹

How does this tie in with Bitcoin mining?

Any organization with limited resources will eventually run out of its assets if it continues in this fashion (coincidentally the Bitcoin Foundation itself has a 40% burn rate).⁵⁴⁰ And this is also what happens with the Bitcoin network which only has 21 million bitcoins in its 'trust fund' (to reuse an apt analogy). To incentivize early adoption, Satoshi Nakamoto, the creator, used an asymptote distribution method which essentially front loaded the reward cycle to the point where approximately 62.4% of all bitcoins have already been distributed in less than 6 years. The remaining will be similarly rewarded over the next 100 years. As detailed below, the reward schedule has not matched security incentives (block rewards) with security requirements (economic activity).

One of the purportedly core strengths of bitcoin (the currency) is that it follows a strict, inelastic monetary expansion hardcoded since day one.

There is no merit-based mining, all wages for the labor (mining) were arbitrarily set for perpetuity on January 3, 2009 and henceforth divvied out irrespective of economic conditions.

While this may sound like a strength to those who view monetary policy through a binary lens, this artificially caused distortions to the incentive and motivational mechanisms and has sustainability ramifications now that the network actually contains some commercial transactions.

I contacted Blockr.io and they provided the following data (that was cross-checked with Blocktrail):⁵⁴¹

- There are 84,580 blocks with “empty” blocks containing just coinbase transactions (a coinbase reward is the first transaction of a block, going to the miner who found the lucky number)⁵⁴²
- 83,867 blocks were rewarded 50 bitcoins each prior to the first halving day in November 2012, the remaining 713 blocks received 25 bitcoins
- There are an additional 12,404 blocks with 2 transactions (the coinbase transaction + one other)
- 12,223 of these blocks came prior to the block reward halving in November 2012 which equates to 611,150 and another 181 blocks each received 25 bitcoins (amounting to 4,525 bitcoins)

Altogether this comes to roughly 4.8 million bitcoins (~37%) of the 13 million total mined thus far that have been indiscriminately rewarded to labor participants, many of whom as noted in chapter 3, had very little downside risk of securing the network in the first couple of years (just turn on a laptop). In other words, unlike in other resource extraction-based industries there was no merit or performance-based decision making as hashers are rewarded for securing (mining) what are essentially transactionless blocks.

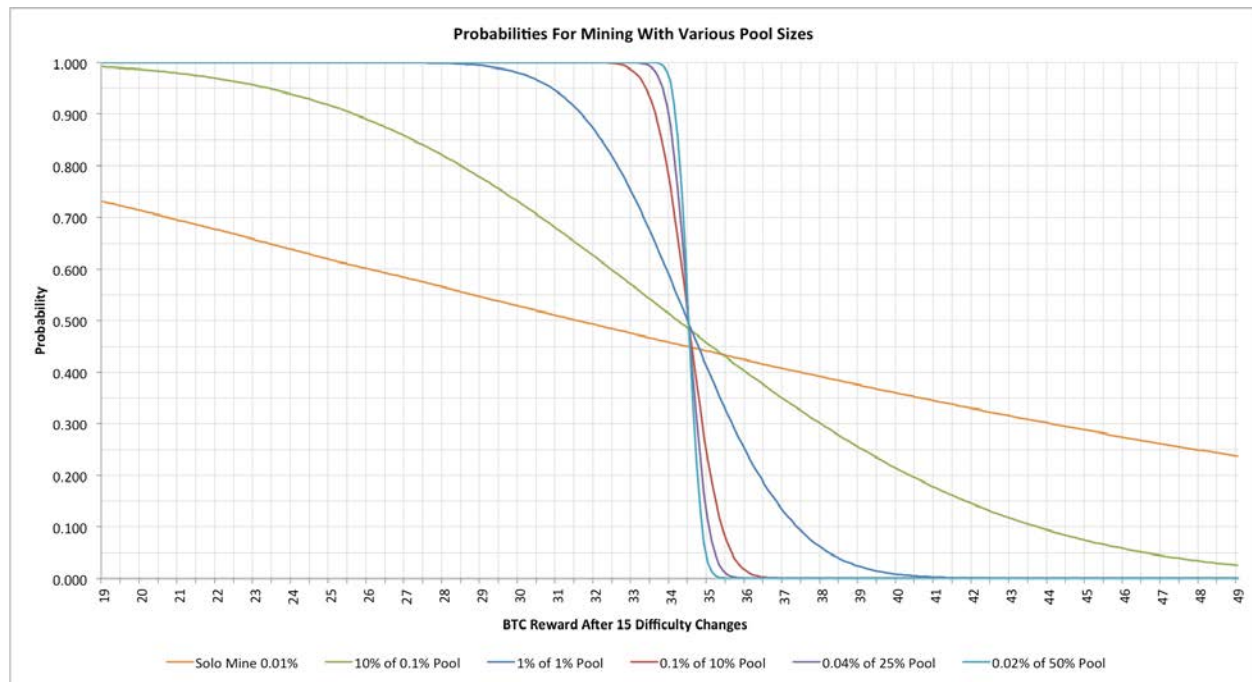
The mining pool Discus Fish (F2Pool) is a notable contemporary example in that they occasionally include only one transaction into a block (perhaps zero looks bad for public relations reasons).⁵⁴³ While speculative, there is some economic rationale behind it, because in practice, the smaller a block is, the faster a miner can broadcast and propagate it leading to less orphans. Or in short, they are maximizing profits. Further research will likely uncover the timing incentives (i.e., is it really just milliseconds or does it aggregate into larger non-trivial units of time?).

David Evans used agricultural labor as an analogy for this fixed payment conundrum. CNPE stands for constrained non-profit entity, his technical name for public ledgers like Bitcoin and a container is semantics for a block:

Then, during the growth period, the CNPE would follow the protocol in awarding laborers with durable containers (coins) in return for their efforts in processing transactions on the public ledger in addition to transaction fees. However, since the CNPE does not have any control over the price of the coins it has no control over the value of the awards. This incentive system is similar to a company hiring workers on a piece rate but where the value of the piece rate is variable and outside of the control of the employer. It would be like a blueberry farmer saying you will be paid X per 13 bushel you pick but where the blueberry farmer has no control over the value of X and where the worker therefore does not know the value of the piece rate. The piece rate would also have to be the same worldwide. Moreover, as we saw above the price of the containers at any point in time reflects long-run expectations concerning the demand for transactions on the platform. The price of the containers at any point in time

therefore does not even reflect current demand for using the platform. To take our blueberry example, the piece rate for picking blueberries does not necessarily even correspond to the current market demand for blueberries.

As described above, the network rewards quantity of hashrate and not transaction processing (e.g., amount or type of transaction). As a consequence you have participants that understandably try to capitalize off the system by pooling as much hashrate as possible sometimes without including transactions: why should they expend extra effort for little reward?



Source: Dave Hudson

The chart above was used in chapter 6 to illustrate the incentives of pooling. That investors with expected return on investments would rather be safe than sorry as anything less than a large pool is effectively gambling on lower probabilities.

What does this have to do with including transactions? Again, while more research will be needed to solidify the motivations for doing so, faced with the variance shown above there may not be a financial incentive to necessarily include transactions (or many transactions) within a block because the fee reward pales in comparison to the seigniorage subsidy.

This in turn results in potential free-rider issues – a conundrum that Gavin Andresen pointed out last year.⁵⁴⁴ It also leads to the question of: who are the actual decider(s) of this system?

One common rejoinder is that in the first few years there were no transactions or few transactions to include – that the first year alone was essentially no commercial transactions.

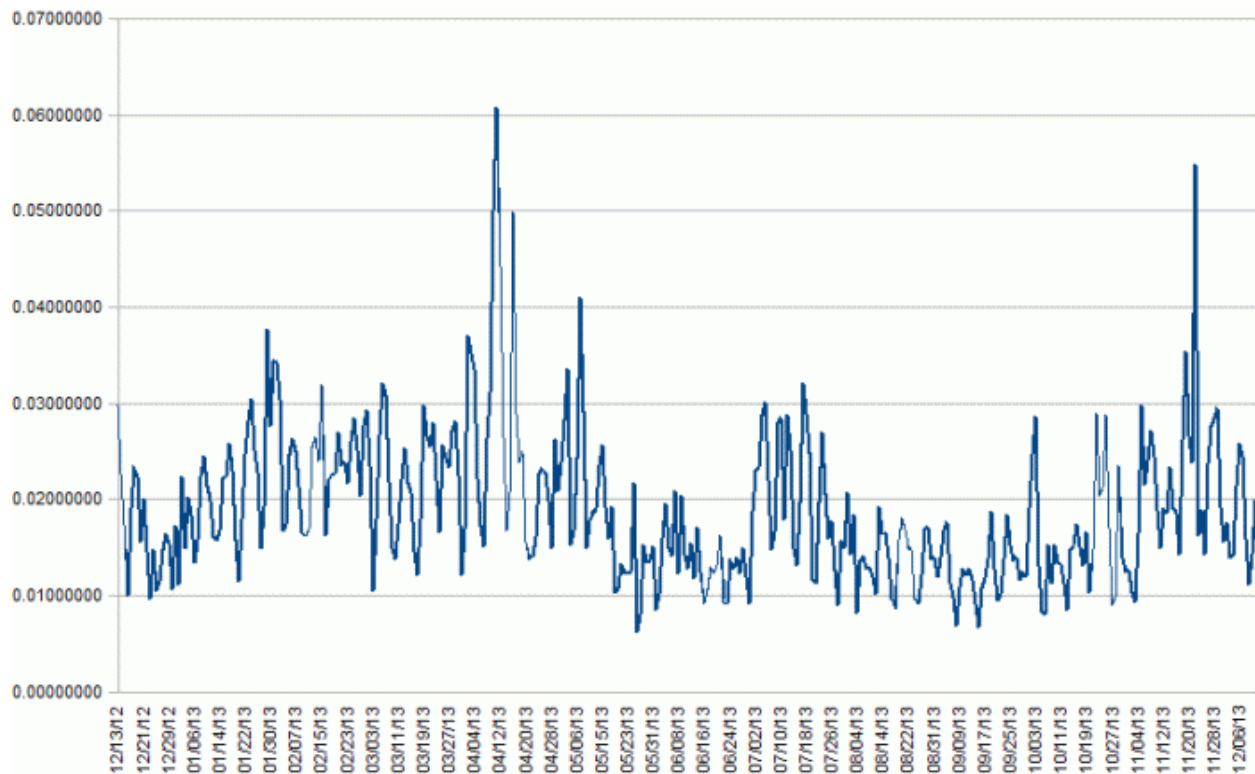
True, but a rational company, country or organization with a flexible ability to allocate scarce resources would simply, dynamically lower the amount of rewards. So instead of receiving 50 bitcoins perhaps the miner would receive 0.1 bitcoin, or conversely if a miner included even more transactions they would receive 100. It is unclear what the number should or should not be because there is no market process involved; the rationing of resources is arbitrarily done irrespective of the underlying conditions – just as the rationing process in command economies is.

Similarly, in its first several years of development, the general idea was that the economic activity on the network would result in a higher incentive to secure the network and that mining is simply the provision of security. This may still be the case long-term, however the data from the blockchain itself does not lend support to this particular interpretation.

To try and change this or set a minimum amount of transactions that need to be processed would introduce other unintended consequences that are part and parcel to price floors or minimum wages (i.e., recreational miners demanding “living wages”). Future analysis can be done on the possible changes that can not only be done but also explore ways to incentivize miners to adopt those changes (i.e., one view is that miners collectively have a long term interest in the networks health and rapidly depreciating capital supposedly makes them more adept to change).

Waiting to get rich

While it is unclear how much other positive-sum value exchange is taking place (such as exchanging construction equipment), with the exception of illicit activities, the on-chain transactional volume of Bitcoin has been relatively muted. Jason Kuznicki has attempted to describe the lack of growth in on-chain transactions in graphical form:⁵⁴⁵



Source: Jason Kuznicki

His chart, above, reflects the daily total transaction value of the bitcoin economy, denominated in U.S. dollars, divided by the total market capitalization of the bitcoin economy on that day, denominated in U.S. dollars. Though, it is probably not accurate to call it a ‘market cap,’ but rather the narrow money stock.⁵⁴⁶

Between December 2012 and December 2013, he points out, the velocity of bitcoins remained within a very narrow band.⁵⁴⁷⁵⁴⁸ The notable two largest peaks are in April 2013 during enormous global media attention of the platform creating a temporary bubble and at the end of November 2013 when Bitcoin Black Friday (BBF) was held. BBF was the busiest ecommerce day of the year for the network, which achieved 1.5 transactions per second (compared with the average of 0.7 transactions per second and its theoretical maximum of 7 transactions per second).⁵⁴⁹

He notes that:

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

bitcoin economy were becoming independent, we might expect a takeoff in the velocity of money, but we're definitely not seeing it yet.

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

For example, in his April 2014 testimony to the U.S. House of Representatives Committee on Small Business, Mark T. Williams, a lecturer at Boston University noted that:⁵⁵⁰

Since inception, Bitcoin has experienced extreme annual price volatility topping 140 percent.⁵⁵¹ Bitcoin is 7 times more risky than gold and 8 times more risky than the S&P 500. Compared to currencies it is 7 times more risky than the unstable Argentinian Peso and 15 times more risky than the U.S. dollar. As a result, it could be argued that small businesses that blindly accept Bitcoin are not actually in commerce but are in the high - risk speculative trading business. In contrast to small businesses, a Wall Street trading company might be willing to assume the triple - digit price risk posed by Bitcoin but only with experienced staff, sophisticated systems, strong controls and a large balance sheet to buffer against daily price swings.

Can small and medium enterprises cushion against this volatility? According to Williams, depending on the segment, small businesses may have less than 10% profit margins.⁵⁵² On any given day bitcoins price may fluctuate 5%-10% which would eat into and wipe out their profits.

In July 2014, Fred Wilson, an investor and venture capitalist with Union Square Partners, gave a speech at New York University and explored this conundrum:⁵⁵³

I also think we need to see real transaction volume happen. Right now, most people who get bitcoin hold it, they don't transact with it. That's part of what causes all of the volatility — if there was a very vibrant system where bitcoin was just getting swapped around like crazy, the velocity of the money would cause bitcoin's price to stabilize and there would be a much more liquid market. I think those are the kinds of things that as an economist you would want to see and I think if we saw those we could start to make arguments to the policy makers that you see this isn't property, it's a currency.

I think the real power of Bitcoin, this is my opinion, that the most powerful uses of bitcoin are as a global system that will work in any country in the world. That it is built on top of the internet for people to exchange value back and forth. We have to see people start to really use it in the way they do money, that they are spending it all the time and transacting it all the time. If peoples notions of bitcoin are that it is property

and you want to hold on and speculate on the way you would with gold, or a building or a stock I don't think we will realize all the transactional and financial benefits of bitcoin.

Unfortunately this is not something that can or will change in the future because of the attributes of bitcoin explored above and the collective behavior that would need to change in users. For example, according to the World Gold Council, as of December 2, 2013, there is roughly \$6.8 trillion in above ground gold.⁵⁵⁴ If bitcoin were to absorb the purchasing power of gold over the next decade as many proponents claim it will, the market value of a bitcoin token would need to increase by three-orders of magnitude, or roughly at a compound annual interest rate of 99.5%.⁵⁵⁵ Why would a hoarder spend a bitcoin with the view that it could increase in value at that rate?

In his December 2013 paper, Brian Hanley explored a similar scenario:⁵⁵⁶

Generating a transactional economic value close to the UK's economy spending virtually all the bitcoins in existence each year would allow us to minimize the required rise in bitcoin valuation. Starting from the valuation of \$430 per bitcoin would require bitcoin's valuation to multiply by 271 times over 5 years. That would be a 109% monthly compounded interest rate.

This upward volatility would incentivize participants to not spend but rather continue holding (or rather hoarding, as there is no savings mechanism built into the protocol). It would thus function not as a type of money, but as some type of commodity or collectible.⁵⁵⁷

The Wall Street Journal noticed the same Catch 22 that Fred Wilson described above:⁵⁵⁸

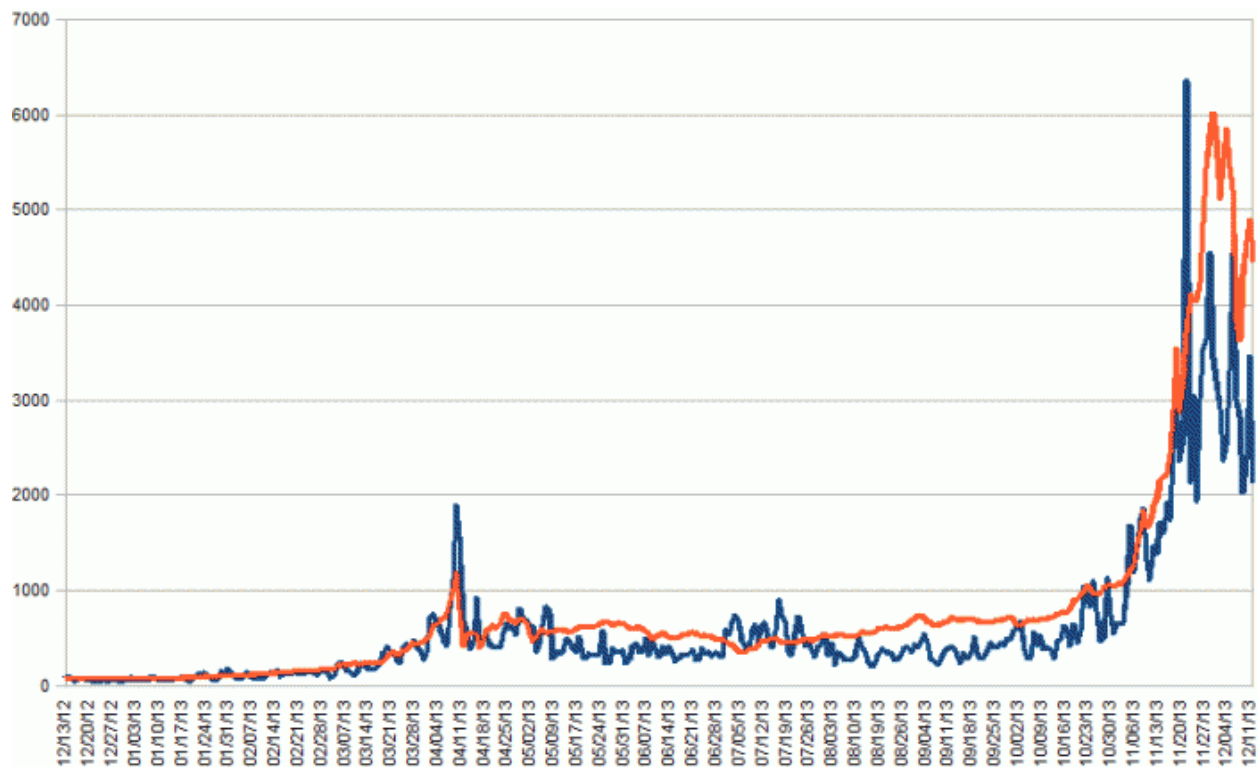
We've noticed over the past few months that hash rates have been rising. While they've been rising throughout bitcoin's existence, it seemed to spike the past few months, from a rate 90 million gigahashes a second, to a rate as high as 140 million gigahashes per second. But trading volume is low. That indicates there is increased activity *somewhere*, and if it's not turning into more spending in the general economy, then maybe Mr. Wilson's right; maybe people are hoarding it, in anticipation of higher prices down the road.

If that's so, it's creating a sort of Catch 22. Hoarding precludes spending, but spending is the sign that bitcoin's becoming a more regular feature of people's daily lives, and that is what would really drive up the price.

In other words, somebody's got to go out and buy a pizza or something.

Contemporaneously, most business that accept bitcoin payments do not see a continual increase in sales in large part because consumers cannot spend what they do not hold for this very reason. People cannot spend it back and forth without having it in the first place and because hoarders are incentivized and motivated to hoard, the economy remains at a standstill.

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



Source: Jason Kuznicki

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

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

As noted in chapter 2, this is related to game theory and even if the legal definition of bitcoin was changed from “property” to “currency” as Wilson surmised, it does not change the underlying attributes that make bitcoin a poor form of modern currency.

An inelastic economy

One consequence is that this leads to what Hungarian economist János Kornai called a shortage economy.⁵⁵⁹ While Kornai was describing the effects of central planning on consumer goods, as noted above, there is a shortage of bitcoins (credit) in the bitcoin economy. In other words, the Bitcoin economy is in a perpetual credit crunch. That growth cannot expand through lending

facilities because its user base (bitcoin holders) are collectively funneled into only one option: non-interest bearing mandatory holding accounts – or what some advocates eagerly refer to as hoarding. Businesses need financing, loans or some kind of investment in order to get off the ground and scale yet because there is no real banking system within Bitcoin, the economy recreates that of a 100% full reserve system. This is a bug.⁵⁶⁰

And consequently most entrepreneurs within the ecosystem thereby need to rely on foreign currency and capital – flexible fiat-based credit – outside the Bitcoin ecosystem, to build the Bitcoin ecosystem.

Incidentally this is not a historical anomaly: nearly all emerging countries go through similar hurdles to attract capital, opening up lines of credit denominated in foreign currencies and stockpiling foreign-exchange reserves in part to provide settlement of debt obligations with trading partners.⁵⁶¹ Yet the inability to natively create credit or lending instruments dramatically handicaps the growth and expansion of the network.

In addition to Brian Hanley's aforementioned paper, for a more thorough explanation there are several other thought provoking papers that critically examine these issues: *Hayek Money* by Ferdinando Ametrano and *Inv and Sav Wallets* by Massimo Morini.⁵⁶²

Hanley notes that, "Bitcoins, since they cannot be used in reserve banking, can only be hoarded, spent, or lost, not saved in the usual sense it is thought of in the modern world."

This is reflected in the data retrieved from the blockchain and will be explored in chapter 12.

Similarly, Morini states that:

Denominating salaries or financial payments in bitcoins would be unthinkable today: from April 15, 2011, to March 29, 2014, the USD/BTC (dollar/bitcoin) rate of exchange moved from 1 to 500. This would mean a 500 times, or 50,000%, change in the dollar value of salary. Also loans are unthinkable when prices are strongly unstable.

And David Evans predicts that:⁵⁶³

My conclusion is that it is highly improbable that public ledger coins, given the current protocols and governance systems, will evolve into general-purpose currencies. That is based on several findings. First, the protocols for supplying public ledger coins do not adjust supply with demand and therefore cannot provide stable values for the coins. Second, the theoretical explanations concerning why public ledger coins have unstable value are borne out by the empirical evidence concerning the volatility of bitcoin. Third, senders and receivers of funds will generally not adopt putative currencies that have unstable values. Moreover, senders will tend to hold rather than use putative currencies if the currencies are increasing in value. Fourth, the importance of currency stability is borne out by the fact that central banks focus on maintaining currency stability and the fact that senders and receivers avoid unstable currencies. Fifth, five years after its

inception there is no empirical evidence that would support claims that bitcoin is becoming a general-purpose currency; rather appears to be a niche currency and one that involves many transactions between speculators.

This presents a challenge: in order for Bitcoin to replace the banking and financial institutions that some of its promoters claim it will do, then it will necessarily have to provide instruments they previously created, sold and managed.

However, one adroit reddit user pointed this out several months ago regarding the possibility of banks such as UBS “absorbing the benefits” of Bitcoin:⁵⁶⁴

Look at the UBS' real focus: It was never about fees, it was about SAVINGS. UBS highlights that point over and over again. Why? Because it's a fractional reserve system and because banks have capital reserve requirements. The higher your reserves (savings), the more you can lend (mortgage bonds, corporate bonds, et cet). Those instruments are then repackaged into mezzanine debt (warrants, credit default swaps, collateralized debt obligations) and resold to investors. Bitcoin pays no interest on savings; therefore it's disruptive potential is limited to remittance and some 3rd world basket case dismediation.

There are at least five companies trying to work on solutions for lending and hedging: BTCJam, LOCKS from Coinapult, Bitreserve, Bitfinex and Bitbond.⁵⁶⁵ And nearly a dozen that are working on building platforms that could eventually provide other services that are lacking in that reddit comment: SecondMarket (BIT), CampBX, TruCoin, Coinfloor, Atlas ATS, Kraken, Coinsetter, Vaurum, itBit, ICBIT, LedgerX.⁵⁶⁶ There is even a new web-based financial firm, Delta Finance that is purportedly offering interest-bearing bitcoin accounts; and OKCoin is relaunching a P2P trading and lending service.⁵⁶⁷ And two different firms, Bitcoin Investment Trust and Winklevoss Investment Trust have submitted proposals for an exchange-traded fund (ETF) in New York by the end of 2014.⁵⁶⁸

Obviously neither Rome nor the internet were built in a day, thus, given time these instruments could potentially be built out.⁵⁶⁹

A luxury good

For perspective about using Bitcoin to perform these functions I spoke with Preston Byrne, a London-based securitization attorney and co-founder of the Eris project, the first decentralized autonomous organization (DAO):⁵⁷⁰

“A bitcoin doesn't represent an obligation - there's an open question under English law as to whether a bitcoin or part thereof is even legally capable of constituting property. Because you can't enforce a Bitcoin against anyone, it'll never serve the function of a security. You could have a security denominated in Bitcoin, certainly. But given the high degree of volatility it isn't something I'd be overeager to put on my balance sheet. Most

money takes the form of promises rather than specie; the world's more efficient that way.”

This is a legal issue that varies depending on each jurisdiction, several countries including Ecuador have banned it (preferring to use their own new national digital currency) and the European Banking Authority warns EU-member banks from buying, holding or selling bitcoins.⁵⁷¹ Conversely in the US, a few states like California have legally recognized bitcoins and on a national level agencies like the SEC has jurisdiction over their use as a security.⁵⁷² This is discussed later in chapter 17.

There may be efficient solutions to this in the future, but if history is any guide, again, the ecosystem is more reminiscent to pre-industrialized agrarian countries set on an inelastic commodity-based (gold) standard. Those with gold can absorb the purchasing power of the country – thereby increasing their own wealth – without actually creating new value or utility. This creates a feedback loop – similar to a prisoner’s dilemma – since gold owners continue to have this incentive to simply hold; why risk spending or investing when you reap the benefits of those that do take risks?

In December 2011, Kay Hamacher and Stefan Katzenbeisser, researchers from the Technische Universität Darmstadt, presented an analysis of the elasticity and inelasticity of bitcoins. They found that as market prices for bitcoin lowered, the elasticity at that time (-2.28 compared with -0.4 for major currencies) made it roughly equivalent to a money substitute but when prices went higher, it was treated like a luxury goods.⁵⁷³⁵⁷⁴ Market prices at the time of their presentation were roughly \$3 per bitcoin:

There is another funny thing, it changes the sign. So that was the average. If you do this now per month over the time here and the red dots are situations in which the elasticity is negative and the black ones are where it is positive. Then you see that's rather a mixture, that is a logarithmic scale. It is really going up down, up down all the time and changing signs. And that is funny because a positive elasticity, if you go back to the defining equation, when this is positive the demand changes or goes up when the price goes up. If gas becomes more expensive, you don't visit the gas station more frequently do you. So in the end that tells you that bitcoin, at least at the black spots, is something like a luxury good like diamonds, or gold or whatever. So people buy it -- or there is a bubble -- people buy it just for the sake because it is going up, so it's more value so I need it, so it is more psychological effect.

For balance, perhaps, one could argue that the above statements do not fully do justice to the fact that the reward does vary based on the economic situation. It is, as some argue, just that it varies in dollar terms, not in bitcoin terms.

Below is a chart representing this volatility from a presentation by David Andolfatto, Vice President at the Federal Reserve Bank of St. Louis:⁵⁷⁵

Purchasing Power of Bitcoin and USD

Nov. 2013 – Mar. 2014



Source: Bureau of Labor Statistics, Haver Analytics and Bitcoincharts.com

According to Andolfatto, this illustrates that bitcoin would and does make a poor currency due to its rapid volatility relative to other money (e.g., USD, euros) which “maintain a stable purchasing power over a short period of time.”⁵⁷⁶ There are some adopters who disagree with this statement, however the current data reinforces Andolfatto’s position (i.e., a dearth of commercial activity on the blockchain) – perhaps this could change over time, but that is not knowable *a priori* as it is an empirical scenario.

While more will be written on the topic of inflation and deflation, Bitcoin and its progeny continue to provide outside observers a chance to see deflationary systems in action. And so far the results are not much different than what economists have predicted would happen, underdevelopment.

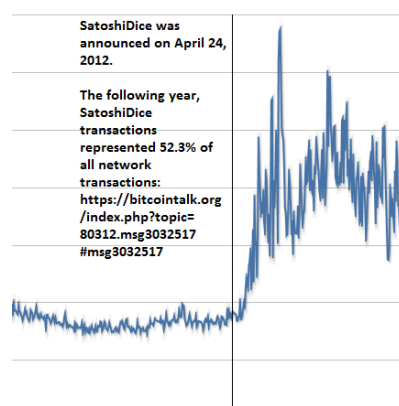
Chapter 11: Zero-sum Entrepreneurship

As noted in previous chapters, wealth is created by businesses and individuals scaling and commercializing value. The chapter below discusses the current ecosystem and how many of the zero-sum activities are not leading to the economic growth that some adopters hope that it would.

Initially announced on April 24, 2012, by the summer of 2012, fully half of the transactions on the Bitcoin network were being used to transmit bets through a start-up on-chain gambling company called Satoshi Dice.⁵⁷⁷ According to one statistical analysis by “Dooglus” and also confirmed in *A Fistful of Bitcoins*, from between its April announcement through August 28, 2013, Satoshi Dice-related transactions accounted for 52.3% of all bitcoin transactions.⁵⁷⁸ During this same time frame, transactions for Silk Road – an anonymous online marketplace which sold wares including narcotics and other banned substances exclusively with bitcoins – were estimated to make up 5-10% of the transaction volume of the Bitcoin network.⁵⁷⁹

Between February 6, 2011 and July 23, 2013 approximately 1,229,465 transactions were completed on Silk Road which generated gross sales estimated at 9,519,664 bitcoins.⁵⁸⁰ It is important to note that this is not to say every bitcoin mined was used on Silk Road, it is likely that coins spent were re-spent in Silk Road several times, generating an aggregate volume equal to this figure. According to a paper by Nicolas Christin, between February and August 2012 approximately 9% of all Bitcoin transactions took place on Silk Road and half of them originated from the United States.⁵⁸¹ Silk Road has since been closed and the alleged founder arrested by the FBI; Satoshi Dice has since been superseded by other off-chain competitors.⁵⁸²⁵⁸³

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



Source: Blockchain.info

If one builds a tool that has few immediate uses besides gambling then it should not be surprising that mostly gamblers use it. As shown in the adjacent chart, this illustrates the before and after of when Satoshi Dice came online in the spring of 2012.⁵⁸⁴ This is not to make a target of Satoshi Dice, they provided a service that apparently was quite popular with the existing user base (or perhaps on-ramped new users, or both). However, based on statistics, most people do not gamble or trade in illicit wares for a variety of reasons.⁵⁸⁵

Perhaps this is just a temporary phenomenon as the network bootstraps itself, though if history is any guide, few countries

developed and joined the OECD strictly because of this type of economic activity (e.g., if gambling actually created real growth, then Las Vegas and Macau would replace New York City and Shanghai as economic centers for growth.⁵⁸⁶ For comparison, the United States casino industry generates roughly \$125 billion in revenue a year (or roughly 1% of GDP), yet most people do not gamble.⁵⁸⁷ There may be a multitude of reasons: in the world of gambling there has to be a winner for every loser; and compounding the issue is that the house tilts the odds in its favor – or as Ambrose Bierce noted, “Lottery: A tax on people who are bad at math.”

For instance, one would not fly to Beijing and tell the political class that the reason they are stagnating is due to a lack of casinos and narcotics. In contrast, one way to measure economic growth is through total factor productivity (TFP) – measuring the increases in productivity for each input. Traditionally the way to make the same inputs (human capital) more productive is through education, training and technology. One of the ways to increase the capital productivity within Bitcoin is through merged mining, sidechains or in some manner allowing user-created assets beyond the simple ledger entry.

In response to this zero-sum description of gambling, I received a number of comments this past spring, including the following from Bob:

Gambling in and of itself does not create productivity, but the businesses that surround gambling certainly can. See: casinos, bitcoin mixing services.

Also, if the house makes a bunch of money, and the owning entrepreneur uses those funds to start another, productive business, then in some sense the gambling has facilitated economic development by liberating wealth from unproductive suckers who participate in online gambling to a highly productive entrepreneur. This was, of course, exactly the case with the most popular bitcoin gambling website.

The issue here is a measurable one. A zero-sum game is one in which wealth is merely redistributed and not grown. What Bob described above is economic activity but not economic growth. While Bitcoin may have, as its proponents note, created the fairest way to lose money via gambling, it is still a zero-sum game. Gambling is zero-sum as is speculating on options or cryptocurrencies, no new utility itself is created.⁵⁸⁸ Tokens are simply being moved from person to person (e.g., a wealth transfer or redistribution). Eventually many people are left with tokens that they cannot sell because all the demand has been fulfilled, and at that point the price may actually crash. Making money in a zero-sum game is only because others have lost an equal amount. In fact, in many cases, value diminishes because of interchange fees or in the case of mixing services, transaction fees.

For balance, if adopters spend money on gambling then in terms of growth that is not different from them spending money on restaurants or TV shows. The primary difference that matters here is between consumption and investment, not between different kinds of consumption.

Investment to sustain current capital structure and investment to innovate – not necessarily desirable consumption versus non-desirable consumption.

This touches on an economic principle of opportunity costs (the “seen” and “unseen”) — the traditional example used is Alice throwing a brick through a shop keeper’s window.⁵⁸⁹ While the seen result is a repairman being hired to fix the window, thus spurring economic activity, this does not actually create economic growth because the shop keeper must now forgo certain opportunities to spend repairing existing physical stock.

A more concise explanation of this phenomenon can be found in *Gambling and speculation*, by Borna & Lowry:⁵⁹⁰

For players, gambling, at best, is a zero-sum game, i.e., the aggregate wealth of the players will not be altered due to a gambling activity. The losses of one party are precisely equal to the gains of the other participants. Of course, if the gambling activity were taxed by the government, or there were other ‘leakages,’ then the expected value of winning would be negative, i.e., the aggregate wealth of the players after the play would not be equal to their original wealth.

Although gambling is a sterile transfer of money or goods among individuals creating no new money or goods, it nevertheless consumes the players’ time and resources and may subtract from the national income. From a macro-economic point of view, the aggregate wealth of the players will change, in the long run, due to the fact that the transfer of wealth is usually among unequal productive sources. It may be argued that the productivity lost due to a transfer of money from one player will be offset by an increase in the productivity of the other player. This assumption is true only if both the winners’ and losers’ production schedules were assumed to be identical and linear.

Trading bitcoins would be similar to trading options, there can only be one winner and no additional value from the trade is created. However in theory, speculation may add value in two ways. First, producers (e.g., farmers) can insure against price changes by taking the opposite side of a trade with a speculator. This makes it possible for them to engage in production that would otherwise be too risky. Second, certain speculators (e.g., in the stock market) provide liquidity.⁵⁹¹ This makes it easier for investors in fixed assets to raise money because people are more willing to buy shares that can be easily liquidated.

Speculators in foreign currencies similarly add value by making it possible for manufacturers to hedge against exchange rate risk. If there were bitcoin futures and options, bitcoin speculators could conceivably play a similar role though this may be challenging in the face of BitLicenses. Similarly, this may not solve the problems above because hedging is not costless and participants will probably prefer transacting with a stable fiat currency to using bitcoin and paying to hedge it.

Anything that has to deal with trading contracts such as options or other derivatives is a zero-sum game. This in effect means that one person's gain is by definition the other person's loss (the person that signed the opposite side to the contract). When Bob is buying shares of a company or purchasing company debt, he is contributing to something that in general has a positive value to the economy. For example investing in Apple equity (assuming a secondary offering, because if Bob buy's shares from the market he is practically taking up another investor's position), or buying Apple debt, Bob is allowing Apple to build their supply chain, invest in research and development and so forth. This provides positive value for the economy because the money is invested. His "counterparty" in that case is Apple. Bob's gain is not their loss but rather a chance for them to reinvest in their business.⁵⁹²

Conversely he can of course have a negative value (or rather invest in a negative value creation) if he gave the money to say a company such as RIM (makers of Blackberry). Furthermore, buying options is not really an investment, they do make financial markets more stable, and allow investors to hedge (effectively move risk) to other investors that are more willing to undertake that specific risk. Bob is effectively taking a position against another investor that has a different viewpoint or risk tolerance. Together though, other than providing risk allocation benefits, they are a zero-sum product by definition. His gain comes directly from that other investor.

Building a mass consumer economy

As described above, speculation in certain securities can also be zero-sum and in some cases a negative-sum game. In his most recent book, *Flash Boys*, among an assortment of issues, Michael Lewis described the *reductio ad absurdum* of this in action: high frequency trading (HFT).⁵⁹³ There is nothing inherently malignant with HFT in fact, liquidity may increase; yet no additional utility is created purely by day trading certain securities (this is also due in part to exchange commissions).

One common refrain by a vocal segment of the Bitcoin community is that "investing" in alts is a zero-sum game, that no new wealth is being created since that money does not go to improving the "company" (network) itself – again, for every winner there has to be a loser. Yet there is a similar issue with bitcoin in that while speculation has drawn in new crowds which often create new demand, those funds are not being lent out as they would in a normal modern economy. That is to say, there are few ways to save bitcoin and lend them out (Bitreserve, BTCJam and Bitfinex are notable examples), you can only hoard them.

This is a vexing issue that Morini Massimo notes in his concluding remarks:⁵⁹⁴

In this work we have provided a solution for a cryptocurrency where both prices and accounts are stable. This is crucial for a cryptocurrency to grow, not only because instability implies a risk of losses that discourages many users. Instability can be a crucial curse for a cryptocurrency even if, like in the case of bitcoins, it has so far led mainly to gains for wallet owners. In fact, for bitcoins to grow in economic relevance, people need

to spend bitcoins for transactions, increasing transaction volumes. But if people anticipate a growth in transaction volumes, they know that, due to non-flexible money supply, there will also be a growth in the value of their wallets. This creates an incentive not to spend bitcoins in transactions but to hoard them as a form of speculation. Thus bitcoins will not grow in economic relevance, but at the same time they will stop grow also in terms of value. Even proposals like Hayek money to transform the growth of bitcoin rate of exchange into a proportional growth of wallet amount for everyone remain a distorted incentive to hoarding.

Because of this known characteristic, some advocates claim that such hoarding actually creates reserve demand for the token. That could be the case if it was a currency or even a real share of equity, but it is not (it is probably a money-like information commodity). Holding a bitcoin is not like holding equity in Bitcoin. Bitcoin (the network) is not a company. With a publicly traded company like Google, shareholders receive a portion of equity (or rather a securitized future stream of revenue) in exchange for providing Google capital today. Google can then reinvest that into operational activity such as funding internal projects to create more utility (through research and development, training, etc.). The way Bitcoin is set up today, that is not possible. For instance, mining pools technically have a built-in incentive to finance developers, but in practice do not (Eligius does not pay Luke-Jr as an employee).⁵⁹⁵

In his paper, Brian Hanley, takes this one step further and argues that a Bitcoin financial system is a losing zero-sum game for investors:⁵⁹⁶

A system where the amount of money is fixed is a zero - sum game – for every winner, there must be a loser, because new money is not created that allows interest or investment return payouts. Bitcoin is designed to be a zero - sum game, and long before bitcoin creation is formally set to zero, the accidental loss of bitcoin wallets will match or surpass the creation rate. It is quite possible that this point has already been passed, but there is no way to monitor it because most bitcoins are hoarded, not used in commerce, and due to the distributed design, there is no visible difference between a hoarded bitcoin and a bitcoin that has been lost forever. Consequently, bitcoin is worse than a zero - sum game. It is a pulse game in which the bitcoin resource is injected and then slowly drawn down.

In terms of gambling, while the legal and ethical reasons could be debated, that is the topic for a different analysis and venue. In practice, if illicit activities were real economic engines instead of mere channels for entertainment, then as noted above, gambling centers would be the economic pillars of society. If Bob wants people (customers) who are non-gamblers or patrons of licit-trade, then Bob needs to build tools for them beyond merchant services. Thus, instead of building “dark markets” for illicit trade, one could build and market tools for sustainable economic activity.

Impacting the bottom line

In its forthcoming August 2014 industry report, Pathfinder Capital noted that:⁵⁹⁷

The performance of publicly listed Bitcoin-related companies has been devastating. It appears as if penny stocks on regulated exchanges have used Bitcoin as nothing but a marketing tool to give a last boost to their ailing stock price. Overall, the performance of companies at Havelock Investments hasn't been much better. As we have seen, only a few companies had a positive return let alone outperformed bitcoin. Moreover, large scandals like Neo&Bee are to be expected. Nevertheless, some of the business models presented are definitely interesting. Investing at Havelock Investments therefore constitutes an opportunity for the risk-tolerant investor with deep sub-industry knowledge of the Bitcoin ecosystem. Investment has to be long-term as liquidity is low.

Havelock Investments, a Bitcoin-denominated stock platform, is owned by the Panama Fund, a private investment company based in Panama. Neo & Bee was a Cyprus-based exchange whose founder, Danny Brewster, absconded with several hundred bitcoins in early April 2014 before the exchange ever opened its doors to the public.⁵⁹⁸ Havelock was an investor in Neo & Bee and ever since this event, according to Pathfinder none of the listed companies on Havelock's platform have generated a positive return in bitcoin.

Pathfinder also highlighted Overstock.com as one ecommerce site whose announcement for accepting bitcoin payments on January 9, 2014, did not have a long lasting effect on its stock price. In fact, Overstock's stock price has declined approximately 51% over the past year (July 2013 – July 2014), including a 32% drop less than three weeks after it announced it was accepting bitcoin.



Source: Yahoo! Finance (OSTK)

Overstock's main clients are women (60%) and globally, the demographics for ecommerce customers tilt towards women.⁵⁹⁹ Based on a number of reports, surveys, events, meetups and anecdotal evidence: women are a small minority of bitcoin holders.⁶⁰⁰ Furthermore, Overstock

as an ecommerce site and its vendors have no incentive to take bitcoin as it adds more tax costs and liabilities – they are not a FOREX or commodity trading firm. For this bitcoin plan to work, Overstock's customers will need to change its demographic makeup. Yet between January and May 2014, Overstock received only \$1.6 million in bitcoin sales, a million of which was in the first two months.⁶⁰¹

Consequently, accepting bitcoin has not helped its bottom line in part because the merchandise on Overstock is not catered to those who own bitcoin. In fact, in his May 2014 reddit ask-me-anything, Byrne was asked the question, “What percentage of transactions (# or revenue) are paid for in Bitcoin on Overstock.com?” He responded, “Tiny. <.1%”⁶⁰² In a follow-up interview in July 2014 Byrne said that, “I think since we announced it, it is a quarter of 1% of sales is the last calculation I saw.”⁶⁰³

Why did Overstock's stock price decline when it announced its Q4 earnings report on January 30, 2014? As one reddit user noted:

Though Overstock (OSTK -19.9%) officially reported Q4 net income of \$73.6M (good for EPS of \$3.01/share), that figure was inflated by a \$72.6M income tax benefit stemming from a \$79.7M deferred tax asset valuation release. If not for the tax benefit, Overstock would've had Q4 net income of \$1M, down from a year-ago level of \$8.8M. EPS would've come in at \$0.04, well below a \$0.52 consensus. Though its sales rose 16% Y/Y to \$297.6M and slightly beat consensus, Overstock's gross margin only rose 10 bps to 18%. Meanwhile, sales/marketing spend rose 52% to \$31.2M, and G&A/technology spend rose 19% to \$39M. Overstock says Google algorithm changes implemented in Q3 hurt the company's ranking "in certain Google search results during some periods." As a result, Overstock turned to other channels such as search ads, which contributed to a surge in marketing spend.⁶⁰⁴

It is unclear in the timing what the motivation for Patrick Byrne, the CEO of Overstock, was for announcing the acceptance of bitcoin and integration with Coinbase, but what is clear is that accepting bitcoin for payments has not helped its net income in part, because in general, few people actually spend bitcoins and because Overstock's merchandise caters towards women. And again, women as a whole represent a minority of bitcoin ownership. This may change in the future but it may not be enough to improve the revenue flow for most retailers.

Actual numbers

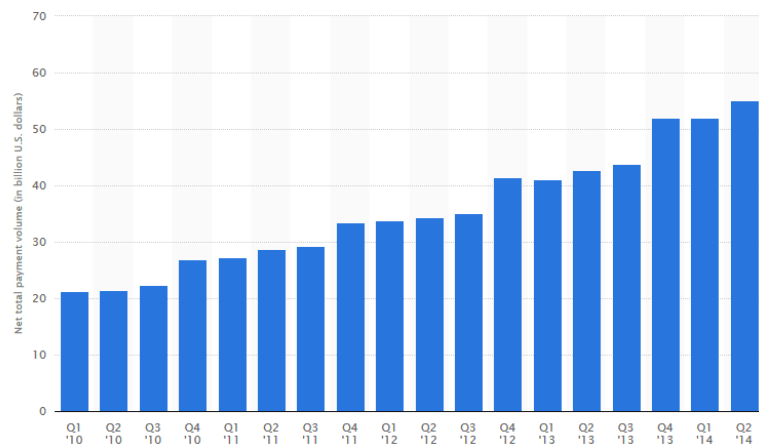
Because of its deflationary nature in the long-run and volatile behavior in the short-run, Bitcoin is not poised to overtake PayPal. In May 2014 an article was published claiming Bitcoin had surpassed Western Union in volume and consequently was republished and cited on numerous sites.⁶⁰⁵ The data it used is cherry-picked. It used the first week of December 2013 as shown on Coinometrics, the week in which transactional volume was at an all-time record high, to suggest that the “\$300 million” in volume would overtake PayPal's.

The problem is the volume has fallen to a fraction of that (to roughly 10% of that) and even that number is incorrect because it does not account for mining payments, mixing, gambling and illicit activities. In fact, Coinometrics has a warning on its site that transaction volume on Bitcoin is not qualitatively the same as other payment networks. As noted later in chapter 14, on any given day Bitcoin may only process \$5 million in actual commerce, or \$1.8 billion a year. Though it is unclear how much off-chain or colored coin value is being transferred, so this may be understated.

In contrast, PayPal currently handles approximately \$200 billion in transactions annually.⁶⁰⁶

While PayPal likely processes illicit activities, what adopters should want to promote and recognize is actual real commerce and not just entertainment. That's how the average mother and father join networks, because it provides a solution to a real need. So something like services from Realty Shares, GBI, Digital Tangible Trust, Proof of Existence, OriginStamp, cloud, compute and storage from Bitcloud, StorJ and Filecoin, payments to merchants selling food and office supplies.⁶⁰⁷

PayPal's total payment volume from 1st quarter 2010 to 2nd quarter 2014 (in billion U.S. dollars)



Source: Statista.com

However because of the pseudonymous nature of the blockchain, even with a full traffic analysis, a graph of all the known public addresses would not fully tell us how much actual economic growth is taking place.

With that said, in May 2014, three researchers at the University of Luxembourg published a paper, *Deanonymisation of clients in Bitcoin P2P network* explaining a method for deanonymizing this type of information.⁶⁰⁸ Thus, while there is potential for such a traffic analysis there are no known public reports on this yet.

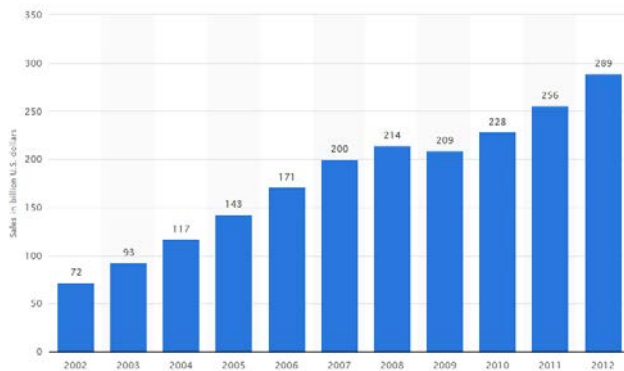
I asked Jonathan Levin, co-founder of Coinometrics, an analytics start-up, about this specific data and according to him:

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

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

Just the first inning?

Annual B2C e-commerce sales in the United States from 2002 to 2012 (in billion U.S. dollars)



Source: Statista.com

This lack of spending or positive-sum activity is not to say that Bitcoin is imminently doomed or will fail – and again – there are known solutions to nearly all of the technical challenges above.

Furthermore its dedicated community will keep it going for many years to come.

In addition, even though it has been a five and a half years since the genesis block it does not mean that the ecosystem has been fully rolling that long. Significant angel and

VC investments first started in earnest just over a year ago. At the time of this writing, \$252 million has collectively been invested in the ecosystem since 2012.⁶⁰⁹ And deals this year are expected to be even larger than all previous years combined with a potential for \$300 million expected by the end of the year.⁶¹⁰ It also took a while for internet startups to become useful. For instance, ecommerce in the US did not catch on until after 2000 and similarly has been going gangbusters in China where it is expected to reach \$300 billion this year.⁶¹¹

Perhaps what is happening are baby steps, not in the developed world but in the developing through services such as BitPesa, BitPagos, Maicoins, Coins.ph, ZipZap, Coincove and 37Coins.⁶¹² This is where immediate user value could lie for trustless bilateral exchange. Yet even the high expectations and potential within the overseas remittance markets should be tempered with the compliance realities and social engineering challenges that need to be overcome for these cross-border channels.⁶¹³⁶¹⁴ However, even if the infrastructure is available, it does not mean adoption.

I spoke with James Duchenne, an attorney who grew up in Mauritius and co-founder of Satoshi Legal, according to him:

Anyone that's lived in or been to Africa can attest to the enormous cultural differences that exist. Thus, to me, the #1 barrier to entry for bitcoin type adoption in Africa is not infrastructure, it is culture & trust. The average African has a culture of "need" and not "want" - the "need" is controlled by those in power and a tacit toleration of corruption is prevalent. Thus, people trust tangible things or things trusted by "trusted people."

Anything complex has a very hard time to get off the ground in a grass roots movement unless those in power (the trusted governors) have something to gain from it.⁶¹⁵

Thus those specific use-cases are mostly likely not relevant in San Francisco, New York, London or other high developed regions with existing effective rails. Simultaneously it may not be fair to expect people starting to use Bitcoin *en masse* before the exchanges, wallets and other basic infrastructure is working properly and is sufficiently easy to use. Mobile is the platform of the future and secure storage is still an issue.

However quick, seamless mobile banking is already a reality in some places including notably China with Tenpay and Alipay and Western companies like Google and Apple are rolling out their own mobile payments platforms.⁶¹⁶

For instance, according to *Business Insider*, between October 2009 - April 2014, the number of iTunes accounts grew by a factor of 8.⁶¹⁷ During the same time frame, accounts used to make or receive payments on Amazon and PayPal doubled. These numbers and trends will probably change but it shows the competitive force that technology firms are providing in the payments space; they will certainly not sit idle in the face of purported challengers.

Therefore maybe future research should start to look at activities more closely in other parts of the developing world. Who else is building Bitcoin ecosystems in those places? 55% of West Africans live on less than \$1 a day.⁶¹⁸ Could these firms create a competitive payments platform in regions where residents make less money than the transaction fees of Bitcoin?

In August 2014, Jason Tyra explored this dilemma of whether not Bitcoin can deliver the promises to the unbanked:⁶¹⁹

However, for those that potentially stand to gain the most from the digital currency – impoverished and unbanked people living in developing regions of the world – bitcoin remains largely inaccessible.

[...]

So, right now, if you have no way to get online, then you have very limited ways to send or receive bitcoin. And, if you don't have a bank account, then bitcoin is unlikely to be an effective solution to your problem, since bitcoin itself requires a bank account for most users to transact business effectively over long periods of time.

For all of their positive features, cryptocurrencies are mostly inaccessible to the developing world for now. Changing this will require bitcoiners to develop robust and realistic solutions that will put it into the hands of the people who need it most.

Tyra's analysis echoes James Duchenne's observation: that without modernized infrastructure and institutions, bitcoins will remain inaccessible to the use-case that many proponents continually extol.

Perhaps the “killer” products and services are gaining traction in the places least expected and are already serving real use cases but they are just still small and invisible to us. Email did not become popular with mass appeal until Hotmail, Gmail and Yahoo made it easy to use even though the protocols and clients (e.g., SMTP, Eudora) were already in place. And maybe there is ways to experiment with funding initiatives, for instance MultiBit wallet will start to charge users 1000 satoshis (~\$0.05) for every transaction.⁶²⁰ Perhaps this will become a modified SaaS model for open source software. Every time Bob uses software for X minutes Bob will pay Y cents to the developers. Pay as you go.

Lastly, entertainment is easy to start with when the basic business model and infrastructure is still pending. Historically, there is precedence with black market activities like gambling as a boot-strap app, that is also how Youku got popular.⁶²¹ Instead, more patience could be required as commentators could be overestimating in the short run and underestimating in the long run.

A diamond in the rough

There may also be potential for the underlying tool (the blockchain) to be used for NGOs, for administrations in developing countries and in dozens of other areas.⁶²² The Startup Cities Institute has created Munibit for this specific purpose yet incentivizing boots on the ground, convincing armchair market experts on Reddit to get on an airplane and fly to where the underbanked live, is an uphill task, yet stranger things have happened.⁶²³

Or maybe there is no “killer app” to be found; perhaps in retrospect it is the protocol itself which allows businesses to remove redundant administrative overhead or maybe it is just the rails that organizations end up gravitating towards (though Ripple and proof-of-stake are competitive options on this front as well). Similarly there may be benefits that the token provides as a store of value for high net worth individuals (HNWIs), institutions, enterprises and governments. Building a business around a product based on how the consumer *actually* behaves today versus how you *want* the consumer to behave will likely save a lot of headaches in the future.

This may be why BitPay may ultimately moves towards API and tech solutions such as Copay and multisig and maybe why BitGo was recently able to attract a highly experienced product manager – enterprises and institutions may be interested in the store of value aspect and they have a lot more capital than sock puppets and gamblers.⁶²⁴⁶²⁵⁶²⁶

However, one thing to keep in mind is that if all the Bitcoin products and services are running off a SaaS platform or exclusively from one API, then these underlying services become a *de facto* point of centralization. If Bob does not run his own full node, how do he know an entity like Chain.com is showing him the real blockchain?⁶²⁷

Readers that are interested in creating a start-up in this space to on-ramp utility, innovation and ease-of-use to the network there are several incubators and accelerators to help out:⁶²⁸

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

In summation, economies grow through value creation, value creation requires credit. Credit comes from lending and lending comes from banks through savings. But users cannot “save” a bitcoin on the network, there is no mechanism to do that without moving off-chain. Users can only spend or hoard. And consequently, most activity within the blockchain revolves around zero-sum games that provide no real growth. What is missing from the current protocol is a fractional reserve system to facilitate dynamic money supply adjustment as a pathway toward heightened transactional volume – meaning, by tautology, less hoarding and consequently less volatility as price discovery becomes “cheaper” when bid-ask spreads converge. Thus, can someone actually create Bitcoin’s hockey stick growth?

The next chapter will look at the movement of coins over time and the challenges in securing these same coins.

Chapter 12: Token movements and token safety

Estimating the success of any technology platform necessarily requires understanding the quality and amount of market share – or in the case of new technologies, the size and activity of user base such a platform may have. As noted in chapter 4, it is presently unclear exactly how many are active users of the Bitcoin network and complementary services, rather than total number of users who have ever interacted with the platform. Studies estimating the conversion rate (CVR) to this new platform based on currently available metrics are publicly unavailable or simply do not exist.

As noted throughout the book, network data points to relatively low flat adoption rates. In this chapter I look at finding plausible reasons for low-usage rates among ordinary consumers including the cost of securing information which is discussed as a possible impediment to wider adoption.

While the Bitcoin community is a very vocal, energetic group, despite immense global media coverage and \$1-3 billion spent on funding infrastructure and services, it is arguable that it's CVR – a ratio of the number of users of Bitcoin per dollar invested or per minute of media attention – is still relatively small.⁶²⁹ Part of it is a user-design (UX) and on-ramping (education) adjustments, some of which will likely be ironed out as the space matures, yet there are other factors at play.

Measuring the impact of media appearances for any platform is historically difficult: both John Wanamaker and William Lever, pioneers of modern advertising, purportedly stated a century ago that “half the money I spend on advertising is wasted; the trouble is I don't know which half.”⁶³⁰ Tracking which demographic segments are exposed to and adopting cryptocurrencies will likely become an increasingly germane research topic in the coming years especially for start-ups looking to build beyond niches.⁶³¹

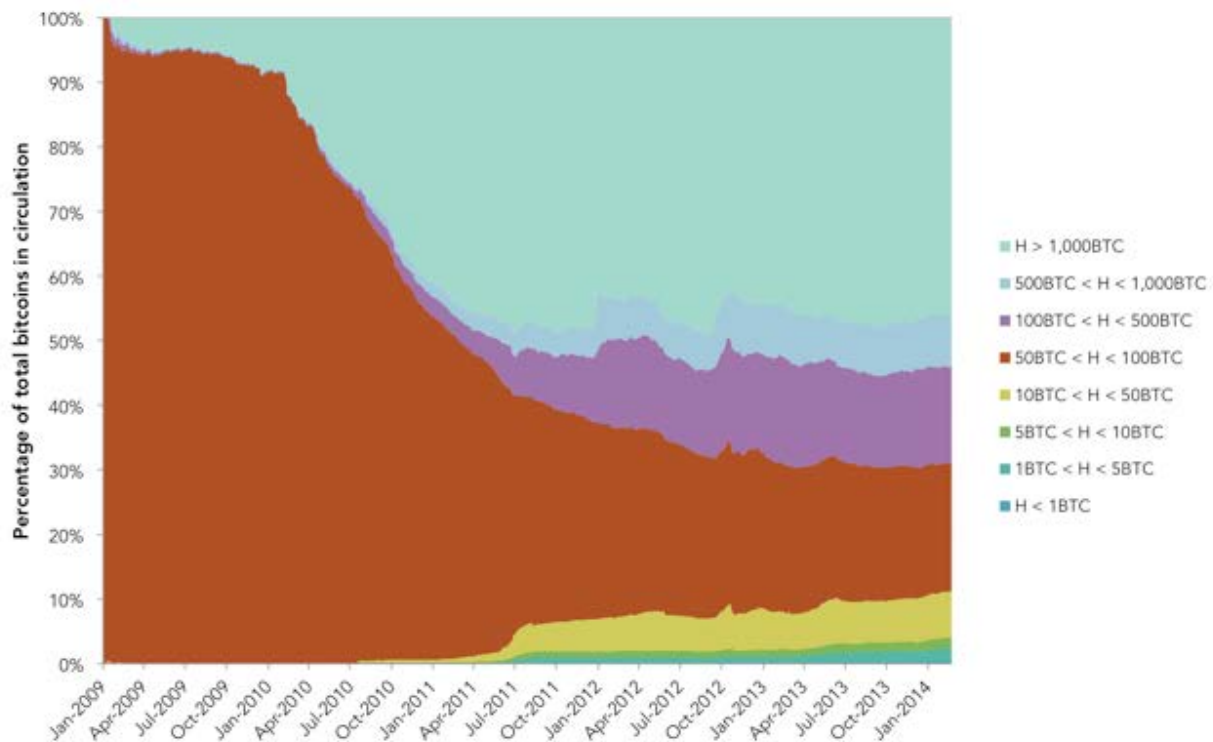
For instance, instead of asking how big the Bitcoin user base is, a more accurate question is, how small? And why is it small?

Perhaps, as noted in chapter 4, wallet usability may hold the key.

For instance, even though wallet creation is not the same as user adoption, by April 2014 there were over 1 million wallets on Coinbase and likely as many on other hosted wallet services; these however, are centralized off-chain solutions.⁶³² Still, these edge services provide a valuable service (e.g., microtransactions, near-instant trades) that apparently market participants are willing to use relative to on-chain solutions as shown by the fact that Coinbase opened 1 million wallets in roughly 14 months, a rate roughly on par with another, Blockchain.info (which dubiously claims to be “on-chain” though the blockchain is not structured to host wallets) which did it in 17 months.⁶³³⁶³⁴ Yet as explored in chapter 4, wallet creation is not equivalent to user adoption.

However, the utility and ease of use offered by reputable off-chain providers may constitute one large component for the rise in bitcoin usage from 2009-2014 and therefore account for the market demand as well. What does this look like?

Visualizing UTXO patterns on the blockchain



Source: Jonathan Levin, *Coinometrics*

The chart above, compiled by Jonathan Levin illustrates the consolidation of bitcoins over time. In his words:⁶³⁵

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

This finding correlates with mining estimates from 'rutkdn' who analyzed the blockchain and found that 1,919,950 bitcoins are stagnant on 38,399 addresses mined between 2009-2010.⁶³⁶ Based on research from Sergio Lerner, roughly half of these are speculated to belong to Satoshi Nakamoto, the creator of Bitcoin, and the other half belong to miners who over the years:⁶³⁷

- Hard drive broke and was returned-to-manufacture but forgot to backup wallet
- Mined as a hobby on old equipment, hard drive now long forgotten and/or reformatted

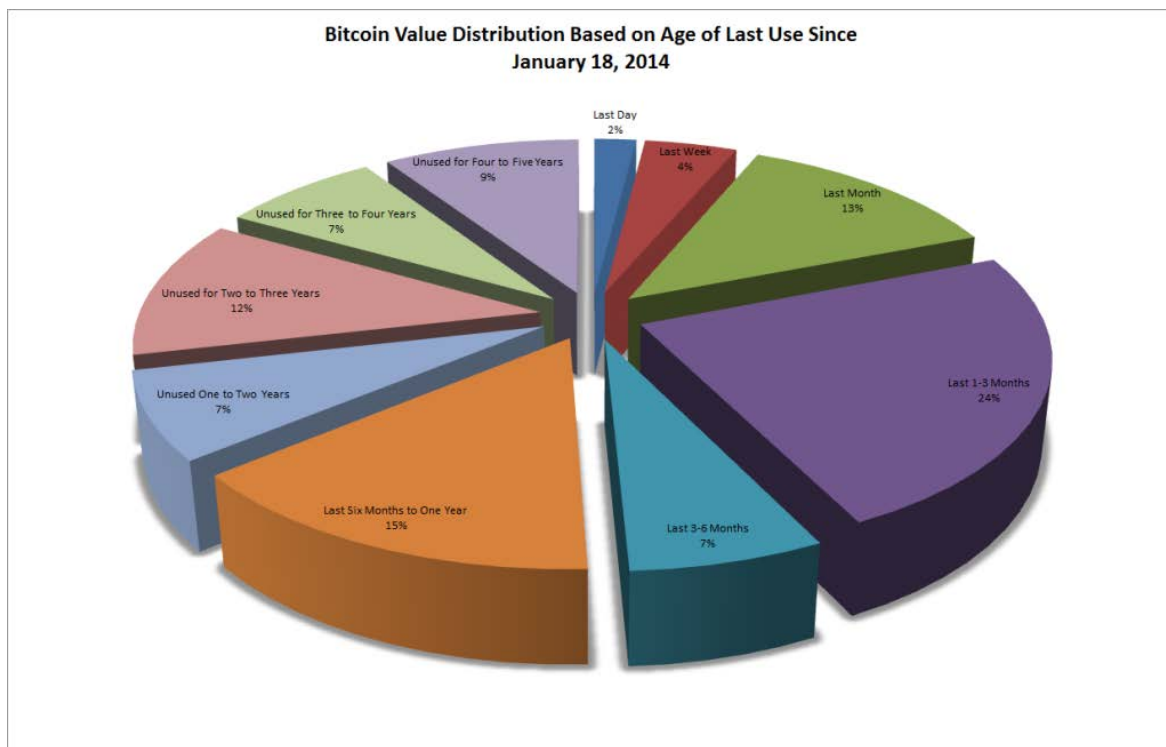
- Sent dozens even hundreds of bitcoins to test it out with other hobbyists, then deleting them because they were “worthless” at the time

Altogether this represents 14.72% of all mined bitcoins as of July 20, 2014.

This is further visualized in three charts from John Ratcliff (below) which illustrates that as of June 2014, more than half of all bitcoins mined have not been moved in over 6 months and 27% of the total have not been active in more than 18 months.⁶³⁸⁶³⁹

The pie charts below show UTXOs (unspent transaction outputs), better known as bitcoins and their distribution by age. That is to say the amount of bitcoins based on their last use.

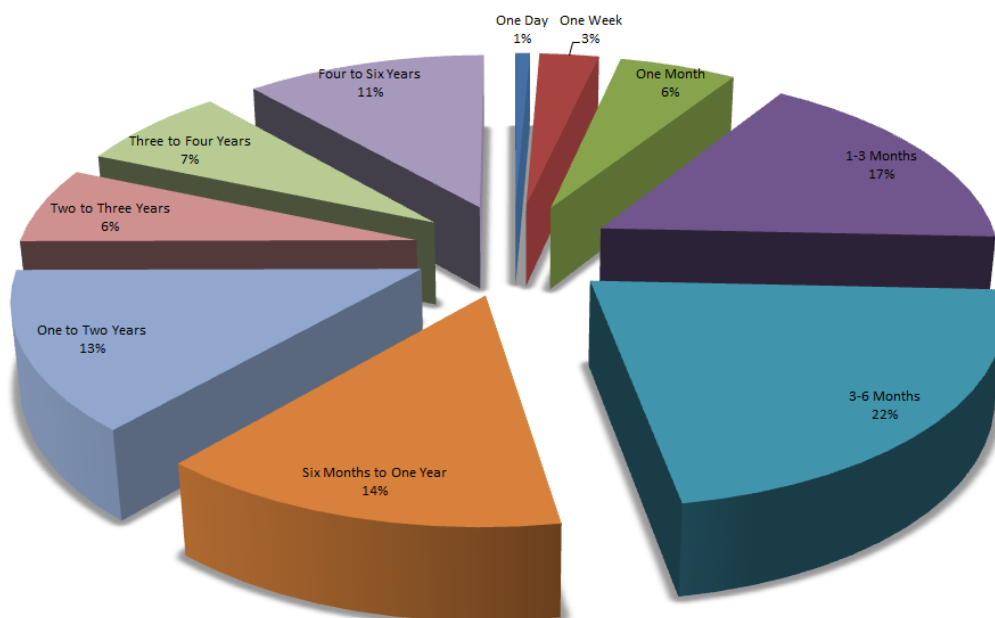
As of January 18, 2014:⁶⁴⁰



Source: John Ratcliff

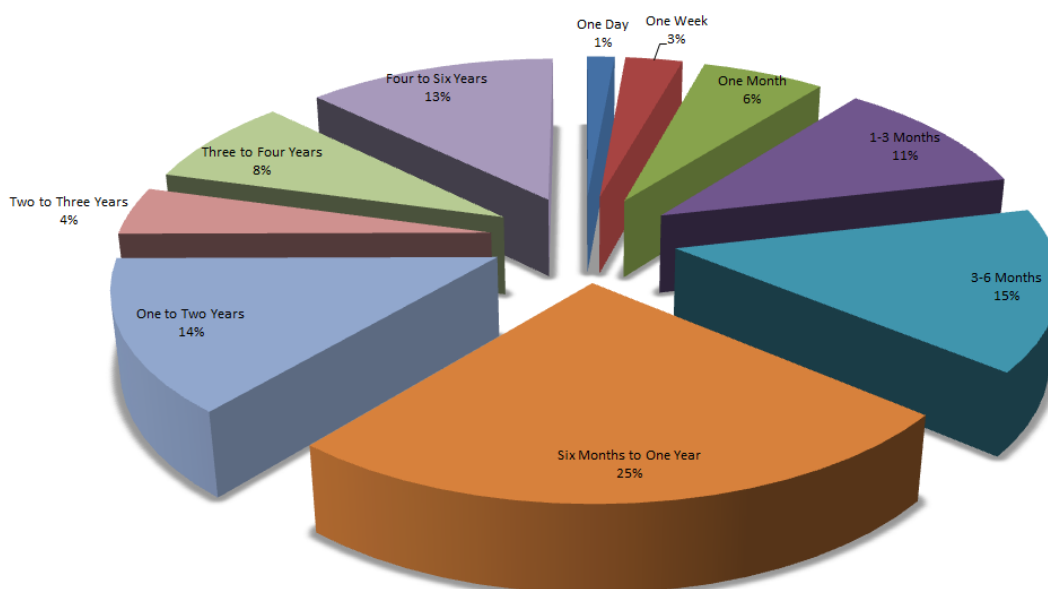
As of May 16, 2014:

**Bitcoin Value Distribution Based on Age of Last Use Since
May 16, 2014**



As of July 27, 2014:⁶⁴¹

**Bitcoin Value Distribution By Age of Last Use
Current as of July 27, 2014**

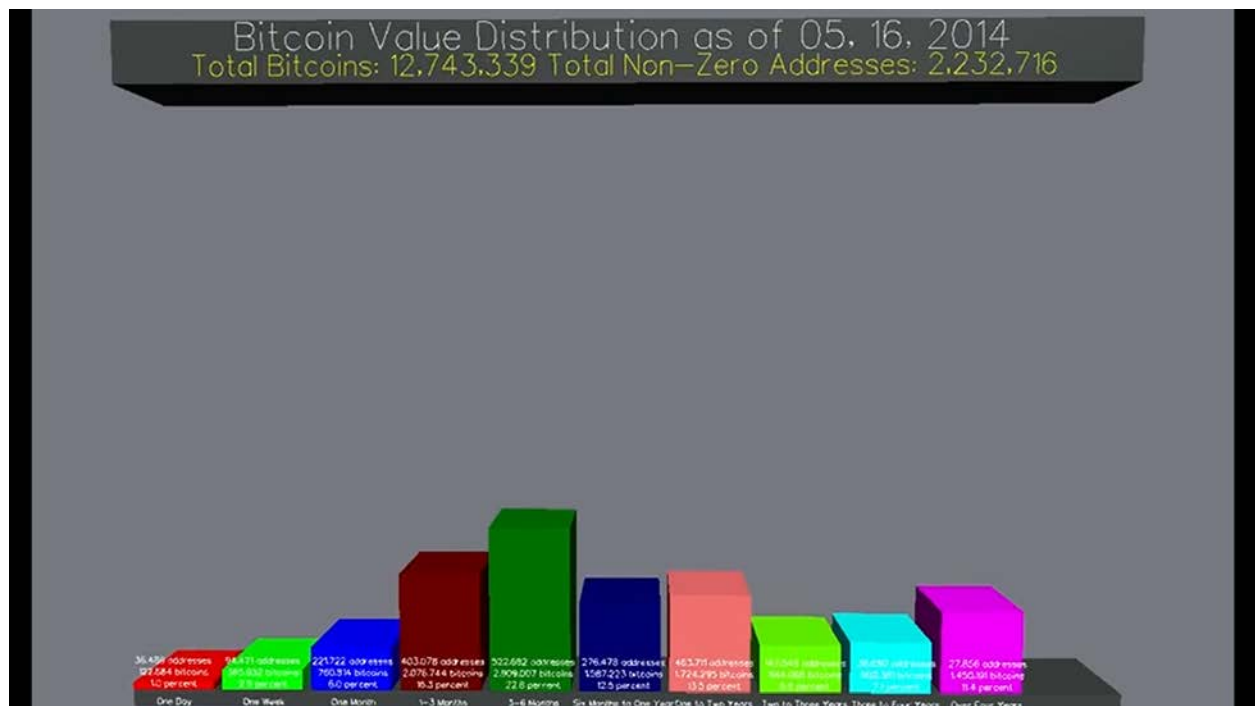


A notable area of growth is the 3-6 month section and the 6-12 month section. While there could be a variety of reasons for why this is now the largest segment (e.g., lost, stolen tokens, Goxcoins), the timing coincides with the late November 2013, early December 2014 bubble that peaked at \$1,100 per bitcoin – it has since fallen to roughly \$625. These holders could and likely did buy during the peak and are simply underwater. If that is the case, rather than cashing out and realizing a loss, they are holding them and waiting (with the hope) that there will be a rally in prices once more.

There is also a notable fluctuation between the number of tokens that have not moved in 2 years or more. In January 2014 the total accounted for 28%, in May that same portion represented 24% and in July this segment was 25%. While it is unclear where they went to (e.g., to new wallets, purchases of Golden State Warrior tickets) it does show that not all older tokens are abandoned.

Some readers may be thinking that three data points are not enough to draw a conclusion. For instance, what does the blockchain distribution look like since the genesis block?

The following is a still-shot from an animation created by John Ratcliff of the daily changes in distribution based on age starting from the genesis block on January 3, 2009 to May 16, 2014 that can be found in the footnotes.⁶⁴²



Source: John Ratcliff

At the beginning of January 2014, the 3-6 months segment represented only 6.8% of all tokens. Now it represents more than 3 million UTXOs in part because people probably do not want to unload because of the ongoing bear market.

However, the activity that is generally associated to commerce happens solely on the left side of the bar graph, in the period of a week or less, representing roughly 10% of all mined bitcoins. Yet as far as how much is related to day traders, gambling sites (e.g., Satoshi Dice, Prime Dice), remittances or other activity cannot be determined by this method.

In May 2014 Ratcliff explained that, “we know what and where the liquid bitcoins are. And what is interesting about the graph is that it shows the difference in liquidity at different time periods.”⁶⁴³

Yet he cautioned that you cannot definitively jump to conclusions from this chart alone. For instance, if Bob moves 100,000 bitcoins, outside observers do not know what Bob was doing (moving a wallet like Bitstamp did in November, conducting real commerce, betting).⁶⁴⁴ In Ratcliff’s view, his approach has one key distinction, if Bob has a bitcoin address and they spend one bitcoin (UTXO), observers will view that event as if Bob moved just one bitcoin – Ratcliff is marking age as age of last transaction. This then proves that Bob still controls this address (an address which represents inputs and outputs) -- this address is not dead which is a subtle distinction.

To him, what you can see is X% of bitcoins that are liquid (moving on a weekly basis), X% that are being “saved” and X% (or in this case, 30%) which may be gone forever. It is unclear if someone such as Satoshi Nakamoto (who is alleged to control approximately 1 million bitcoins) still controls the keys or what is he going to do with the keys creating market uncertainty.⁶⁴⁵

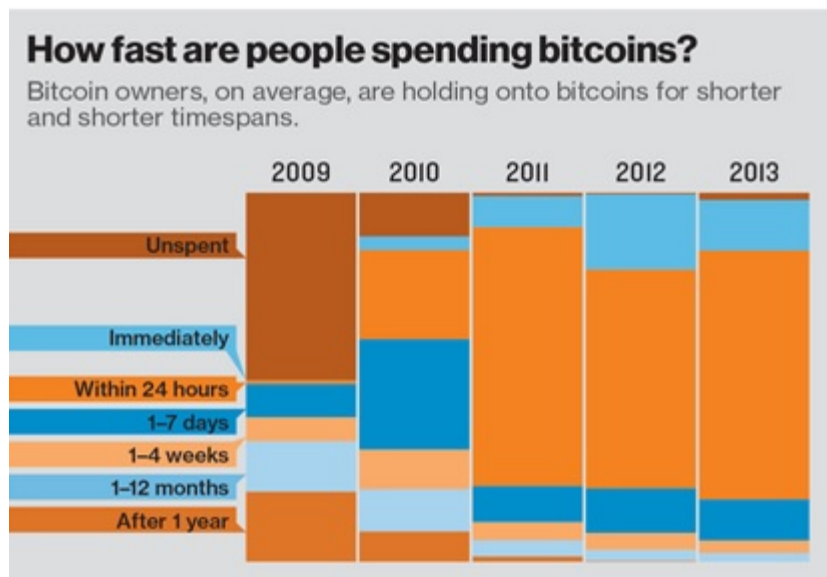
For additional analysis, according to Jonathan Levin, co-founder of Coinometrics:⁶⁴⁶

The underwater explanation for the 3-6 month period is plausible but the problem with the method is that this measure is highly susceptible to changes in the exchanges and so inferring behaviour of individuals is difficult. If Bitstamp has not done another reshuffle since the one last year that would probably show up in the 3-6month section.

I am interested in the 1 month and 1 week decreases as well. It seems that less Bitcoin’s are being moved around the blockchain now rather than in January. We have also seen volumes on the exchanges drop since December levels which may explain some of this drop.

Other ways to measure movement

Below is another picture that purportedly measures the spending and movement of bitcoins:



Source: MIT Technology Review, Sarah Meiklejohn

The source is a *Technology Review* infographic yet the data source comes from the paper, *A Fistful of Bitcoins*, from Meiklejohn *et al.*⁶⁴⁷

According to her the data in question comes from Figure 3 in the same paper.

However, the likely explanation to the infographic is that many miners typically must sell off their bitcoins to cover their operating costs which makes it difficult to isolate actual commerce from mining

activity (though there are some notable exceptions).⁶⁴⁸

The graphic could simply visualize the competitiveness and professionalization of the industry. Virtually all miners have to spend their tokens within a month of mining them. This is not real economic activity for the ecosystem as nearly all of those funds are converted to a foreign exchange (fiat currency) and then paid to a utility or hardware company, this does not improve the protocol, usability or on-rampability (sic).

What do other qualified people have to say about it? I reached out to Jonathan Levin, co-founder of Coinometrics and a post-graduate student at Oxford. His explanation is thus:⁶⁴⁹

- Looking at some of the mining pools there are plenty of transactions that are used just to pay miners and also to conceal identities.

- There are also transactions used by exchanges and other large corporations every day for internal settlement and security. Every transaction that gets done through BitPay and the like will inevitably trigger multiple transactions for privacy protections and security
- Private individuals also move coins between wallets to ensure privacy and security of funds

His conclusion is that, "A lot of this creates price insensitive demand for transactions as it is not strictly economic activity."

This is the Kevin Costner problem: if you build it, will they come? So far the answer has been a muted no. Perhaps this will change as security and usability improves and more merchants and users adopt the technology yet as seen in chapter 3 energy centralization could become a factor.

Consolidation of coins

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

- February 6, 2010, Bitcoin Market opens becoming the first exchange which coincides with the beginning of consolidation
- July 18, 2010, Mt. Gox opens, ultimately reaching 80% of exchange marketshare at its peak two years later⁶⁵⁰
- July 18, 2010, the first GPU hash farm (run by ArtForz called the "AntFarm") finds its first block and later purportedly reaches 25% of network hashrate at its peak for several months⁶⁵¹
- December 16, 2010, the first mining pool, Slush's pool finds its first block and reportedly reaches 10,000 Mhash/s the following month (~8% of global hashrate) by January 8, 2011
- July 2011 – December 2013, the ZeroAccess botnet spreads to between 1 – 2.2 million systems. During one phase reported in September 2012, the botnets theoretical collective hashing power reached 2,480 gigahash/s generating up to 1,022 bitcoins per day (~14% of global hashrate)⁶⁵²
- January 30, 2013, Jeff Garzik received the first ASIC manufactured by Avalon which performed at 68,252.65 Mhash/s (earning up to 11 bitcoins per day)⁶⁵³⁶⁵⁴
 - Note: for comparison a contemporary quadcore desktop CPU from Intel reaches approximately 10-11 MHash/s

Increased hashing asymmetries have substantially raised the barriers to profitably enter this segment leading to potential centralization concerns.⁶⁵⁵ Initially mining was a common gateway into the cryptocurrency economy.⁶⁵⁶ While increases in upfront capital costs do not completely explain the relatively low adoption rate, it does explain some of the centralization seen in token distribution as visualized by address analytics.

Information security is hard

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

Tabulating publicly reported bitcoins that were lost, stolen, seized, scammed and accidentally destroyed between August 9, 2010 and November 28, 2013 comes to approximately 803,285 bitcoins.⁶⁵⁷ A large bulk of this (171,955 bitcoins) comes from funds seized by the FBI from Silk Road in October 2013.

Between the end of November 2013 through March 2014, more than 150,000 bitcoins are known to have been stolen, destroyed, scammed, lost and “burned” bringing the total publicly known amount to 966,531 bitcoins that are no longer with their “legitimate” or “rightful” bearer.⁶⁵⁸⁶⁵⁹ Legitimate meaning, in this context, the person whom the law of a particular jurisdiction would be most likely to recognize as their legal owner, and from whom these bitcoins would be capable of being “stolen” in such a way that criminal sanctions would arise in relation to the theft.

Yet from the network’s point of view, it does not matter what is stolen.⁶⁶⁰ There is no protocol distinction between ownership and possession. Stealing is a legal term – not a physical phenomenon – thus whether it is rightfully transferred or not is the subject for legal scholars to debate. The bitcoins still exist. However, legitimate bearer issues are important in so much as they create uncertainty about the safety of attaching assets to the blockchain.

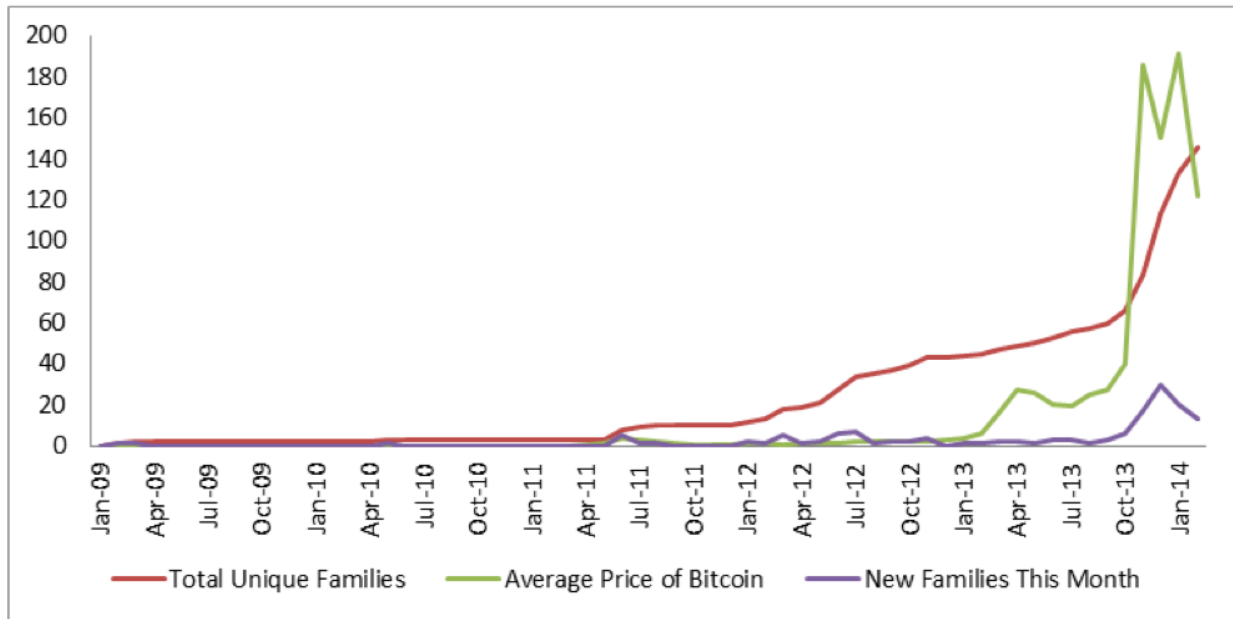
Furthermore, it should be noted that the concern here is not that bitcoins have necessarily been lost, since from a technical standpoint that does not make much of a difference. The concern is the uncertainty. The concern is that the market does not know what happened to or will happen to those stagnant tokens. If the market knew, for a fact, that all of Satoshi Nakamoto’s bitcoins or Mt. Gox’s bitcoins were gone and lost forever, the market could incorporate that knowledge into how it values the economic basis for the remaining bitcoins.⁶⁶¹ But as of this writing, this is uncertain. Further research should be done to reorganize lost coins into a group that increases uncertainty and a group that decreases uncertainty. It should also be noted that it is difficult to distinguish between bitcoins which

may have also been stolen from thieves by still other thieves during this tabulation (e.g., double counting).

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

- Coins stolen from mining pools (operator scalping/skimming)
- Unclaimed or unused promotions and dust tips on reddit and Twitter
- Coins stolen from insecure brainwallets (such as Naval Ravikant's "Hello World")⁶⁶²
- Dust on mining pools, exchanges and wallets
- Intentional spam for taint analysis (1Sochi and 1Enjoy in mid-February 2014)
- Money or undisclosed bitcoins stolen off numerous exchanges in which only fiat value is disclosed (e.g. GBL platform, on which \$4.1 million in user money was stolen in November 2013)⁶⁶³
- Ransomware copycats (CryptoLocker 2.0, CryptoDefense)⁶⁶⁴
- Accidental destruction arising from transfer to "temporary addresses" (i.e., many exchanges will issue new deposit addresses for each user, but by sending tokens to an identical address even minutes later could result in permanent purgatory or coin 'destruction.' All addresses are meant to be single-use however due to "user confusion" some users repeat spending to single addresses)
- Marginal cases of mining and forgetting keys or throwing away a laptop (e.g., Stefan Thomas, James Howell).⁶⁶⁵ Hal Finney remembered to back-up, others have not.⁶⁶⁶
- Jaded spouses⁶⁶⁷
- Flood or fire damage to a home or office⁶⁶⁸
- OTC and "hidden" order book⁶⁶⁹

What is ransomware? It is a type of software, or malware precisely, that prevents users from using their computer unless the user pays the malware creator some kind of "ransom." In this case, bitcoins.



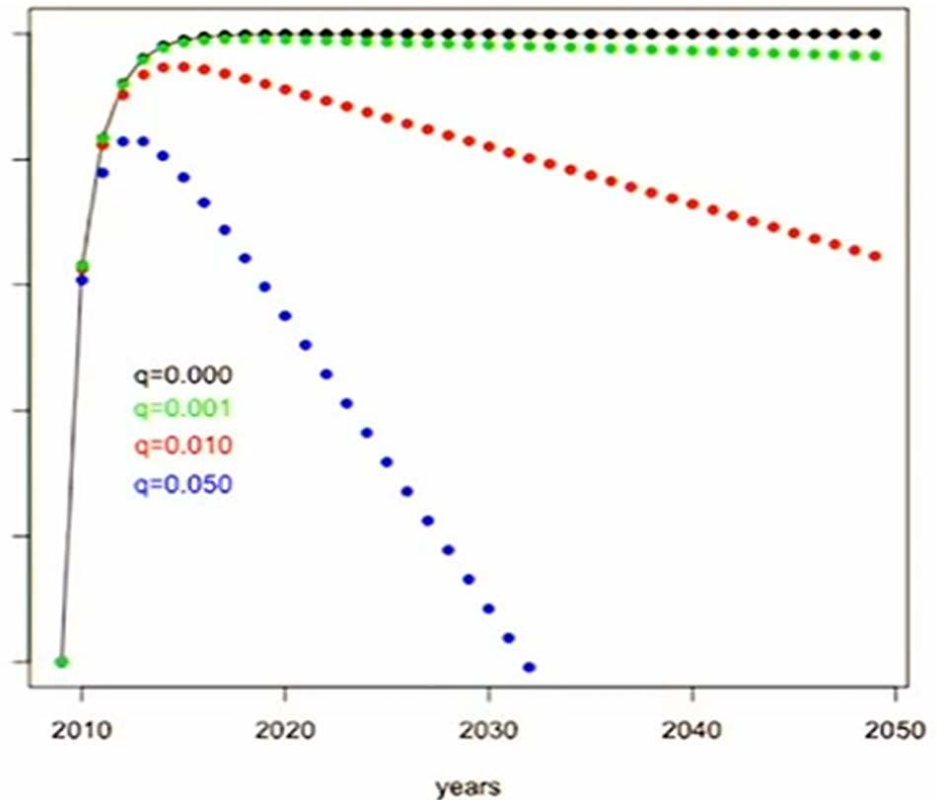
"SecureWorks' chart showing the correlation between Bitcoin's price increases and the creation of new Bitcoin-targeting malware." Source: Forbes

While this type of malware has existed for several years, Cryptolocker itself stole nearly 42,000 bitcoins last fall thus signaling to market participants that this successful method of attack could be copied.⁶⁷⁰ And as shown by the chart above, there were as of February 2014, 146 different families of "Bitcoin-stealing malware."⁶⁷¹⁶⁷²

How does someone steal coins from mining pools and farms? On July 15, 2014, a man under an assumed name, "Joe Simms" was accused of stealing 55 bitcoins from BTCJam (a P2P lending platform) and roughly \$160,000 in mining equipment from Digital Mining Investments where he was employed.⁶⁷³ At one point in his employment, Simms purportedly redirected the mining equipment to a "secret wallet" and then after leaving the company, attempted to sell some of the equipment online. There are other such instances in which employees or outside hackers redirect mining equipment to private wallets beyond the control of the intended recipient or in the case of pools, "skimming" off imperceptibly small amounts of bitcoins that was supposed to be awarded to a miner.

In terms of losing bitcoins, the chart below illustrates what the money supply looks like with an annual loss of 5% (blue), 1% (red) and 0.1% (green) of all mined bitcoins.⁶⁷⁴

effect of losing wallets with probability q



Source: Kay Hamacher and Stefan Katzenbeisser

In December 2011, German researchers Kay Hamacher and Stefan Katzenbeisser presented research about the impact of losing the private key to a bitcoin. The chart above shows the asymptote of the money supply (Y-axis) over time (X-axis).

According to Hamacher:

So to get rid of inflation, they designed the protocol that over time, there is this creation of new bitcoins – that this goes up and saturates at some level which is 21 million bitcoins in the end.

But that is rather a naïve picture. Probably you have as bad luck I have, I have had several hard drive crashes in my lifetime, and what happens when your wallet where your bitcoins are stored and your private key vanish? Then your bitcoins are probably still in the system so to speak, so they are somewhat identifiable in all the transactions but they are not accessible so they are of no economic value anymore. You cannot exchange them because you cannot access them. Or think more in the future, someone dies but his family doesn't know the password – no economic value in those bitcoins anymore. They cannot be used for any exchange anymore. And that is the amount of bitcoins when just a fraction per year vanish for different fractions. So the blue curve is 5% of all the bitcoins per year vanish by whatever means there could be other mechanisms.

While it is unlikely that the monetary stock of bitcoin will be reduced to zero (let alone by 2030) his explanation highlights the fragilities in building an economic system around a gold standard-like model that assumed Bob can always dig up what somebody else buried.

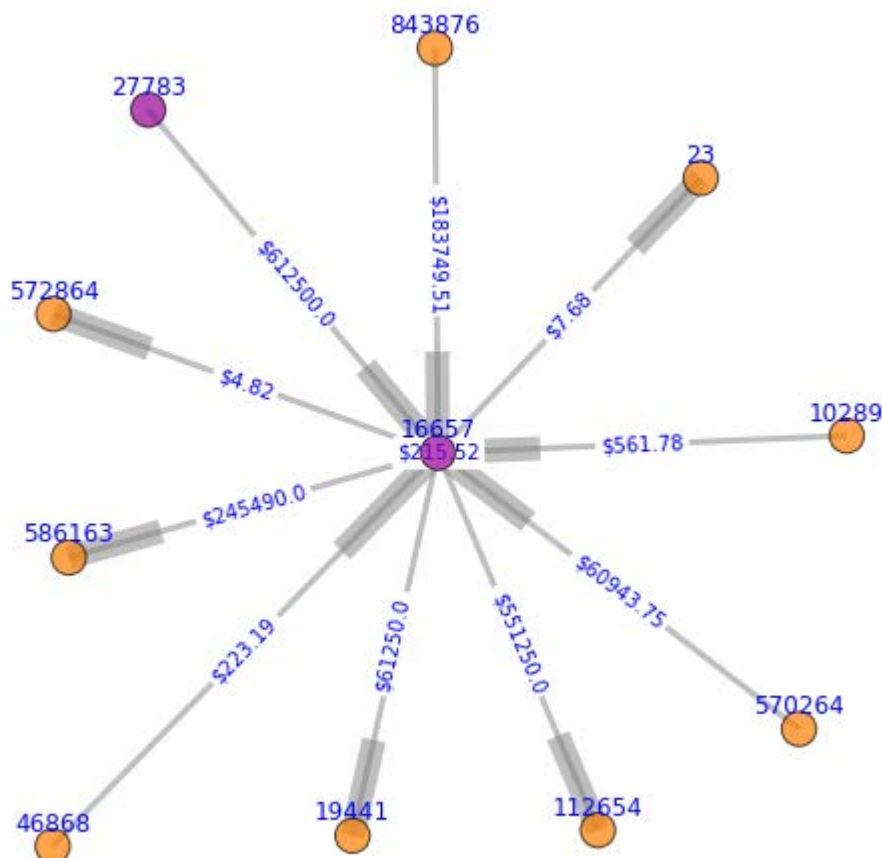
What about theft?

Dissecting a theft

One of the largest purported thefts in the history of Bitcoin, thus far, has been the allinvain heist.⁶⁷⁵ This is named after the eponymous user on Bitcoin Talk who in June 2011, reported that someone compromised his computer and stole 25,000 bitcoins.

Three years later, researchers at GraphLab used visualization software called SGraph to analyze the connections of where these funds travelled to.⁶⁷⁶

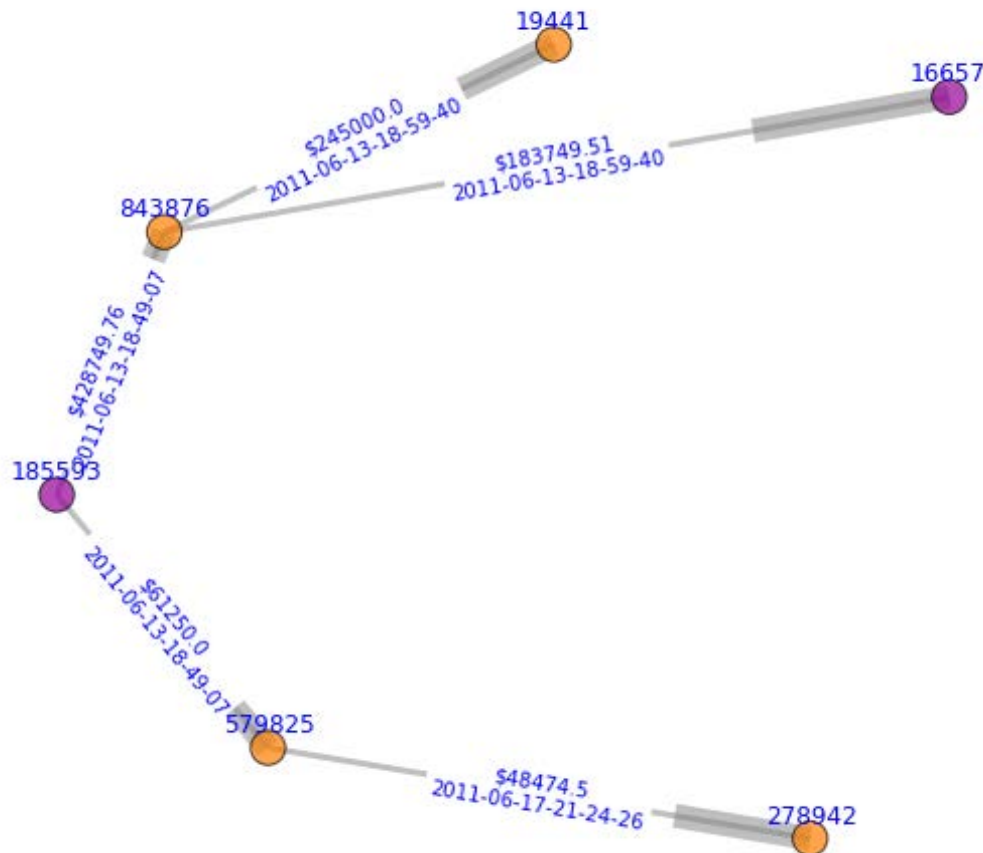
For instance, the diagram below depicts one such transaction point called ID 23 which received 0.31337 bitcoins (which is leetspeak for “eleet”):



Source: GraphLab

According to another team of researchers —Fergal Reid and Martin Harrigan — ID 23 is the MyBitcoin wallet service which is briefly mentioned in the next chapter because months later it also, incidentally, suffered one of the biggest hacks in the history of Bitcoin.⁶⁷⁷

After several more hops, the GraphLab team traced the funds to User 185593 who then effectively sent funds to two other users, 843876 and 19441:



Source: GraphLab

I would encourage all readers interesting in visualizing a traffic analysis – to see that a public ledger can keep track of thefts as well as what someone bought from the corner store.

Why is this important?

One area that is continually overlooked or hand waved are the bad actors involved in this process; there are more than a few bad apples and scammers, and as a consequence there are enormous wealth transfers and ill-gotten gains that have taken place, hence a never ending series of scams that have created real economic losses for some participants.⁶⁷⁸ The first time

Mt. Gox was hacked in June 2011, the trading and sell-off created a short-lived boom and then prolonged bust (e.g., “the Great Depression of 2011”).

A large portion of other thefts, such as the MyBitcoin Theft, took place during the “early years,” when there was low or no market value for the tokens, and as the space matures emphasis on security will likely reduce the threats and vulnerabilities. Yet every week there are new stories of scams and looting that surface — and because the ledger is public, you can actually view the movement or, in many cases, the non-movement of criminal activity — stolen bitcoins that cannot be moved because they have no exit.

A traffic analysis such as that from GraphLab, Reid and Harrigan or Sarah Meiklejohn illustrates this phenomenon.

How to exit the system unnoticed?

In China, you may happen upon a fly-by-night restaurant that offers relatively cheap food, being sold at a loss.⁶⁷⁹ Sometimes, these are fronts for organized crime, trying to anonymously mix their illicit funds into the real economy. There is a built-in incentive for criminals in the Bitcoin ecosystem to fund such exits, as well, especially mixing services.

While it is a controversial issue in some circles within the community to point this out, it is an important to recognize that the theft of property (the ledger entry corresponding to a private key) has taken place, continues to take place, and there is no built-in mechanism to rectify that.

This does not inspire confidence for those on fixed incomes such as disabled or retired workers whose welfare would be destroyed in the event that their keys are compromised without recourse. In practice, “being your own bank” is incredibly difficult for people not wanting or unable to memorize a hodge podge of passwords or go through the dozen-plus steps to make and secure a paper wallet.⁶⁸⁰ Solving this not only would engender confidence, but successful Bitcoin-related institutions in the future may look a lot more like Coinbase, Circle and Bitreserve than someone running Electrum or Armory on an air-gapped laptop.

Ironically cyber criminals themselves are aware of the double-edged nature of Bitcoin security. According to a *Reuters* story this past March:⁶⁸¹

But the fact that such payments can be traced would raise a red flag for cyber-criminals, says Daniel Cohen of RSA, the security division of EMC Corp (EMC.N), even though there are online services that can “launder” bitcoins to hide their origin. “Sure, there are bitcoin laundering services, but still if I tie a wallet to an identity I can see every single movement,” he said.

And, ironically, the success that some criminals have had in stealing bitcoins has made it less appealing to the underworld. RSA's Cohen says his team monitoring underground forums has noticed criminals lately see bitcoin as “volatile, seizable and, with the recent thefts, unsafe.”

Mt. Gox

Pre-eminent among these unknown numbers is Mt. Gox, an exchange that filed for bankruptcy on February 28, 2014. In its initial filings it noted customers may have lost 750,000 bitcoins and Mt. Gox itself lost another 100,000 bitcoins.⁶⁸² Subsequently on March 20, 2014, Mt. Gox announced that it had found 200,000 bitcoins in a wallet the company no longer used.⁶⁸³ On July 30, 2014, Tokyo police announced that they were formally investigating the theft of 27,000 bitcoins from Mt. Gox.⁶⁸⁴

While it is still unclear what exactly happened, many commentators have likened its operation to a stealth fractional reserve bank, which lent funds they did not have, effectively trading while insolvent without disclosing this fact to any party involved.

On the one hand it appears that post-2011, Mt. Gox may have been fraudulently lending out customer funds without informing them (publicly or privately) that Mt. Gox was not a 100% full reserve database. Yet Mt. Gox was never a bank. In fact, it was never *technically* lending customer funds as banks do.⁶⁸⁵ Rather it was a business that did not properly separate customer funds from its own or there was some outright illegalities or bad management (e.g. security breaches).

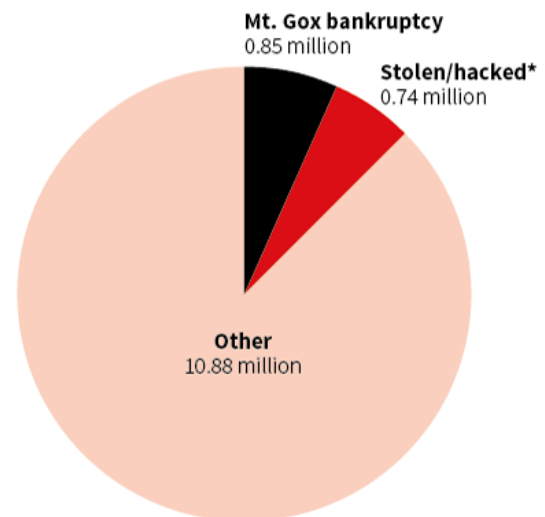
Financial institutions are required to separate their own funds from clients' and Mt. Gox apparently failed to do this somehow. In addition, in practice, modern banks and institutions using fractional reserve banking have certain lending requirements, depository requirements, and independent oversight in place prior to the creation and lending of credit. On the other hand, Brian Hanley and others argue that Bitcoin itself (the economy) cannot expand as the protocol has no dynamic method for lending or expanding credit but this is a debate that will likely continue for decades. The Mt. Gox bankruptcy case is still on going and despite data from The Willy Report, it is unlikely that we will know for sure what was actually happening for many more months and perhaps years.⁶⁸⁶

Missing bitcoins

Criminals may have already made off with up to \$500 million worth of bitcoins since 2009 excluding Mt. Gox. The exchange has blamed hackers for the disappearance of another \$500 million worth of bitcoins.

ESTIMATED NUMBER OF BITCOINS MINED

Global total: 12.47 million



Note: *Some bitcoins may have been counted twice if criminals stole them from each other or they were put back into circulation and stolen again.

Source: Reuters calculations.

J. Wagstaff, C. Chan 13/03/2014

REUTERS

Pie chart credit: Reuters

Why was one exchange able to impact the ecosystem so severely? Richard Brown concisely summarized the risks that bitcoin holders face when using that system:⁶⁸⁷

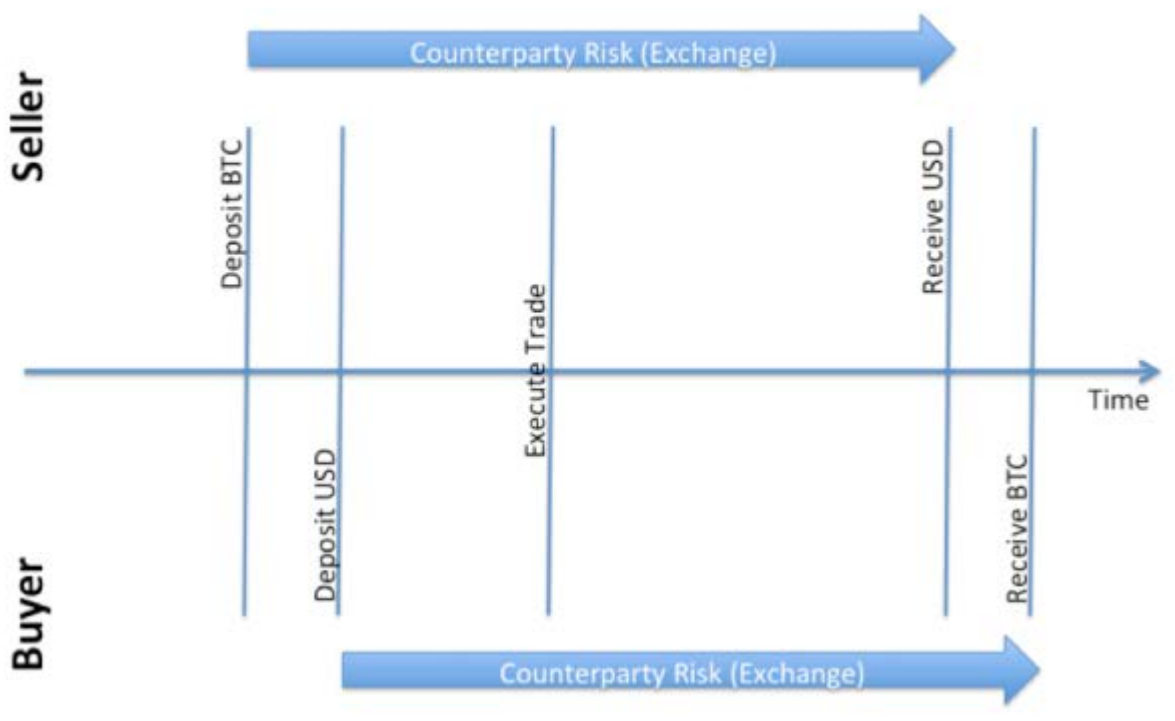
Imagine you were an equity trader and used a Stock Exchange to trade between equities and cash and back. What would happen if they unexpectedly filed for bankruptcy? How much money would you stand to lose? The answer is *zero*. You would lose *nothing*. Your equities would be safe at your custodian bank and your cash would be wherever you left it.

However, if you were a *Bitcoin* trader and your Bitcoin exchange went bankrupt, you could have lost everything – as users of Mt.Gox discovered to their cost last week.

How can this be? Isn't Bitcoin supposed to be the ultimate decentralized financial system? Well, yes... the Bitcoin network is decentralized but many of the major players are not. And, worse, exchanges like Mt.Gox acted as more than just exchanges: they are also the Bitcoin custodian, clearing house and bank.

The diagram below shows the problem. From the time a buyer deposits cash or a seller deposits Bitcoins, they are utterly dependent on the solvency of that exchange until they withdraw their funds at some later date. You have counterparty exposure to the exchange for all this time.

Risk faced by users of centralised Bitcoin exchanges



Flow chart source: Richard Gendal Brown

Brown aptly notes that in practice “[t]he equity world is more decentralized than the Bitcoin world!” The flow chart above is an illustration of how this worked in practice.

By 2013, it was generally accepted that approximately 1 million bitcoins had been lost, stolen, seized, scammed or destroyed in some manner. Therefore, to answer the question of what the edge-case statistics are for the aggregate of private key loss, tabulations provided by these empirical examples validate the notion that at least 1 million bitcoins were no longer with the property owner in some fashion. Adding Mt. Gox to this amount brings the figure to approximately 1,650,000 bitcoins which represents 13.5% of all mined bitcoins.

Thus if all Mt. Gox coins are recovered, then the lower bound is 10%, if less are recovered then closer to 15% altogether.

Including the 14.72% of mining rewards which are stagnant or lost forever and the 0.89% of dust and near-dust that resides on over 41 million addresses and most may never be used, approximately 30% of all mined bitcoins as of this writing are either lost, stolen, seized, destroyed, scammed, “dust” or forgotten. It bears mentioning, that as the pie chart from *Reuters* above notes, double-counting of coins stolen and yet stolen again may have occurred so there is likely an error term on either end of this number.⁶⁸⁸

While the non-collection of mining rewards will likely fall to zero as the industry consolidates and professionalizes, there are still on-going cases of fraud and abuse on exchanges. During the month of March 2014, the exchange CoinEx got hacked; in this case the customers were refunded. Also in March, another exchange Coinmarket.io, stopped processing withdrawals but continued accepting deposits leading to accusations that it was stealing customer funds.⁶⁸⁹ The following month, Cryptorush.io had internal mismanagement issues which culminated in a purported “hack” leading to a suspension of trading on and withdrawals from the exchange.⁶⁹⁰ And on April 2, 2014, Danny Brewster the CEO of Neo & Bee, a Cyprus-based exchange, allegedly absconded with up to several thousand bitcoins in investor funds.⁶⁹¹

In July 2014, a class-action lawsuit was filed against Coinabul, a bitcoin-to-gold trading platform as it allegedly failed to make delivery of gold:⁶⁹²

The plaintiff, Yazan Hussein, sent 1,644.54 bitcoins -- around \$970,000 at current market prices -- to Coinabul in exchange for gold coins and bars, the complaint says. Despite touting a short delivery timeframe, the complaint said, the company never delivered the goods and then refused to give Hussein a refund after he waited several months.

Furthermore, one study published in 2013 found that from 2010-2013, 18 out of 40 (45%) Bitcoin exchanges closed, often wiping customer balances with them.⁶⁹³ And revisiting the list of exchanges used in the study today would include 5 more exchanges that have since frozen or closed.

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

- Trezor, a hardware wallet that must be activated (similar to an RSA token or Google authenticator)
- Proof-of-reserves, such as that offered by Bitfoo⁶⁹⁴
- Insurance from a wallet and vault provider, Xapo and Coinbase⁶⁹⁵
- Hierarchical, deterministic multisignature (HDM) and oracle-based wallets such as Cryptocorp and BitGo⁶⁹⁶⁶⁹⁷
- Armory, an advanced desktop-based wallet⁶⁹⁸
- Paper wallets and cold storage⁶⁹⁹
- Two-factor, two-party transaction between untrusted peers via BIP38⁷⁰⁰
- Wallet-as-a-service from Coinkite and Blockchain.info⁷⁰¹⁷⁰²

Looking forward: expanded functionality brings extended risks

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

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

What if the new owner of Alice’s home is a non-governmental organization (NGO) or a non-profit organization? What if several days, weeks or months pass before the original, the owner realizes the deed or title to their boat or summer home has been resold and sold again and last owner is an orphanage or church? The underlying principle for this issue is called *nemo dat* (the buyer of which is called a bona fide purchaser). In the US there is an exception related to legal tender that has been sold and resold. This issue is compounded by what Robert Sams recently explained to me: What about ill-gotten performance of the 2.0 metacoin and digitized financial instruments? That is to say, in the event that sidechains, colored coins or other secondary protocols attached to Bitcoin begin issuing financial derivatives or even something as simple as a dividend, what happens in the event of theft?

For instance, if Bob’s colored coin representing a stock was stolen by Alice, does the company issuing the dividend still pay it? If yes, then this opens up the company to lawsuits, and if no, then Bitcoin (the protocol) ceases to function as a decentralized ledger, as the protocol would need to verify the identity, taking away the anonymity behind it. Currently, there is no way to do this on Bitcoin itself today without a major code rewrite and change in the social contract.

Preston Byrne, a cryptocurrency lawyer and securities lawyer in London, thinks that on account of problems such as these, the most likely future is hybridized - where decentralized computing would be paired with centralized key issuance and user registries. He adds: "it is entirely plausible to say that many of Bitcoin's descendants could be less free and more centralised than the Bitcoin of today, perhaps even state-run."⁷⁰³

Conclusions

Because of several barriers to entry, or frictions such as technical savviness, comparing the adoption rate with conversion rates used in advertising – where barriers to entry often merely consist of directing a shopping cart in planned routes in mature ecosystems – is a topic for further refinement and study.⁷⁰⁴

Securing tokens, as described in copious detail above, will likely be paramount for the continual adoption of any digital currency. Yet building a profitable business model to fund the development of tools such as multisignature wallets could be difficult if adoption remains stagnated – revenue needs to come from somewhere.

And because no two histories are alike, Bitcoin adopters have no specific blue print to build their ecosystem to or from. After all, if the development of Linux is an indication, someone else will likely capitalize off Bob's volunteer efforts for adding extensibility features to the code, so why bother developing a robust wallet if it is simply going to be forked and cloned?⁷⁰⁵ This conundrum is compounded by the incentives to use scarce talent (such as a penetration testing and security auditing) to steal coins from the undersecured.

As a consequence, some liken the current experiment as a five year condensed version of the past century in banking involving scams, booms, bubbles, fractional reserve schemes and outright theft. Providing incentives to overcome these challenges may result in new data illustrating growth in on-chain activity including transactional volume or renewed activity by old dormant addresses.

Chapter 13: Social engineering and groupthink

It is likely premature to call all proof-of-work-based cryptocurrencies unsustainable or bubbles. However, the non-linear variety, the asymptote-based money supply version used in Bitcoin, Litecoin, Dogecoin and several hundred others has created a “get rich quick” distribution model (because that is how the trust fund's principal is divvied out, it tapers off over time). In a sense, the internal incentive mechanics (the scheduled inflation) creates froth and irrational exuberance by design. This chapter briefly discusses historical bubbles and several social themes that underscore how several portions of the community set policies and attempt to influence the ecosystem.

For example, one response I received from the content in chapter 4 came from an executive, “Alice,” at a Bitcoin merchant payment processor who asked:

Regarding your overall point about Bitcoiners boxing ourselves into a corner, do you ever foresee a situation where (motivated by long-term self-interest), some of the original holders of large amounts of bitcoin actually conspire to give away a good chunk of their holdings so that more people on Earth are actually in possession of the coin?

Short answer, no.

While there may be some edge cases like Roger Ver donating to FEE last year, it is unlikely that more than a small minority will voluntarily give away their coins.⁷⁰⁶ Why should they, especially if upward valuation incentivizes users to “hodl” (sic) to the moon?⁷⁰⁷

John Kenneth Galbraith wrote several books on this topic, most notably *The Great Crash, 1929* and *A Short History of Financial Euphoria*.⁷⁰⁸ The latter version has several germane excerpts that relate to just about any historical financial bubble.

One notable, relevant passage was reused in *The Essential Galbraith* and has Galbraith describe (contrarian) analysts who predicted bubbles and were called a number of names for trying to identify risks and bring challenges to the forefront.⁷⁰⁹ Below is a portion of one passage:

Strongly reinforcing the vested interest in euphoria is the condemnation that the reputable public and financial opinion directs at those who express doubt or dissent. It is said that they are unable, because of defective imagination or other mental inadequacy, to grasp the new and rewarding circumstances that sustain and secure the increase in values. Or their motivation is deeply suspect. In the winter of 1929, Paul M. Warburg, the most respected banker of his time and one of the founding parents of the Federal Reserve System, spoke critically of the then-current orgy of the “unrestrained speculation” and said that if it continued, there would ultimately be a disastrous collapse, and the country would face a serious depression. The reaction to his statement

was bitter, even vicious. He was held to be obsolete in his views; he was “sandbagging American prosperity”; quite possibly, he was himself short in the market.

Is all criticism of Bitcoin or its progeny merely a new form sandbagging?

No, Carol could like the technology Alice uses yet could still equally be critical of the missionary mentality surrounding the marketing of the technology.

Galbraith’s *A Short History of Financial Euphoria*, goes through a handful of well-known bubbles which can be instructive to both novice and veteran’s within the digital currency space alike.

Some common themes and parallels he found throughout each episode are (in reverse pagination):⁷¹⁰

- Regarding manias, “Individuals and institutions are captured by the wondrous satisfaction from accruing wealth. The associated illusion of insight is protected, in turn, by the oft-noted public impression that intelligence, one’s own and that of others, marches in close step with the possession of money. Out of that belief, thus instilled, then comes action – the bidding up of values, whether in land, securities, or, as recently, art. The upward movement confirms the commitment to personal and group wisdom. And so on to the moment of mass disillusion and the crash. This last, it will now be sufficiently evident, never comes gently. It has always accompanied by a desperate and largely unsuccessful effort to get out.” (p. 106)
- On Bernard Cornfeld’s activity with Investors Overseas Services and perhaps some Bitcoin adopters, “It is difficult to believe that he was guilty of anything beyond his own misguided energy and ambition. The guilt lies, as always, with those who sought so eagerly and by such a transparent device to be so separated from their money.” (p.93)
- Regarding the crash of 1929, “How little, it will perhaps be agreed, was either original or otherwise remarkable about his history. Prices driven up by the expectation that they would go up, the expectation realized by the resulting purchases. Then the inevitable reversal of the expectations because of some seemingly damaging event or development or perhaps merely because the supply of intellectually vulnerable buyers is exhausted. Whatever the reason (and it is unimportant), the absolute certainty, as earlier observed, is that this world ends not with a whimper but a bang.” (p. 83)

Again, this is not to say that bitcoin (the token) is a bubble itself, we can only know for certain later on. But, a lot of the promotion, marketing and overall ambience around it is very similar to traditional financial bubbles including the usage of the same phrases “this time things are different” or “we have reached a permanent high plateau” or “don’t you want to be rich?” or “you don’t have to do anything, just sit back and relax” or “no way you will lose” or “you simply do not understand its ability to disintermediate” or “it’s a new financial innovation that the world has never seen.”

Yet, the world has seen new commodities before (DRAM). The world has seen new currencies before (euros), it has even seen the likes of pre-Bitcoin cryptocurrencies such as Beenz (which

raised \$100 million as a “web currency”).⁷¹¹ Alice cannot sit back and relax indefinitely, someone has to work. Plateaus do not last forever. Coin speculation is a zero-sum game and affluence can be ephemeral. Lastly, being your own bank is a Pyrrhic task; you can do it but have a high chance of failing. Perhaps the protocol is the real deal for certain use-cases, but the tokens are probably not the cure-all remedy that many proponents make it out to be. Furthermore, one area for future research is to look for whether or not a specific user base or pool of potential speculators has been exhausted (e.g., beyond redditor saturation).

The issue Alice was confronting at the beginning of this chapter is that she and all other merchant processors are effectively having to compete for the same small liquid tokens, roughly 1 million bitcoins at most and according to Total Volume Output, more likely no more than 500,000 bitcoins. That pie is not getting any larger; bitcoins are not being added to the long-term liquidity pool because again, most bitcoin holders are speculating – they have an incentive to hold and several disincentives to spend.

Thus in effect, all merchant processors are fighting after the same small portion of the pie. A pie that is not growing because it is static, inelastic. Or in more colorful terms: Bitcoin does not really have a consumer economy, it has a speculative futures market attached to an emerging, capital starved country. And instead of creating utility for the actual country, most bitcoin holders instead have an incentive to buy and hold. It is a classic type of prisoner’s dilemma – everyone would be better off if all participants cooperated, but there are numerous incentives not to (see chapter 2).

In fact, they are encouraged not to by endless threads on community sites and social media.

Hence, in this case, Bitcoin is still largely a zero-sum and even negative sum economy that is probably only growing on the edges in trusted-silos (where economies of scale are larger and more efficient per unit of capital). This is not to say that trusted solutions do not provide utility (in fact, they empirically do as shown by their continued popularity) however users of those services are essentially trading IOUs of an SQL entry.

This could be one of the reasons why BitPay recently had a leadership change and has hired specific people with traditional payments experience over the past few months. Despite the roughly \$1 million in daily payments they are processing, they have no real way to extract value due to their thin margins (Coinbase and others may be in the same situation; few people spend in part because there are few liquid bitcoins).⁷¹²

Why?

Bitcoin is a brutally one-sided against spenders. Not only is what effectively could be termed “foreign exchange” volatility an issue that normal consumers prefer not to have to deal with (e.g., why does Alice want to be exposed to foreign currency movements?), but consumers have to pay a fee if they want their transaction put into the next available block.

For instance, following the announcement by the US Marshals Service that it would begin selling seized coins from Silk Road, on June 12, 2014 the price level of bitcoin dropped by 9% in a matter of 6 hours and then regained half of that amount six hours later.⁷¹³ In finance terms, it has a high beta (β). And while helpful, it is unlikely that any amount of temporary discounts will on-ramp merchants who would prefer not to have to juggle through known processing steps.⁷¹⁴

Even if the merchant base that accepted bitcoin tripled again tomorrow it would not change the number of possible tokens that can be used in commercial transactions. This is a bug in a modern economy, it is the side effect of having an inelastic money supply. And it is unclear how this will change going forward as volatility upward just incentivizes people to hold onto it longer for the dream of becoming Bitcoin Rich.

A viable economy or a support group?



Source: The Onion

The mythos of Satoshi has amplified, enlarged and even turned some advocates into creating a mini cult-like apparatus just as the Red Guard deified Mao during the Cultural Revolution. However this is unproductive and likely only fans the flames of outside criticism which includes the same skilled people that any country or ecosystem needs to survive and thrive. While their passion is laudable, the stonewalling rhetoric by some adopters is inimical. What will likely happen is that because the underlying technology is an open-source protocol it will likely be used as an agnostic tool and agnostically absorbed.

Institutions, enterprises and governments will take what is useful to them and internally incorporate it. Anything that provides them an additional edge will eventually be ingested and the rest is discarded. And they will probably not change their own existing behaviors or worldview just because

The direct historical facsimiles would be with the free and open source (FOSS) movement in the early 1990s. A small vocal group of GNU advocates believed that tools like Linux would revolutionize and democratize regimes like China. But in point of fact, the Chinese government simply absorbed the technology and used it for its own goals, erecting a powerful digital funnel called the Great Firewall which allowed them to survive the information age – an age that would bring them a loss of face (*diu le mian zi*). They adapted and most likely other governments and institutions will do the same with this technology. Satoshi, whomever he, she or they are, were clever and should be acknowledged for creating this very interesting experiment. However, a significant coterie of Satoshi fans have recreated something

reminiscent to the “cult of personality” parody from *The Onion* (above) – it is likely counterproductive.⁷¹⁵

For perspective, in his June 2014 paper, Gianluca Miscione notes that:⁷¹⁶

Myths are performative in legitimising something to the extent they make it believed as real. So, myths can engender a ‘suspension of disbelief’. In other words, myths leverage the Thomas theorem: ‘If someone believes that something is real, it will be in its consequences’. A contemporary example comes from Bitcoin: we do not know how this crypto-currency may affect global financial transactions cutting middle-men (central and private banks). But as long as a growing mass of users believes in its libertarian myth enough to convert their money, its chances of bootstrapping beyond small circles of tech-savvies are real.⁷¹⁷

In his paper, *Bitcoin and complexity theory*, Marc Pilkington provides some additional analogues between Bitcoin, altcoins and the anthropological and socio-psychological approaches to money, noting:⁷¹⁸

The True Believer: Thoughts On The Nature Of Mass Movements (Hoffer, 1951) offers an explanation of mass movements that originate in a desire for change from human communities discontented by the prevailing cultural artifacts and traditions. Interestingly, the Bitcoin discussion features elements of the psychology of mass movements. Hoffer offers insight into what drives the mind of the fanatic and the dynamics of mass movements. The book is a twentieth century landmark in the field of social psychology, and is more relevant today than ever. Regarding Bitcoin, viewed as mass movement, the coexistence of several virtual currencies today bears testimony that “all mass movements are competitive” (Hoffer, 1951, p.17). Likewise, drawing on the philosophical and anthropological insights of René Girard about the mimetic rivalry, contagious in essence, originating from the struggle for the possession of goods in ancient societies, thereby leading to the threat of violence, the mimetic nature of money was further explored by French authors Aglietta and Orléan (1982) in their landmark book *La Violence de la Monnaie*.

If Bitcoin is a “movement,” altcoins would fulfill the notion that “all mass movements are competitive.”⁷¹⁹ Yet, Izabella Kaminska, a writer at the *Financial Times*, pointed out the irony of how on the one hand, numerous Bitcoin proponents extoll the virtues of a competitive market place for monies (e.g., denationalization of money, removal of legal tender laws) yet on the other hand, disdain similar competition from altcoins:⁷²⁰

In the free-market world of crypto currencies all private alternatives to fiat are theoretically equal, but some are more equal than others. Meaning in the eyes of the Bitcoin community it’s okay for some people to be able to mint themselves free money and encourage its acceptance for real-world goods, but it’s not okay for everyone to be able to do the same — in line with competitive free market principles.

Altcoins are a very divisive issue, as early adopters foresee how competing alts could erode their net worth in bitcoin and thus actively campaign against their further creation. Whether it leads to different outcomes and reactions in the long-term is an open question.

How then has the behavior of users changed over the years?

The abstract and Section 1 of Satoshi's whitepaper describes the trusted third party vulnerability in the payments and exchange space. Similarly, the title of the paper suggests that bitcoins will be used for a peer-to-peer electronic payment system. Satoshi even intended to build a P2P marketplace inside the protocol itself, but later removed the code.⁷²¹

Yet in practice what has happened is that once there was a market rate for bitcoins, behavior switched from a Dogecoin-like faucet service to a money-like informational commodity.⁷²² Economically rational actors treated bitcoins (and the protocol) based on its core qualities: a deflationary (in the long-run) inelastic money supply. Spenders are uninterested in having to deal with a volatile currency or one they have to pay to use. This price volatility coupled with the expectation of price appreciation incentivized people to hold it.

For balance, by removing the popular addresses such as the gambling sites, there may be some real economic commerce taking place on the chain, roughly 60,000 transaction per day.⁷²³

That may sound like a lot, but it is not. At the beginning of the year there were an estimated 20,000 to 30,000 merchants and that figure has doubled to more than 63,000 by the end of June.⁷²⁴ And most merchants that accept bitcoin payments do not receive one daily, instead the distribution probably looks like a power law (or the 80-20 rule).

For instance, assuming that wallet installations equal user numbers (which is not the case), in July 2014 Brett King pointed out that:⁷²⁵

At around 3 million users in December, we're looking at an average of just *one transaction per month*. With double that number of users expected in Q3 2014, and half the transaction volume, we're looking at a decrease to less than one transaction every two months per user. That is not a growth economy for payments or commerce, it is respectable volume for trading.

Either way, whether wallet installations equal users or not, there is no subsequent increase in on-chain transactional volume. Though perhaps volume is merely at the early part of the curve where it is not clear what the trajectory is.

Demythification

There are a few other areas that tie into what Galbraith noted above; for instance, despite the contention that early Bitcoin adopters took risks, they actually did not take *large* risks. While this is a topic that could and will fill additional pages, securing the bitcoin network with hashrate in the first two years was virtually risk-free as capital and operating costs were both minimal (this is not to say it is or was a risk-free asset under CAPM). The biggest risk was

accidentally destroying the hard drives (not backing up the wallet.dat) or sending them to hosted wallets like MyBitcoin, which as noted in chapter 12, involved one of the largest thefts ever.

While there are indeed greater risks to capital outlays for large mining farms today (e.g., amortization cost curves), one of the reasons for the continual popularity for creating alts is that it is not very risky to be a first mover when all you have to do is fork open source code and promote it on a forum. This is not to say that early adopters do not deserve the tokens they have but it would be false to claim they had any specific unique ability that has not occurred in other bubbles as quoted above. And at the same time, some aspiring fund managers are suggesting bitcoins performance seems to have a high Sharpe ratio; going forward, financial researchers may be interested in looking at whether kurtosis or skewness (such as coin distribution) impacts it as well.

As a friend recently pointed out, this is not an appropriate measure when return distributions are asymmetrical or for something that is treated as a collectible. For example, if the distribution is negatively skewed, you might calculate a Sharpe ratio for a period when there were a large number of small gains. This would not correctly reflect the small probability of occasional large losses (e.g., writing call/put options, an activity that has been likened to “picking up pennies in front of a steamroller”).

Again, in practice, it trades more like a commodity than something with P/E ratios (it has no earnings). On the face of it, it appears as if the vast majority of bitcoin price data is likely explainable via an exponential growth curve. In fact, 90.1% of the historical price variability is accounted for by the equation: $y = 10^{(-36 + 0.0029 \cdot x)}$, where y is the price and x is the fractional year.⁷²⁶ Yet this is *ex post*; the error term does not seem random. There is a deterministic trend that would have to be filtered out first. It is the same problem with modeling long term GDP growth. After all, why would we need all these economic models if we can simply draw a straight line and predict GDP using high school math? Many things follow an exponential growth curve, that is nothing new. The exciting thing is to forecast it in the short term, which this method is poor at.⁷²⁷

However, despite knowing the inherent problems of “technical analysis” for Bitcoin, there is tendency of people to favor information that confirms their beliefs and this is how many participants get trapped in the bubble.

Consequently, this self-reinforcing groupthink has produced a number of ideas such as the notion that all fiat globally will be replaced by bitcoins. Yet what these advocates are effectively saying when they claim total global fiat value will be mapped onto bitcoins is that these adopters will control 13/21st of the world’s fiat-based wealth (e.g., 13 million bitcoins out of the 21 million). There is no reason to believe this is the case, for the same reason that global fiat value was not grafted onto any other commodity.

Nor is this stated to defend existing institutions and their policies, there is simply a difference between what can happen and what will happen. For instance, Bitcoin could theoretically become the sole reserve currency of a major country, but it will not be due to how reserve currencies actually function.

The Chinese RMB

Because there is an enormous amount of confusion in the Bitcoin community as to what reserve currencies are and how they are used, it is recommended that readers peruse what Patrick Chovanec wrote several years ago – perhaps the most concise explanation – as it relates to China (RMB), the United Kingdom (the pound) and the United States (the dollar):⁷²⁸⁷²⁹

There are four main factors that set the Pound and the Dollar apart as viable and attractive reserve currencies. Each was necessary. They were liquid. They were available. And they were perceived as safe. I'm going to run through each of these conditions in turn. I will consider how they applied to the Pound and the Dollar, and to what extent they are satisfied by China's Renminbi.

(1) Necessity. The fundamental purpose of a reserve currency is to settle external obligations. The greater quantity and variety of obligations a particular currency can settle, the more useful it is as a reserve currency. The currency of a country that produces little of note and lacks funds to lend or invest is not nearly as useful as one whose home economy produces many goods and services desired around the world, serves as an important source of capital, and has many commercial partners who also find its currency relevant to meeting their own obligations. This idea — that the dominant reserve currency derives its status from its connection with the dominant national economy in an interconnected world — is what underlies Roubini's reasoning that the Renminbi may be next in line to replace the Dollar.

But this conclusion misses something important. A reserve currency must not only be capable of settling obligations in connection with a heavy-weight economy. It must be required to. Because if you can settle those obligations, as sizeable and important as they may be, using your own currency — or the currency of another leading economy — there is no reason to hold that country's currency as a reserve. That is precisely the case today with China.

It is unclear how or why some Bitcoin advocates can suggest that bitcoins will ever be used as a reserve currency when there is no demand for the currency to meet external trading obligations let alone in the magnitude that these other currencies do (RMB, USD, GBP).⁷³⁰ As noted in chapter 7, despite a concerted push from within, the RMB, backed by a multitrillion dollar economy that produces real goods and services is only used in 1.4% of all global payments compared with the US dollar at 42.5%.⁷³¹

Expanding credit alone is not the answer to making bitcoin a reserve currency. For instance, China's money supply grew leaps and bounds since November 2008 when it implemented a series of stimulus packages.⁷³² It also signed bilateral currency agreements with new countries every year which led many outside commentators to erroneously conclude that this somehow leads to mass adoption of the RMB.

In an effort to increase its internationalization, in 2005, the Chinese RMB was marginally unpegged from the dollar. Over the subsequent 9 years the RMB has been traded in a managed band in which the People's Bank of China (PBOC) allows it to swing 0.5% in either direction of a peg set each day. Consequently, the RMB has since appreciated roughly 30% during this time (though remains virtually unmoved in the past two years).⁷³³

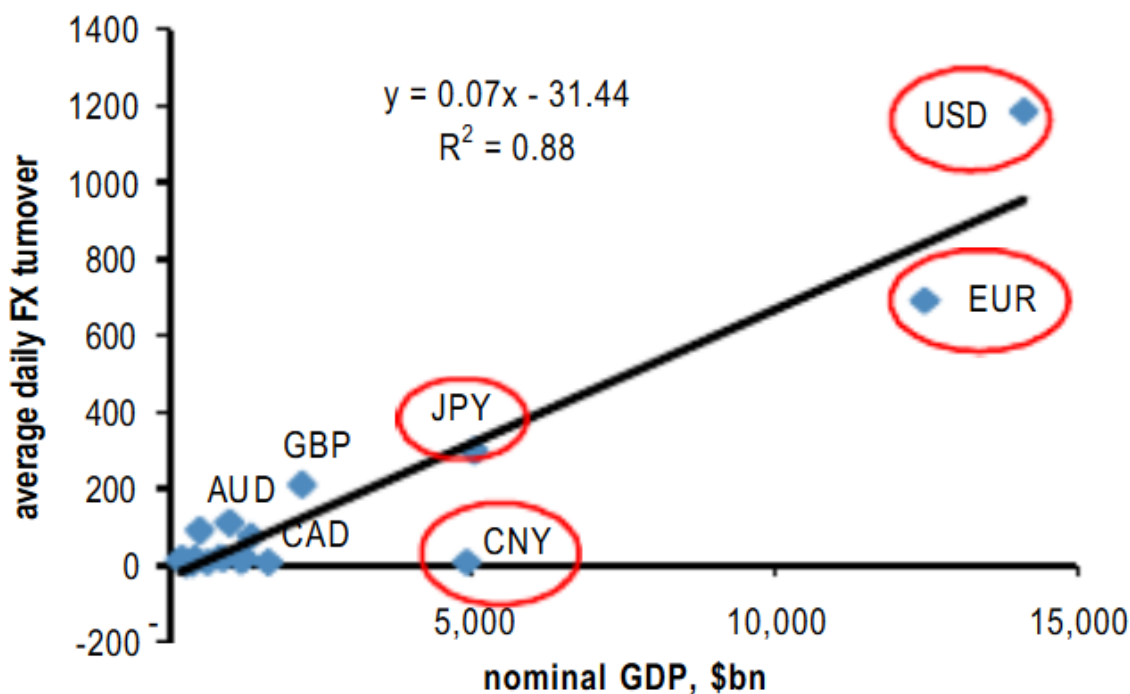
However, even in its current doldrums, the Chinese economy still produces real goods and services to the tune of trillions of dollars per annum. Obviously it is unfair to compare Bitcoin, a five-and-a-half-year old "startup" to China. Yet the emerging market aspect, the reuse of capital stock, the implementation of new financial instruments, the training of unskilled laborers and ultimately the creation of needed utility to outside parties can be viewed as facsimiles to learn and grow from.

If history is any indication, the RMB has a significantly better chance of internalization than bitcoin or any of its direct descendants. For instance, as noted above the RMB, despite a variety of controls imposed on it by the PBOC (e.g., not free floating, no real bond market) the RMB has still made some in-roads with trade finance.⁷³⁴ While liberalizations have been deliberately measured, this will eventually include letters of credit, bank guarantees as well as collection and discounting of bills. In contrast, because of its structure as a non-national currency, it is unlikely that bitcoin or any cryptocurrency will be demanded by exporters or importers to be used as a settlement instrument before the RMB is. Thus the imprecise logistics of how bitcoins are used in this multilateral, multinational role is ambiguous at best. However this is a topic for future researchers to discuss.

What does this look like?

Chart 4: Certain currencies are widely used internationally because a government compels their use in large, open economies

Nominal GDP (x-axis) versus average daily FX turnover for reference currency versus all other currencies (y-axis)



Source: J.P. Morgan, BIS

Above is a chart from a report by John Normand at JP Morgan.⁷³⁵ Despite the fact that the Chinese economy overtook Japan's to become the world's 2nd largest four years ago, its currency (RMB) still has a fraction of the daily FX turnover compared to the Yen. Part of Normand's argument is that one of the advantages that these national currencies have is that their issuing governments can compel trading partners to accept them which obviously is point of contention by many Bitcoin adopters.

Building a continuous series of bubbles or building utility

Another common refrain by some Bitcoin advocates is that the open source network is similar to the origin and evolution of Linux. Yet apart from a few superficial attributes (open codebase written in C++ and developer disagreements), the similarities end. For instance, did the last wave of enthusiastic volunteers in the technology space generate as much revenue as the early adopters of bitcoin merely by releasing code and leaving their laptop on? No. Someone had to create value and utility which was later incorporated and funded by real businesses with real needs to customers with real needs. Similarly, someone is going to have to roll up their sleeves

and do the same for this space. In fact, *Bloomberg* noted this dissimilarity, that “[u]nlike Linux, bitcoin rapidly became a channel for billions of dollars in transactions, making security and capacity bottom-line issues for entrepreneurs.”⁷³⁶

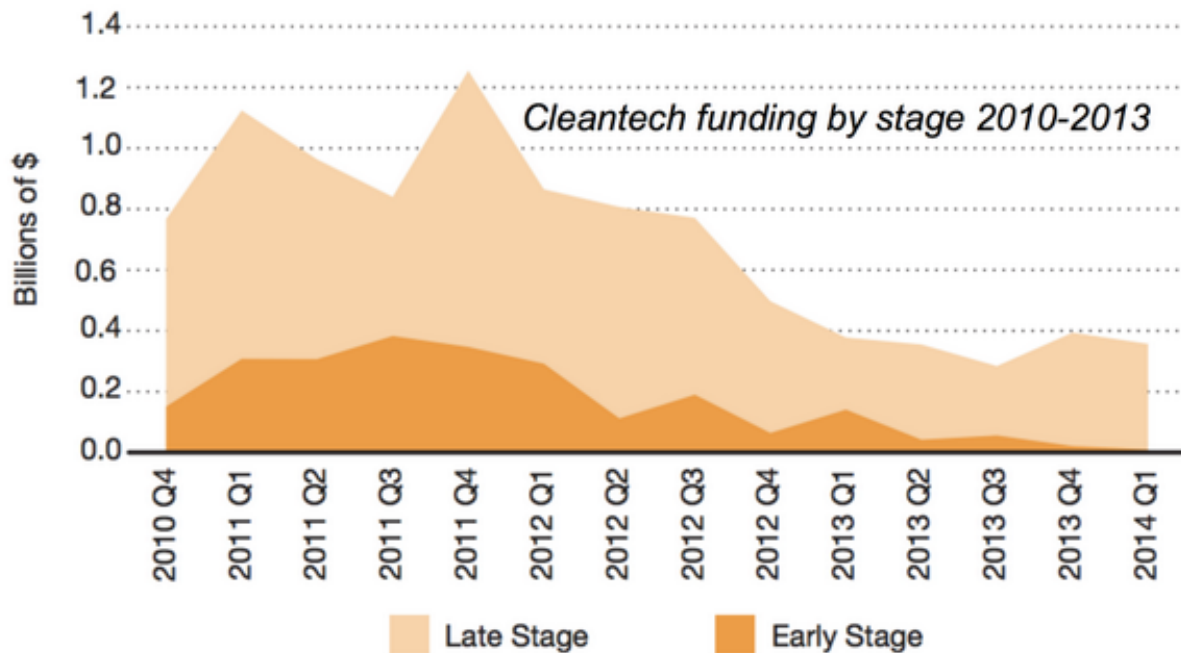
A popular grievance leveled again altcoins and appcoins in general is that none of the underlying systems are able to give out real equity and thus cannot have P/E expectations – neither does bitcoin, nor will it. As noted in chapter 8, this is a bug and it is why using the "TCP/IP" analogy is probably incorrect. The internet is an amalgam of private-public intranets cobbled together and cost real capital to build. It was not built with wizardry; real incentives had to be provided to build it. Imagine if those incentives decreased 50% every 4 years? That's Bitcoin's internal economy. The Bitcoin network cannot operate without bitcoins – the app or currency or commodity (choose your definition). The two are united together. Yet TCP/IP, the protocol, can still work even if substantial portions of the network fails; it is not tied to a specific set of hardware or limited amount of tokens (TCPIPcoin).

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

VC CLEANTECH DEAL FLOW BY YEAR



So what kind of bubble is bitcoin then? Some claim that it “crashes upwards” – yet it is unclear how bitcoin (the token) is immune to the laws of economics. Perhaps as illustrated above, the current investment cycle in bitcoin is more akin to Cleantech circa 2005?⁷³⁷



Source: Ilan Gur and Danielle Fong

What this means is that, even though many of the startups are clever, they may lack sustainable business models. Once this ebullition is removed, the businesses that survive will likely be those that are actually creating real pain killers (utility) to real needs; perhaps reusing the infrastructure of the network as distributed asset digitization platforms (via merged mining proposed by startups such as Peernova, or Salpas) to process contracts and property titles.⁷³⁸

Again, all of this is speculative, yet it warrants attention because Cleantech also had a similar dedicated ideological group of early adopters that created economic activity (though, not much growth yet) and wanted to change the world. And despite their best efforts it popped.⁷³⁹⁷⁴⁰

What about the potential from retail payments?

As noted in chapter 4, when Dell announced that it was accepting bitcoin as a form of payment in July 2014, while it may provide a sales boost for the following month or two, this is only helpful to those who own bitcoin. And most bitcoin holders already have multiple ways of purchasing electronic equipment with or without fiat; the same targeted consumer base already has credit cards. Or in other words, it is unlikely that someone has enough bitcoins to buy a computer who does not already have a credit card that can do the same thing.

In contrast to the RMB, which can be expand as a form of credit, bitcoin cannot expand – Dell would likely see larger amounts of transactional volume and revenue if they accepted the RMB. And they did.⁷⁴¹ After initially rejecting a plan in 2003 to sell computers online in China, Dell reversed course and within 2 years online sales to China represented 6% of all orders at Dell.⁷⁴²

China is now Dell's second largest market by revenue only behind the US. It is unlikely that bitcoin will ever reach a similar percentage.

Can all the utility in this space be crowdsourced?

Probably not. There is only so much capital that can be extracted from the vocal crowds of social media such as reddit. Significantly more capital is needed to scale operations to enterprise-level reliability. While some advocates believe eschewing the *ancien* regime of venture funds and private equity is the way to move forward, this is likely short-sighted; capital markets are orders of magnitude larger than the collective wealth of all Bitcoin holders.

Deciders

In terms of social engineering, another core attribute of command economies is that they typically do end up having some decider (a “strongman”) who invariably decides the course of action.⁷⁴³ In the case of Bitcoin, the deciders are mining pools who *understandably* will only secure code that is profitable to them – after all, it is their depreciating capital goods (mining equipment) that provides the entire utility for the network, why can't they decide what to do with it? As a consequence they each decide which transactions to include (or what to leave in the mempool), what blocks to propagate (or potentially refuse) and what fees (if any) to set. And these issues are likely to become more prominent as the mining becomes more professionalized.

Simultaneously, another group of stakeholders are the core developers, who have proposed a myriad of clever, innovative features, but there is no immediate incentive for miners to currently adopt these changes.⁷⁴⁴ We saw this with the deliberation over the size (40 bytes versus 80 bytes) for OP_RETURN in March as well as the debate over the double-spend as a service startup (BitUndo) the following month.⁷⁴⁵ As a consequence, the challenge Mark DeWeaver noted in chapter 8 related to special interest groups and emerging countries bears repeating:

“The thing about developing economies is that they usually seem to be held hostage by special interest groups that insist that development must proceed along a path that doesn't threaten their interests. So they tend to end up with what the political scientist Fred Riggs called “prismatic development”— a Potemkin version of the development seen in advanced countries. If it's like a developing country, it could be stuck where it is now pretty much forever.”

It is unclear what pressure either entity, developers and miners, would have in the event of a multi-billion dollar heist. For instance, on July 13, 2014, an exchange called MintPal was hacked and 8 million Vericoins (an altcoin) were stolen.⁷⁴⁶ The hacker managed to withdraw these coins (as well as bitcoins and litecoins on the exchange) before the site could stop them. This represented about 30% of all vericoins in existence. As a consequence, the Vericoins developers

created a hard fork which reversed the transactions, nullifying the transfer of those stolen coins.

While hailed by some as heroes to the community, others critically viewed this as a vulnerability as it removed the major competitive advantage a blockchain was supposed to have: a lack of a trusted entity. It is unclear what would happen if such a heist took place in Bitcoin today, if \$1 billion was stolen from a venture funded wallet or exchange, would this put pressure on developers (who work for venture funded companies and mining companies) to fork and reverse the transactions? Could collusion happen if the price was high enough?

There is actual historical precedence of this problem and type of solution occurring in Bitcoin. In August 2010, an attacker exploited a vulnerability, CVE-2010-5139, enabling them to create 100 billion bitcoins. The core developers solution was to roll back the blockchain, nullifying the post-exploit transactions:⁷⁴⁷

The fix was the bitcoin equivalent of dying in a video game and restarting from the last save point. The community simply hit 'undo', jumping back to the point in the blockchain before the hack occurred and starting anew from there; all of the transactions made after the bug was exploited – but before the fix was implemented – were effectively cancelled.

Could this happen by accident? In an interview last year, Andrew Miller explored a hypothetical scenario in which a user accidentally sends (or his wallet accidentally glitches and sends) 1,000 bitcoins as a transaction fee – which as of this writing would be worth \$610,000.⁷⁴⁸

In his view:

Well, the best example is that, suppose that here's a very large transaction fee, something like a 1000 Bitcoin. This happens when somebody has a glitched client, and accidentally makes a transaction that has no transaction outputs. Then the total balance of the transaction would be a reward to a miner. That means that if you're the winner of this block, then you get this 1000 Bitcoin reward from that awesome transaction that just gave you this huge fee. Normally a Bitcoin reward is just 25 Bitcoin per block. So if you are the lucky winner of this particular block, you get an unusually huge amount. If someone else wins the block (your chance of winning any particular block is pretty small, right?), then they get that enormous fee not you, so if you follow the first rule of mining, as soon as someone finds a winning answer, you say "oh they have the lower block, they win the fee. I'll just build on theirs" that's what altruistic behaviour would be. But in this case, rational behaviour would be: Screw them. I'm going to win this block for myself. I'm not going to mine on the longest block chain. I'm going to mine on the one before that. Now I have a chance to win this large transaction. And if you're get really lucky, and you're able to somehow win, e.g. the next two blocks in a row, or you're somehow able to circulate your version of this block faster than the other guy's able to convince everyone that it is his, then you would potentially be able to have that

extra chance of getting that huge fee, deviating noticeably from the protocol. And it's plausible to me that if there's rational mining software – there isn't any rational Bitcoin mining client that you can download right now – but I can just imagine that it's plausible that someone will make one of those at some point especially if Bitcoin catches on, and more people with money care about Bitcoin, and someone will build an optimized nonaltruistic Bitcoin client, then this nonaltruistic Bitcoin client would deviate in a systematic way, which is that if there's a really large bit reward, then all the rational clients will reveal themselves, because they will stubbornly keep fighting over that same block.

Last summer, an unknown user accidentally paid 200 bitcoins as a transaction fee to ASICMiner, a large mining farm in China.⁷⁴⁹ If such an occurrence, a black swan event happened such as what Miller hypothesized, would developers or pools or both be under pressure to fork the code and roll back the transaction?

Payola

Virtually every technical challenge that Bitcoin has in this study involve something related to its code base, all of which can be arbitrarily changed.⁷⁵⁰ Yet in practice this cannot happen because of the sunk costs and lobbying by stakeholders.

This then dovetails into a question another friend recently asked me, “Will every failure of a bitcoin business be blamed on incompetent operations rather than the underlying structural problems?” If the answer is yes, then not much has changed since the previous financial bubbles. One ongoing, tangential solution for many seems to be, to keep changing the name and denomination of units to tweak the marketing for people into buying the tokens whereupon the price is driven back up. If that eventually wears out, it could have laid the precedence for printing more under the guise of divisibility.

While these topics will continue to be debated, there are at least two more questions which need to be addressed at some time: should new denizens of this space follow adopters, many of whom have not disclosed their financial attachment to bitcoin? Is skepticism not warranted for a space rife with conflict of interest, such as adopters with a vested interest in bitcoin, pushing for more adoption solely for the subsequent price bump?

For instance, in July 2014, Tom Buttercoin (a pseudonym) created a new email address and subsequently emailed dozens of cryptocurrency news sites with the following message:⁷⁵¹

Hi!

I'm working on a new Bitcoin exchange that will be launching soon and we are looking to get some coverage. I was curious if we could pay and have your site feature us in an article?

Anthony

What he uncovered are more than a handful of websites willing to pay-to-play, or as it is referred to in the music industry: payola.⁷⁵²

While his investigation is ongoing a rough facsimile to describe this scenario is thusly: imagine that 20 GMC employees each started their own GMC fan club, fan forum and fan convention.⁷⁵³ Because the employees own equity in GMC they may have incentive to pump positive stories about the auto industry and GMC in particular. What the digital currency community needs is more investigative journalists and fewer ideologues whitewashing negative news about scams or centralization vulnerabilities – or in short, a Consumer Reports or Yelp for cryptocurrency.⁷⁵⁴

An accidental mania

For balance, Galbraith is likely overly negative on his account of bubbles involving new technologies. Despite the capital misallocation and hyperbole, at the end of the day sometimes there do end up being a few practical uses for some of the new technology and new human capital that the bubble helped finance (e.g., dark fiber). Consequently, bitcoin (the currency or commodity) may be closer to the dotcom boom than to the Chinese property market.⁷⁵⁵

It should also be noted that despite the critical analysis above, Bitcoin does not meet the definition of a Ponzi scheme. In July 2014, the World Bank published a paper on financial frauds and characterized Bitcoin as an accidental Ponzi:⁷⁵⁶

One can buy Bitcoin the way one can buy euros and trade freely with others having euros. Trouble started when people began speculating that the value of Bitcoin would rise, thereby raising the demand for Bitcoin and making the value-rise a self-fulfilling prophesy. In other words, what we witnessed recently in the Bitcoin phenomenon fits the standard definition of a speculative bubble

Contrary to a widely-held opinion, Bitcoin is not a deliberate Ponzi. And there is little to learn by treating it as such. The main value of Bitcoin may, in retrospect, turn out to be the lessons it offers to central banks on the prospects of electronic currency, and on how to enhance efficiency and cut transactions cost.

In the future, data driven firms will begin to look at blockchain activity, correlate it with a variety of edge-cased variables and will be able to advise their clients on what trends are taking place. And there are companies like Coinalytics and Coinometrics that are beginning to provide these resources and analytics to investors. The Cliff's notes version of what is happening can be found in chapter 4. Incidentally, there may be a reflation of the boom-bust bubble down the line because of “BitLicenses.” If that is the case, it may just be a matter of time until Galbraithcoin is minted – or maybe we should just wait for its fork, Galbraithmaniacoin.

Navigating these issues could just be a matter of growing pains, perhaps as the industry matures there will be less friction in these areas. The next chapter looks at the security to commerce ratios and some of the new innovations on the blockchain.

Chapter 14: Separating activity from growth on Bitcoin's network

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

Let us put that aside for a moment and consider ways to estimate real commercial volume. Are there any other ways to do so besides a full traffic analysis? This chapter will look at some of the costs to secure the on-chain activity of this commerce.

Sell side pressure

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

As noted in the previous chapter, in late May 2014, BitPay announced that it was processing about \$1 million in daily payments.⁷⁵⁷ It is unclear what amount of bitcoins that constitutes, depending on the time frame and therefore price levels (early December or the month of May) it could represent 1,000-2,000 tokens per day.⁷⁵⁸

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

This puts pressure on the sell side of the price equation. To minimize exposure to volatility, nearly all merchants elect to immediately convert bitcoins into fiat and those bitcoins are sold onto the market (both Ben Edelman and David Evans have written on this before).⁷⁵⁹

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

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

Thus altogether, in theory, there may be a regular 10,000 – 15,000 bitcoins representing commerce that are sold daily on the market today. It also bears repeating that, although technically the miners receive money, virtually all of it is spent towards utility (electricity) and hardware, not on the bitcoin ecosystem itself.

Is there a chart that shows this amount of transactions?

In chapter 4, I mentioned Total Volume Output – the total value of all transaction outputs per day – yet this includes coins which were returned to the sender as “change.” Recall that a bitcoin is comprised of unspent transaction outputs (UTXOs) and when used as the input of a

new transaction, it has to be spent in its entirety. Consequently, if the value is higher than what has to pay, the wallet clients generates a new address and sends the difference back to the address, as “change.” Thus the real number trying to be measured is substantially less. And taken to its maximum readings, roughly 1,000,000 bitcoin outputs (UTXOs) are used each day.

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

What is the real economy?

While the debate over what percentage of bitcoins are being spent in positive-sum activities, between October 15 and December 18 of last year, 41,928 bitcoins were sent to addresses controlled by Cryptolocker (a type of malware) – this is not real economic growth, in fact it is negative-sum.⁷⁶⁰ And as noted in chapter 12, because it signaled to the market that it was a successful way of generating (stealing) wealth, there are numerous copycats using similar methods (including CryptoDefense and Cryptolocker 2.0).

The cost of information security

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

What this actual activity translates into is the following:

Miners are the labor force that secures and processes transactions. The cost for their services amounts to roughly \$2.3 million per day (3,600 bitcoins X \$650 per bitcoin).

In practice however, most miners are operating at losses. For instance, according to a recent report from the National Science Foundation (NSF), a now-banned researcher used, “about \$150,000 worth of NSF-supported computer use at the two universities to generate bitcoins worth about \$8,000 to \$10,000.”⁷⁶¹ The researcher externalized the real costs of mining (energy and capital depreciation) onto another party (the NSF and therefore taxpayers). This is inefficient, yet there are many cases of such activity taking place each day, all of which collectively adds up. As Senator Dirksen might say, a gigahash here and a gigahash there, and pretty soon you're talking real money.⁷⁶²

Thus while the Bitcoin ‘trust fund’ (a more accurate description for the network which divvies out a finite amount of block rewards) pays out security of \$2.3 million each day, the labor force is providing significantly more security than they are being paid, probably closer to \$6 - \$7 million if not more.⁷⁶³

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

For comparison, MasterCard spent \$299 million on their capital expenditures in 2013.⁷⁶⁴ As part of these expenses, it builds data centers similar to the “fortresses” (with moats) that Visa has also built.⁷⁶⁵ In 2013, MasterCard and Visa processed a combined \$7.4 trillion in purchases.⁷⁶⁶ Together with American Express and Discover, these four companies generated \$61.3 billion in revenue during the same period.

While this is not an entirely apples-to-apples comparison, what this means is that the Bitcoin network is enormously oversecured compared with other transactional platforms. This is because it is decentralized which creates overhead (since all the nodes have to process and verify the transactions). Yet, as shown with GHash.io in June 2014, the network is qualitatively insecure due to economies of scale. That is to say, so as long as the proof-of-work mechanism can be economically scaled, this leads towards centralization. No amount of white papers or tweets will change that.

If the labor force of bitcoin is spending \$10 million on protecting the network yet real commerce is only \$30 million, this would be equivalent to a mall issuing 1 out of 3 customers a personal security detail to go shopping. Or in other words it is, arguably, quantitatively oversecure (it is not qualitatively trustless as shown by the trifecta of DeepBit, BTC Guild and GHash.io).⁷⁶⁷ Perhaps this mix will change over time.

However one thing to consider is that some advocates contend that the Bitcoin network will one day supplant and compete head on with PayPal and even Visa. In order to do so, the Bitcoin labor force are still (assumedly) being paid a fixed income (the marginal revenue) to provide the same services (hence why marginal cost always approaches that figure). Thus perhaps in the future, the opposite will occur – the network could become undersecure due to *disproportional* rewards as noted in chapter 8.

I spoke with Greg Simon, founder and CEO of Salpas, who worked as head of International Equity Sales for JP Morgan in Japan.⁷⁶⁸ According to him,

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

If miners are the equivalent of Japanese banks perhaps there other challenges related to marginal revenue (which is fixed) as well.

Will colored coin extensibility throw a wrench into the automated information security costs of Bitcoin?

Is there an economic flaw of proof-of-work as it relates to security? For instance, on most cryptocurrency chains the asset value of the chain has to be proportional to the proof-of-work otherwise this could lead to an economic incentive to attack the chain. Compounding this issue are new financial instruments such as metacoins, colored coins and smart contracts that can be exchanged on the same chains and unquestionably increase the enterprise value of the chain, yet which do not proportionally incentivize security beyond the existing seigniorage subsidy.

Are there any other areas of asymmetric, unbalanced security?

Colored coins, metacoins, smart contracts and user-created assets are buzzwords trumpeted by many cryptocurrency enthusiasts this past year. Considerable publicity has been dedicated to new functionality which promises to expand the extensibility of cryptoprotocols to go beyond tracking ledger entries for just one specific blockchain-managed asset (a coin) and allows users “colored” tokens to represent cars, houses, commodities, stocks, bonds and other financial instruments and wares. In March 2014 I even published a short book about these groundbreaking possibilities.⁷⁶⁹

For example, there are several colored coin projects currently in beta that allow users to take a fraction of a bitcoin, such as 0.001 BTC and “color” it “blue” (or any other arbitrary color) which represents say, a specific make and model of an automobile like a 2010 Camry LE. The user can then transfer that asset, the title of the Camry, along a cryptolledger (such as the Bitcoin network) to other individuals. Instead of having to transfer tens, hundreds or thousands of bitcoins in exchange for a good or service, users can instead exchange and manage entire asset classes in a trustless, relatively decentralized framework.

However, in this model the labor force providing security has no incentive to consume more capital or create additional hashrate just because the market value of colored coins is in excess of the uncolored value (since the value of miners’ new coins will be solely based on uncolored exchange value). Just because social conventions on the edges of the network add value perceptions to the network, based on the current code, miners do not automatically receive any additional value for providing that security. In effect, users of these metacoin platforms have access to security guards even if they do not directly pay for it.

So we should ask: does this raise the risk of a double-spend? Perhaps, because more hashrate is required for a proof-of-work blockchain with additional color value transactions on the chain. Yet, there is no automatic mechanism to reward this additional labor leading a (remote) possibility of having to remove some Script’s altogether.⁷⁷⁰ Script is the built-in scripting

language used for creating and customizing transactions and should not be confused with “script” the hashing function used in Litecoin and Dogecoin.

The gap between mining value and enterprise value

For instance, assuming this colored coin technology works and is adopted by 1,000 people the following scenario could take place. The total market value of a block reward (currently 25 bitcoins) is roughly \$12,500 (or \$500 per bitcoin), thus *ceteris paribus* the labor force is only spending \$12,500 every 10 minutes to secure the blockchain (in practice it is a lot more, there are several exceptions). One such exception is the expectation of token value appreciation – that is to say that if Bob the miner believes that a bitcoin’s value is \$1,000, but the price is currently \$500, Bob is still willing to expend up to \$1,000 for mining each bitcoin, discounted by his internal calculation for the probability that bitcoin will rise to that price.

However, if colored coins are adopted and used via the built-in scripting methods, there is potential for a seemingly unlimited amount of assets to be traded on the Bitcoin network. If these several thousand colored coin users add additional value, this creates an incentive for attackers to attack the network through colored coin-based double-spending attacks.

For example, where each of these 10,000 users places the title of a 2010 Camry each valued at \$10,000 that would theoretically add \$100 million in value that the network is transferring, but for which miners are not being proportionally rewarded or paid to secure those assets. As a consequence, over time as tens of thousands of assets – and functionality – are added to the network, the gap between mining reward value and enterprise value widens which creates a vulnerability, an economic incentive for criminals to use hashrate to attack the network. A rogue attacker could sell an asset and build a competing tree (consensus in Bitcoin is based on whatever is the longest tree of blocks).

After a successful 51% attack, the rogue attacker could then broadcast a fake chain built without the corresponding asset, having switched it out thus effectively double-spending. And if the total value that the network is transacting is at least twice as much as bitcoin value is, then there is a financial incentive for rogue participants to attack the network. The impact of a successful attack involves a lot of speculation and will likely continue to provide researchers many more volumes of conjecture and modeling.

Money for nothing

This scenario raises the question: what then is the potential divergence in value between bitcoin the currency and bitcoin the network (which can transfer and protect other data)? This issue only presents itself now as, previously, only bitcoins – and no other apps, assets or instruments – existed on the network. This gives rise to a coordination problem because miners would have to also keep track of the color, keep track of the exchanges the color is being traded on, and keep track of the settlement price (if there is such a thing) so that they could adequately gauge market clearing prices and readjust the coinbase reward every 10

minutes. Again, even if this coordination problem is solved the seigniorage reward does not increase – the current fixed income does not reflect the actual value being transacted on the network. So colored coins on a fully decentralized network could end up on an *undersecured* network of their own making with the only solution: recode the block rewards based on the value of the color and this presents a number of technical and social engineering challenges. In some ways this issue is related to the hypothetical economic disconnection between blacklisted and whitelisted tokens (due to Coin Validation) – a blacklisted token would be sold for less than what a whitelisted token would sell for.⁷⁷¹

A follow-up question that the community will likely debate is: Why wouldn't the value of a bitcoin increase as items of value are transferred on the blockchain via colored coins or another protocol, such that the miner's block rewards would adequately compensate the miners?

According to Preston Byrne, a securitization attorney in London, the answer to this is “that the value of bitcoin used in a colored coin transaction does not need to bear any relationship to the value of the associated asset – the network is being used to transmit information, and that information represents rights, and is the rights – not the token – which are valuable.” If the price of bitcoin does not adequately incentivize the miners, then there will be a difference between value of a bitcoin and the network and then some entity will have to step in to compensate for that difference. Whether collective action is sufficient to provide this compensation is currently unknown but there are coordination problems inherent in this model that would make this difficult.

In contrast, in the Ripple protocol, sidechains and perhaps even a proof-of-stake system could probably alleviate at least this specific concern. These alternative consensus mechanisms have one advantage to hash-based proof of work systems like Bitcoin, at least for the transfer of non-crypto value (i.e., colored coins). For instance, Ripple's distributed consensus mechanism allows users to exchange assets via gateways without needing to proportionally incentivize the security labor force. This is not necessarily an endorsement of this particular platform, rather it serves as examples of how it is immune to that particular attack vector.

Alternative approaches to network security

I reached out to several experts for their views on this issue. According to Robert Sams, co-founder of Swiss Coin Group and Cryptonomics:⁷⁷²

One of the arguments against the double-spend and 51% attacks is that it needs to incorporate the effect a successful attack would have on the exchange rate. As coloured coins represent claims to assets whose value will often have no connection to the exchange rate, it potentially strengthens the attack vector of focusing a double spend on some large-value colour. But then, I've always thought the whole double-spend thing could be reduced significantly if both legs of the exchange were represented on a single tx (buyer's bitcoin and seller's coloured coin).

The other issue concerns what colour really represents. The idea is that colour acts like a bearer asset, whoever possesses it owns it, just like bitcoin. But this raises the whole blacklisted coin question that you refer to in the paper. Is the issuer of colour (say, a company floating its equity on the blockchain) going to pay dividends to the holder of a coloured coin widely believed to have been acquired through a double-spend? With services like Coin Validation, you ruin fungibility of coins that way, so all coins need to be treated the same (easy to accomplish if, say, the zerocoin protocol were incorporated). But colour? The expectations are different here, I believe.

On a practical level, I just don't see how pseudo-anonymous colour would ever represent anything more than fringe assets. A registry of real identities mapping to the public keys would need to be kept by someone. This is certainly the case if you ever wanted these assets to be recognised by current law.

But in a purely binary world where this is not the case, I would expect that colour issuers would "de-colour" coins it believed were acquired through double-spend, or maybe single bitcoin-vs-colour tx would make that whole attack vector irrelevant anyway. In which case, we're back to the question of what happens when the colour value of the blockchain greatly exceeds that of the bitcoin monetary base? Who knows, really depends on the details of the colour infrastructure. Could someone sell short the crypto equity market and launch a 51% attack? I guess, but then the attacker is left with a bunch of bitcoin whose value is...

The more interesting question for me is this: what happens to colour "ownership" when the network comes under 51% control? Without a registry mapping real identities to public keys, a pseudo-anonymous network of coloured assets on a network controlled by one guy is just junk, no longer represents anything (unless the 51% hasher is benevolent of course). Nobody can make a claim on the colour issuer's assets. So perhaps this is the real attack vector: a bunch of issuers get together (say, they're issuers of coloured coin bonds) to launch a 51% attack to extinguish their debts. If the value of that colour is much greater than cost of hashing 51% of the network, that attack vector seems to work.

In other words, while these new financial instruments could technically be exchanged in a trustless manner, the current protocol cannot automatically incentivize their protection or account for their enterprise value, the equivalent of using a mall security guard to protect Fort Knox. While miners may be able to protect against amateurish shoplifters or even unorganized cat burglars, once organized criminals calculate and realize that one "color" asset is worth the economic effort of attacking the vault they may try to do so.

And because the blockchain is public and color assets could be known to the world-at-large, taking the Fort Knox analogy further, this would be like a mall cop standing in front of the contents of Fort Knox piled up on an open field (or behind a see-through glass vault). It is an

attempt to guard the Crown jewels not in a fortress with armed guards, tanks and turrets, but with Paul Blart.

On this point, Jonathan Levin, co-founder of Coinometrics explained that:⁷⁷³

We don't know how much proof of work is enough for the existing system and building financially valuable layers on top do not contribute any economic incentives to secure the network further. These incentives are fixed in terms of Bitcoin – which may lead to an interesting result where people who are dependent on coloured coin implementations hoard bitcoins to attempt to and increase the price of Bitcoin and thus provide incentives to miners.

It should also be noted that the engineers and those promoting extensibility such as colored coins do not see the technology as being limited in this way. If all colored coins can represent is 'fringe assets' then the level of interest in them would be minimal. Time will tell whether this is the case. Yet if Bob could decolor assets, in this scenario, an issuer of a colored coin has (inadvertently) granted itself the ability to delegitimize the bearer assets as easily as it created them. And arguably, decoloring does not offer Bob any added insurance that the coin has been fully redeemed, it is just an extra transaction at the end of the round trip to the issuer. That is an implicit negative for investors and users.

This raises some concerns in the future, if a party had the ability to invalidate Bitcoin accounts based on their own criteria that the miners might gain an influence over the colored coins and may bias various aspects of the economy incentivized through some kind of backchannel payment. For instance, BitUndo is a new "double spending as a service" project that is trying to do just that, provide a way for users to send transactions to a mining pool in an attempt to reverse transactions something that has created a flurry of reactions in the community.⁷⁷⁴ In the end, colored coins ends up being expensive through imposed TX fees, and thus becomes less attractive to issuers and users.

According to Alex Mizrahi, lead developer of Chromawallet a colored coin project:⁷⁷⁵

It is true that currently block subsidy has a significant impact on network's security, but it is not meant to work this way in the long run.

We'll go through 5 subsidy halvings in next 20 years, at that point block subsidy will be around 0.78 BTC. Reward miners get from fees is already on that scale (e.g. 0.134 BTC) even though blocks aren't full yet.

So transaction fees are going to play bigger role than subsidy. And value of those fees is linked to usefulness of transactions (i.e. value of those transactions) rather than to exchange rate.

Colored coins increase incentive to attack, but they also increase usefulness of transactions, thus it isn't clear whether they will have negative or positive impact on network security.

A couple other comments: "Script" is not required for colored coins, they work with very plain bitcoin transactions too. The incentive structure for bitcoin mining sucks from security perspective anyway, so I hope we'll eventually upgrade to a better protocol (e.g. including proof-of-stake) regardless of colored coin woes. And merged-mined sidechains will have even worse problems unless they are 'hardened' in some way.

Another way of looking at it is what attorney Preston Byrne explained in an interview with *Epicenter Bitcoin*:⁷⁷⁶

From a political perspective, I'm aware that a lot of Bitcoiners are of the view that Bitcoin will democratise finance. That may be, but I think that a lot of Bitcoiners are also of the view that more people using Bitcoin will drive up its price.

Smart contracts are quite agnostic in a sense that you don't have to pin yourself to any one protocol to get the utility and then capitalise that utility at a later date... in a sense they're very fair, because you can set up this architecture and people will be charged very little to use it. They can transfer value by writing new contracts on top of it really in any way they wish.

So it's a platform that doesn't necessarily benefit early adopters in the form of a rent, which Bitcoin admittedly does, but offers much of the same utility, and in fact offers considerably more utility than Bitcoin. I'm surprised a lot of people don't see that.

In this example Byrne could use a metacoin or colored coin of some kind to represent such a contract and as he noted, no rent is earned for this instrument or transaction because the current blockchain cannot natively segregate or distinguish one uncolored coin from a colored one.

I also contacted Jack Wang, founder of Melotic and co-founder of Bitfoo, a hosted wallet that was the first to implement proof-of-reserves. In his view:⁷⁷⁷

The security of the network depends on the aggregate hashing power. In one method of implementation, if Colored Coins could pay just one pool, say Eligius, extra to prioritize their transactions, but Eligius had only, say 25% of the network power, then the rest of the network could collectively decide to exclude the blocks that Eligius mined. This makes some sense to me since Eligius itself couldn't secure the network, yet is the only pool extracting the extra value out of Colored Coins. Colored Coins would need to distribute the extra rents to at least 50% of the network, and unless this lies within one pool then this is a danger to the Bitcoin network, but if it is 2 or more, this requires coordination and introduces potential holdout problems.

A more natural way to implement this would be that colored coins users would pay higher transaction fees on their own so that any and all miners that included those transactions in their blocks would get more fees. But unless those fees are mandated by colored coins, what is the incentive for individual colored coins users to pay extra?

Ray Dillinger, who interacted with Satoshi Nakamoto on the original Bitcoin announcement list and who is still actively providing commentary in the community, independently observed a similar problem as the experts above:⁷⁷⁸

Colored Coins etc. make it much harder to know how much value we need the blockchain to protect. The fact that these values are essentially “hidden” from the protocol means we can’t tell what we need to do to maintain any kind of parity with them.

One popular (and possibly correct) view of things is that in the long run the cheapest available price of electricity times the amount of electricity spent per block, will approach the value of the block reward in a PoW system.

Right now we have a Bitcoin block reward worth approx. \$12000. If this view is correct, we should expect, worldwide, to see about \$12000 worth of electricity (increasingly concentrated where electricity is cheapest) expended per block by hashing rigs.

Right now transaction fees are providing a very small percentage (one third of one percent? I think?) of the block rewards.

At some point in the future, moving to transaction fees as a primary source of mining revenue, implies that each kilowatt-hour of electricity invested in securing the blockchain will have to secure three hundred times as much value (relative to its own value) from attack as it does now.

I’m convinced that’s not really enough. If we stick with Proof-of-work, we’re going to have to start charging transaction fees based on how much value is changing hands, because we want to buy security proportional to the value we’re trying to secure, not proportional to the amount of space it takes to store the transaction. And that means the amount of value changing hands has to be visible, and that therefore Colored Coins etc will have to be more ‘transparent’ in terms of the protocol knowing how much they’re worth (and therefore how much security we need to buy to keep them secure).

There is at least one more economic and legal issue that Robert Sams foresees: what about ill-gotten performance of the 2.0 metacoin and digitized financial instruments? That is to say, in the event that sidechains, colored coins or other secondary protocols attached to Bitcoin begin issuing financial derivatives or even something as simple as a dividend, what happens in the event of theft?

For instance, on July 12, 2014, Coinprism (a colored coins project) announced that it now supports dividend functionality.⁷⁷⁹ What if Bob's colored coin representing a stock was stolen by Alice, does the company issuing the dividend still pay it? If yes, then this opens up the company to lawsuits, and if no, then Bitcoin (the protocol) ceases to function as a decentralized ledger, as the protocol would need to verify the identity, taking away the anonymity behind it. Currently, there is no way to do this on Bitcoin itself today without a major code rewrite and change in the social contract.

Yet a 51% attack is not necessary to double-spend even in the scenario above. An attacker can force a large reorganization with some probability with less than 50% of the network hashrate.

Greg Maxwell, a Bitcoin core developer, created a probability of attack success calculator that illustrates the concern of one entity having more than 40% of the hashrate and its ability to successfully conduct a double-spend attack:⁷⁸⁰

- 40% of hashrate, successful probability of ~50%
- 49% of hashrate, successful probability of ~96%
- 51% of hashrate, successful probability of 100%

And a 51% attack does not always involve double-spends, it does allow Bob to fork from any block and win 100% of the time, or just ignore the rest of the blocks created and generate 100% of the blocks for himself.

Will transaction fees alone be able to support Bitcoin? Maybe not. A miner may try to double-spend \$40 billion when the network is only secured by \$20 billion in rewards. With block subsidies, there is a constant 25 bitcoins of rewards securing the network. During periods of low block-space demand and low fees, miners may opt to make their money through double-spending. Perhaps the variance in transaction fees will be too high, but if it is, ideas such as demurrage to reward miners may be enacted upon; a "prohibited change" to Bitcoin, though as some have argued, it may be necessary to keep Bitcoin alive.⁷⁸¹ This is a challenge that sidechains will need to cover immediately since the majority of them will not have a subsidy.⁷⁸²

This is not necessarily an issue that the community needs to fret about yet as very few financial instruments are trading on the Bitcoin blockchain in this manner and because BitLicense compliance is a much larger issue. However, *ceteris paribus*, it is a real issue that developers and miners will continue to talk about and reflect upon over the next couple of years.

Towards a more functional future

While this is a speculative issue, what is knowable is that the economics behind it are built into these protocols. What is also known is that some proposed solutions should be easier to implement than others. For instance, Bitcoin developers could fork the code and create a proof-of-stake ledger proposed by Stephen Reed.⁷⁸³ Alternatively, because this new extensibility could create fungibility issues, a different – and admittedly impractical – solution might be for

mining pools to utilize a trusted Oracle data feed to colored coin exchanges and adjust mining rewards accordingly. Perhaps removing scripts entirely, implementing tree chains or relying on merged mined sidechains, instead, could alleviate this potential pain point as well.

What is definitely known is that market participants have an existential incentive to keep miners mining and not dropping off. If fees are floated users will likely pay higher transaction fees if they do not want miners to go elsewhere. While speculative, colored coins users could become the biggest payer of transaction fees, though in practice, most users do not like paying any fee.

Over the past several months this is an issue that Mastercoin and Counterparty developers have promoted: pay the miners higher fees for access to these new platforms because miners expect the value of these special transactions to go beyond the excess of bitcoin transactions. Miners could potentially auction block priority to these transactions over regular bitcoin transactions. One pool, Eligius, operated by Luke-Jr is already filtering out (or threatening to filter out) specific bitcoin transaction today.

The next chapter will look at the ramifications of losing the security to a network and the potential for a cascading collapse effect for any instrument on top of the network.

Chapter 15: What Altplatforms can teach Bitcoin

The key ingredient to the success of any decentralized public ledger, such as Bitcoin, is incentivizing its transactional network to simultaneously secure the network from attackers and process transactions. This chapter explores the impact of subsidies that are removed within such a system.

In the case of virtually all other cryptocurrency forks of Bitcoin this incentivization process is handled through seigniorage reward. For Litecoin this reward occurs roughly every two-and-a-half minutes and in Dogecoin, every minute. Consequently, these altcoins pay their labor force (miners) in the same method that the Bitcoin network does via a coinbase transaction to the miners address.

For some advocates, one of the purported advantages of cryptocurrencies is that their money supply creation rate is actually deflationary (or contractionary) in the long run. In the short run, Bitcoin's expansionary rate is high, with inflation at 11.1% this year alone. That is to say, it is a hardcoded asymptote, tapering off over a known time period. In the case of Bitcoin, the wage for the labor force (miners) is split in half roughly every 4 years (every 210,000 blocks), for approximately the next 100 years – until its money supply is exhausted at a final 21 million bitcoins. More than 13 million bitcoins have already been paid to miners.

With Dogecoin's 100 billion dogecoins, this process is accelerated, with the mining income dividing in half every two months. While it took about five and a half years for about 62% of bitcoins total monetary base to be distributed, as of this writing 89% of dogecoins reward (income) has already been divvied out to its workforce in less than 9 months.⁷⁸⁴

While this has frenetically fast money supply has provided a psychological motivation for early adopters to partake in the Dogecoin ecosystem, economic law suggests that this network could cease to exist in its current form within the next 4-6 months through a 51% attack. Though this may be mitigated with the 'AuxPoW' announcement discussed below. In addition to the aforementioned Coiledcoin and Auroracoin in previous chapters, several other coins that have been successfully attacked due to losing security include Feathercoin (several times), Worldcoin, Powercoin and Terracoin.⁷⁸⁵

The reason is simple: with every block reward halving (also called "halving day"), the labor force is faced with a 50% pay cut. The contractors (laborers) incapable of *profitably* providing hashrate at this level can and will leave the work force for greener pastures.

This same issue has impacted other altcoins in the past, such as the original MemoryCoin, which died after 9 months due to a combination of factors including diminished block rewards (it attempted to divvy out its entire monetary supply in 2 years).⁷⁸⁶ MemoryCoin has since relaunched and time will tell if the developers have incorporated the lessons learned from its original demise.⁷⁸⁷

In his paper, *On The Longest Chain Rule and Programmed Self-Destruction of Crypto Currencies*, Nicolas Courtois independently found that halving rates are detrimental to the security of a cryptochain, leading to what he calls “programmed self-destruction.”⁷⁸⁸

Table 1. The Unobtanium Reward

blocks	approx. dates	UNO/block
1 – 102K	18 Oct 2013-	1
102K – 204K	15 Dec 2013-	0.5
204K – 300K	12 Feb 2014-	0.25
300K – 408K	4 April 2014-	0.125
322,050	-today-	0.125
408K – 510K	5 Jun 2014-	0.0625
510K – 612K	1 Aug 2014-	0.03125
612K –	after 29 Sep 2014	0.0001

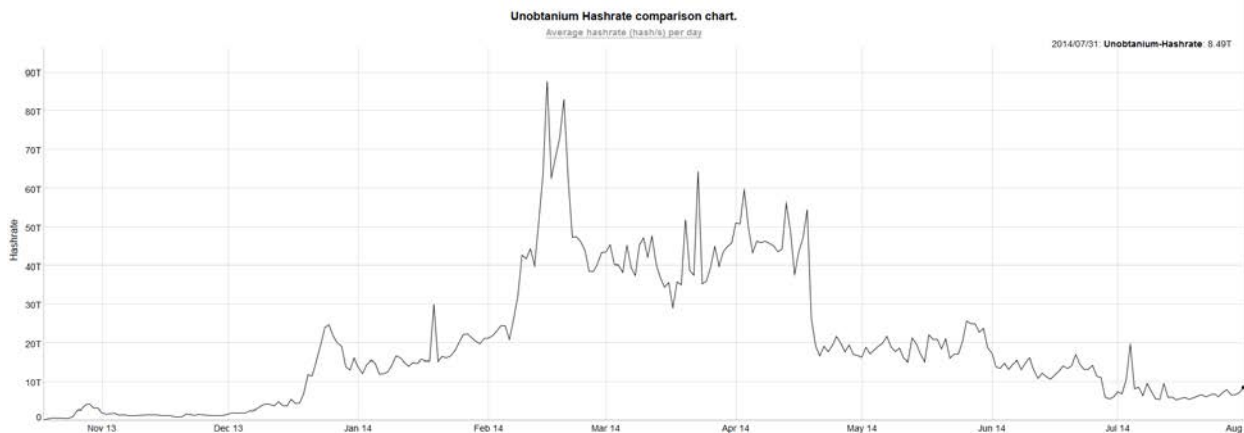
Source: Nicolas Courtois

One case-study is that of Unobtanium Coin (UNO). UNO was originally announced on October 17, 2013 and uses SHA-256d as its hashing function (the same that is used in Bitcoin). Only 250,000 Unobtanium coins will be minted with block halvings every 2.88 months.

With such a rapid decline in rewards (above) Courtois states that Unobtanium must “double or die” in order to incentivize miners:

When the next rewards block halving comes in April, the price of UNO needs to be at 12 USD in order to keep mining equally profitable (cf. later Theorem 11.1 page 46). Then in June it would need to become 24 USD, then in August it would need to become 48 USD. Such rapid appreciation at an exponential rate is unlikely to happen and the hash rate must decline accordingly, until mining becomes profitable.

Courtois explains the most striking change is that “after 29 September 2014 the miner reward is going to be divided by 312.5 overnight.” Based on the market value at the time of his writing he estimated that “UNO need to be 15,000 USD each to compensate for that again (or mining will not be profitable and hash power protection will go elsewhere).” Or in other words, without a 100% appreciation every 3 months this network is vulnerable to attack. In fact, on the final halving in September alone he estimates that the market value would need to increase 10,000% to incentivize the labor force to stay. Suffice to say, as shown in the hashrate chart below this trend has not occurred.⁷⁸⁹



Source: Bitinfocharts.com

While it is unknown when the network will be attacked by rogue miners, this again illustrates the need to financial incentives for security and longevity.

This is a similar observation, or rather prediction that Ray Dillinger explained in May 2014. In his view, an altcoin can survive if it has a number of properties including:⁷⁹⁰

It doesn't halve its remaining coin supply more often than it can double its value. That's kind of hard to predict, but at this point I think the double-value time for cryptocurrency is up to about a year, maybe two. It'll get longer until it catches up to double-value period for the rest of the economy, which is 7 to 15 years depending on the industry. This is important because whenever the block reward goes down, the hash rate goes down in the same proportion; and when the hash rate gets too low, the blockchain becomes vulnerable to an attack which can destroy its value completely. Expect any coin that mines out its coin supply too fast, to collapse. I think even Bitcoin is going to be too fast in the long run; there'll come a point when its double-value time is slower than its block-reward halving time and alts will start sucking up the hashing power making bitcoin vulnerable to attacks.

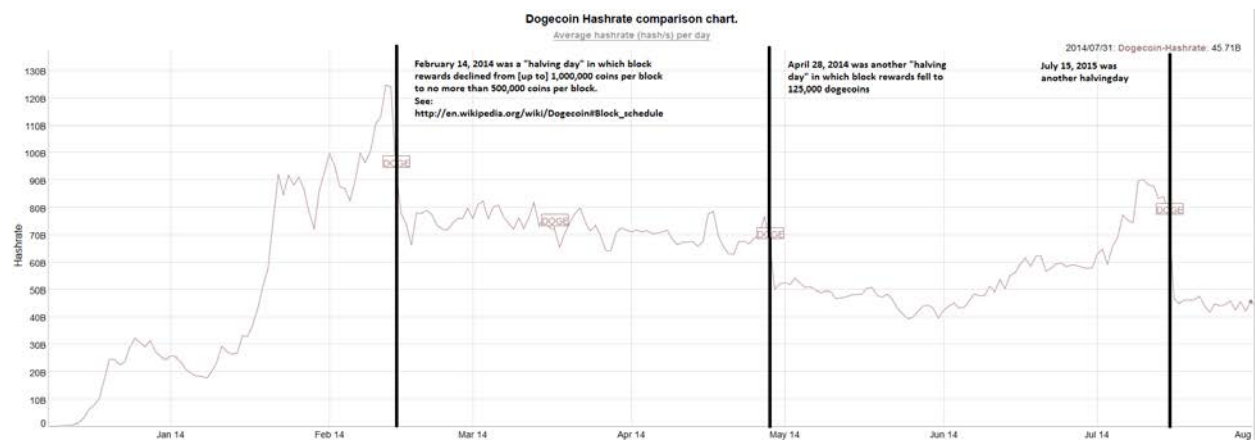
Unfortunately for Unobtanium adopters, the predictions of Courtois and Dillinger will likely come to pass as the market price has declined, as of this writing, to \$2.70 per coin.^{791 792}

Dogecoin

Early adopters of Dogecoin like to point to outlier events such as when the doge community funded the Jamaican bobsled team or sponsored NASCAR driver, Josh Wise, at Talladega or even a vaunted tipping economy (which is actually just faucet redistribution) as goal posts for dogecoins growth and popularity.⁷⁹³ Yet after three halving days the actual Dogecoin blockchain has lost transactional volume each month over the past seven months and the labor force has also left for new employment elsewhere.

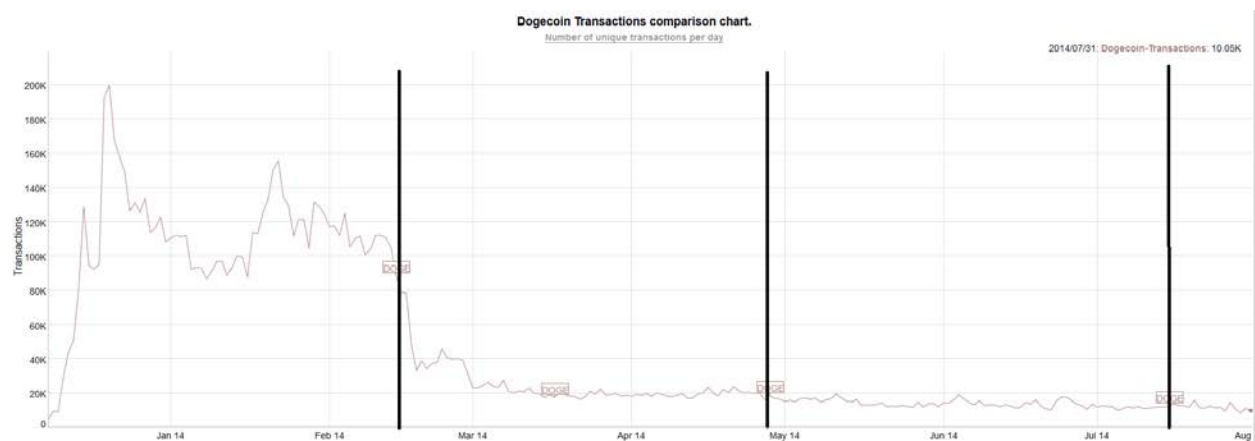
This is visualized in the following two graphs.

Chart 1:



Source: [Bitinfocharts.com](http://bitinfocharts.com)

Chart 2:



Source: [Bitinfocharts.com](http://bitinfocharts.com)

The first chart shows Dogecoin's collective hashrate. The black lines indicate when the "halving day" or rather "income-halving day" occurred. Because the price level of a dogecoin remained relatively constant during this time frame, there was less incentive for miners to stay and provide labor for the network. If token values increased once again, then there may be incentives in the short-term for laborers to rejoin the network. Yet based on this diagram, roughly 20-30% of the labor force left after each pay cut.

The second chart shows on-chain transactional activity. The first three months are erratic because of how mining pools (similar to lottery pools) paid their workforce (miners). Following the first halving day in February, the network transaction rate fell to roughly 40,000 transactions per day and then leveled off to around 20,000 until April 28, 2014. Another halving day occurred on April 28th and the subsequent transactional volume remained relatively

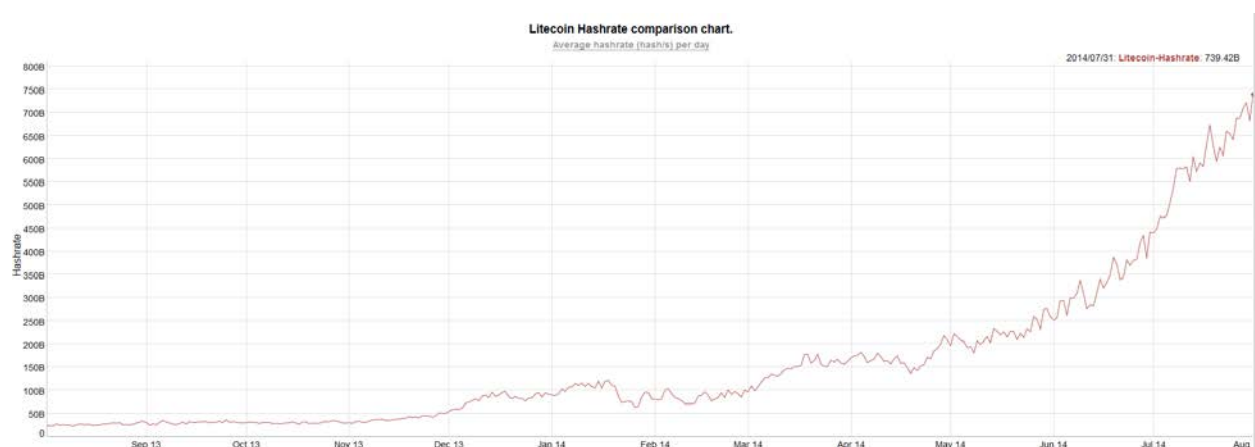
flat to negative. As of this writing it is 10,250 transaction per day, or roughly the same level it was during the first week of its launch more than seven months ago (most of it is mining payouts from pools).

Now some readers may claim that a lot of the transactional volume such as tip services and tip bots are being conducted off-chain and thus the total number of transactions is likely higher. And they would be correct. But that would completely defeat the purpose of having a blockchain in the first place – a trustless mechanism for bilateral exchange that negates the need for “trust-me” silos (as Austin Hill calls them). Also, while this topic deserves its own series of papers, there is little literature that suggests that tipping can grow an economy; it is *not* a particularly good signaling mechanism or way to cultivate a developing economy (i.e., China is not stagnating for lack of tipping activity).

However the key issue is this: if the trend continues and the network hashrate continues to fall 20-30% after each halvingday, then within the next 2-4 months it will be increasingly *inexpensive* for competing mining pools on other ledgers to conduct a 51% attack on Dogecoin’s network, destroying its credibility and utility.

For instance, the chart below is the Litecoin hashrate over the past year. Litecoin is Dogecoin’s largest competitor based on its proof of work (PoW) mechanism called scrypt:

Chart 3:



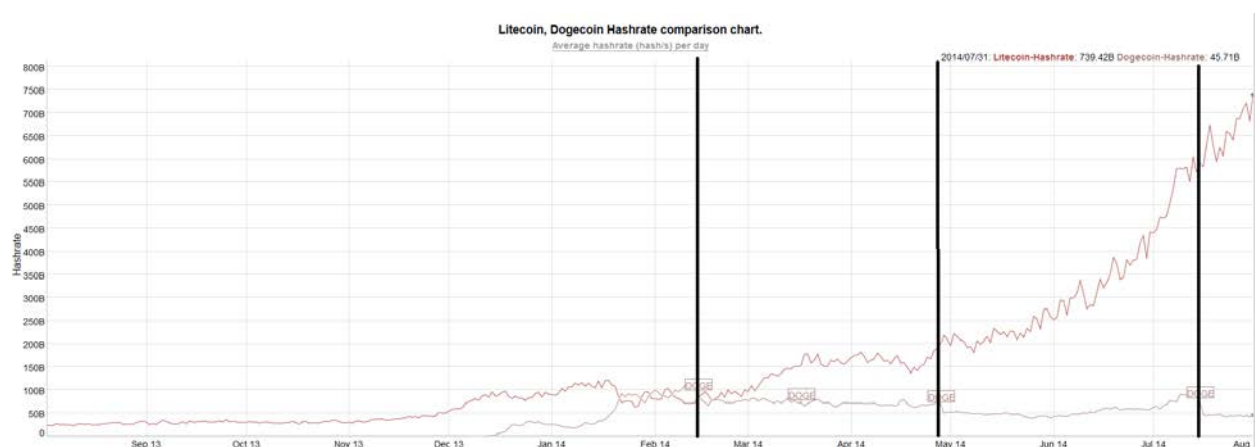
Source: [Bitinfocharts.com](http://bitinfocharts.com)

One of the reasons the Litecoin hashrate is not rising or falling at a constant rate but is instead jumping and down erratically is that miners as a whole are economically rational actors. When the cost of producing security is more than the reward (block reward income), the labor force turns towards a more profitable process such as another alternative scrypt-based “coin” (note: Bitcoin’s PoW method uses SHA256d whereas Litecoin and Dogecoin uses scrypt). The same phenomenon of hashrate jumping up and down occurs with the Bitcoin network.

For example, currently the Litecoin network has roughly 600 gigahashes/second versus the Dogecoin network which is roughly 45 gigahashes/second, roughly 1/13th the processing power of the Litecoin network. To conduct a 51% attack on Dogecoin today, an entity would need to control approximately 23 gigahashes/second. The current ‘market cap’ for Dogecoin is \$20 million, *ceteris paribus* on paper it could cost less than \$1 million in capital and operating expenses to successfully attack the Dogecoin network for an entire day.

For comparison, the ‘market cap’ of bitcoin as of this writing is around \$8.0 billion, roughly equivalent to the market capitalization of the Mauritius Stock Exchanges or Peruvian government bonds.⁷⁹⁴

Chart 4:



Source: Bitinfocharts.com

The chart above shows both the hashrate of Litecoin (in red) and Dogecoin (in grey) with the vertical black lines representing the dogecoin “halvingday.” What this shows is that while Dogecoin, for roughly one month in early 2014 was more profitable to mine than Litecoin, the halvingday led to an exodus of labor. Because both of these tokens utilize the script-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 script-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:



Source: Bitinfocharts.com



Source: Bitinfocharts.com

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 a larger 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.

Will dogecoin survive?

While the development team could theoretically switch its proof of work algorithm (to a cluster like X11 as used in Darkcoin), the doge community is really faced with six options:

- Merge mine. Namecoin was (and is) an independent blockchain, but since block 19,200 about 80-85% of its network hashrate (and block rewards) are tied to Bitcoin mining pools through a process called “merged mining.” Charlie Lee, creator of Litecoin explained how Dogecoin could be “merged mined” with Litecoin in a series of posts in April 2014.⁷⁹⁵

- Transaction fees. Both the development team and mining community could agree to float or raise transaction fees on the doge network (similar to what Mike Hearn has been discussing for Bitcoin).⁷⁹⁶ In practice however, even if approved, very little actual commerce (and therefore transactions) is conducted on the dogecoin network thus it is unlikely that this will compensate the large drop in mining income. Similarly, as Gavin Andresen pointed out in Amsterdam in May 2014, increased transaction fees reduces the participation rate (note: the actual transaction costs are much higher than stated, block rewards (token dilution) are usually not factored in).⁷⁹⁷
- Proof of stake. There are several variations of proof of stake. Whereas Bitcoin, Litecoin, Dogecoin and most other cryptocurrency experiments use a proof of work mechanism to protect the network from malicious entities, a proof of stake (PoS) system, such as that used in NXT, will randomly assign a “mining node” (called a “forger” a poor marketing term for sure) to process all the blocks for the next minute.⁷⁹⁸ Because all of the other nodes in the network know which miner to trust, this lowers the amount of infrastructure needed to protect the network. In theory this sounds amazing. In practice however, most proof of stake systems end up almost immediately centralized in one manner or the other (Andrew Miller, Andrew Poelstra and Nicolas Houy call it “proof of nothing”).⁷⁹⁹ Perhaps Stephen Reed’s Cooperative Proof-of-Stake can work in the future.⁸⁰⁰
- The market price of dogecoin increases, incentivizing the labor force to continue providing security of the network with the expectation that the tokens they are given in return for their labor will continually appreciate in value. This is betting on hope. Charlie Lee pointed out the uphill task this would require beginning next year when rewards fall to less than 1/10th of they are today, explaining in April 2014, “At Dogecoin block 600,000, only 10,000 coins will be created per block. So in order for Dogecoin to keep the same amount of security as today, Dogecoin price would need to go up by 25 times. And Dogecoin price would need to gain on Litecoin by 50 times in order to catch up on Litecoin's security. And assuming everything stays the same, the market cap of Dogecoin needs to reach \$1.5 billion by January of next year.”⁸⁰¹ For comparison, the ‘market cap’ of Dogecoin as of this writing is roughly \$20 million.
- Migration. Dogecoin could also migrate to a platform like Counterparty and become a fully secured atcoin with a dash of Proof of Transaction thrown in to inflate the coin with ongoing usage that this particular community likes to embrace.⁸⁰² It could be fully protected by the Bitcoin hashrate with no further need to try to acquire miners to protect it.
- Further experimentation. While it is unlikely the Dogecoin has the resources to create secure production code in the shortened time frame, Robert Sams

“growthcoin” and Ferdinando Ametrano’s “stablecoin” could provide a mechanism that enables the network to live on in a different manner.⁸⁰³

While all of these have been discussed at length, it appears that ‘AuxPoW’ will be attempted which is described below.

With that said, stranger things have happened. A rising tide supposedly lifts all boats and thus in the event that BitLicense approved exchanges in Wall Street come online later this year and new capital actually flows into Bitcoin and other alternative ledgers, perhaps similar speculative funding will flow into Dogecoin as well. However, this is not something that can be known *a priori*.

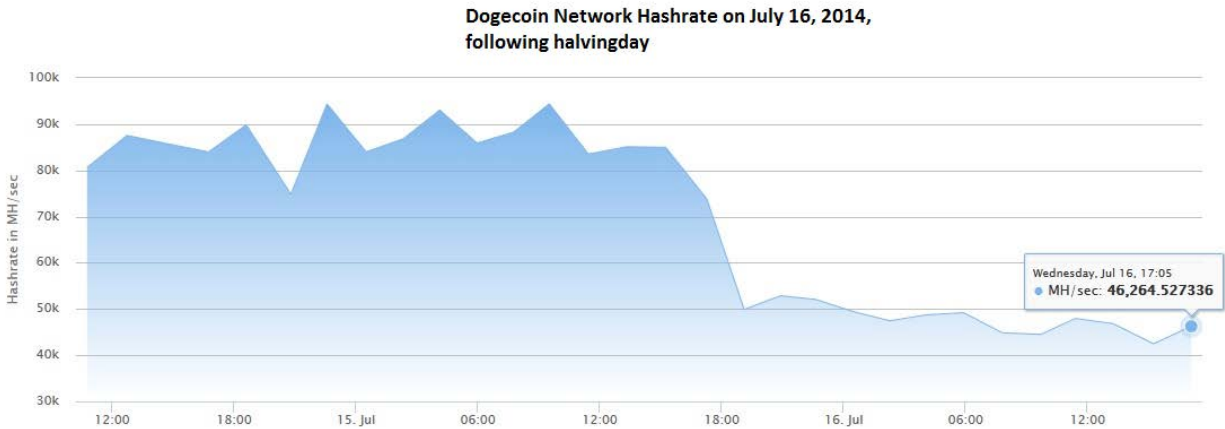
In May 2014, I contacted Jackson Palmer, creator of Dogecoin for his thoughts on the situation. In his view:

It is definitely a challenge that Dogecoin (and all current-gen crypto currencies) will face in the future. I’m very concerned about the impact of centralized mining and reliance on transaction fees could hold for Bitcoin as it becomes less enticing to mine - really, the network can be held at ransom to attach hefty transaction fees if the mining pools are cherry picking as they create blocks.

At the end of the day, I think the viability of cryptocurrency really hinges on a move away from PoW-based mining to something new and innovative that doesn’t just stimulate an arms race and put all the power back into the hands of the fiat-wealthy. I don’t have a solution unfortunately, but hopefully someone will find one and bring about a new generation of digital currencies in the coming 5-10 years.

That being said, cryptocurrency as a space is very unpredictable so it wouldn’t surprise me at all if Dogecoin beats the odds and overcomes these challenges in some weird, wacky way. It’s in the community’s hands, and they’re certainly passionate about seeing it reach the moon, as am I.

What has happened in the interim months? The Dogecoin development team worked on a number of other issues but was divided on how to handle this situation. As a result, the situation has been exacerbated with the July 15, 2014 block halving effectively removing 50% of the hashing rate as shown below:



On July 18, 2014, Charlie Lee once again brought up this issue the Dogecoin community:⁸⁰⁴

When I did my merged mining AMA, the dogecoin hashrate was about 1/2 of litecoin's hashrate. Today, the hashrate is 1/15 of litecoin's. Pretty much all the ASIC hashrate went to Litecoin, which I warned would happen. The Dogecoin's network security is in danger of being attacked. The top 3 Litecoin pools can easily pull off a 51% attack on the Dogecoin network. In a few weeks, the top 6 Litecoin pools can easily do it.

A Script ASIC farm can decide that it wants to have some fun. The Dogecoin network hashrate is about 45 ghash/s. So as an example, a 50 ghash/s farm can easily 51% it. Here's the earning ability of 50 ghash/s: [litecoin mining calculator](#). It makes about \$20500 per day. Let's say it takes about 30 minutes to pull off this attack... that's 30 Dogecoin confirmations. The attacker loses about \$430 if he stops mining Litecoin for an hour. They could try to attack one of the top Dogecoin exchanges and try to steal 0.7 bitcoins to make it worth their time. Or they can double spend a lifetime subscription to Hustler.com, which is worth about \$500. Or maybe they just don't like Dogecoin. And it only costs them \$430! Dogecoin's network security is worth only \$430.

What are the exact conditions for an attack? According to Lee, as of July 20, 2014:⁸⁰⁵

Not everyone is capable. The estimate is about 6 pools (and ASIC farms) has enough hashrate to do it. The reason not to is because they either:

- Don't think it's worth it to risk upsetting their miners (in case they are caught)
- Don't have the technical expertise to pull off the attack
- Aren't malicious

As the hashrate keeps dropping, the number of people that has enough hashrate will grow. And you will likely run across someone who has the technical expertise, is malicious, and will attack. It's not a matter of if but more of a matter of when. How low would the dogecoin hashrate need to be (relative to Litecoin) before someone does attack.

Lee's solutions are:

- Don't do anything and hope
- Do merged mining and try to convince all the pools to do it
- Switch to another algorithm, and hope you can compete better against other GPU mined coins
- Switch to proof of stake, and accept all the problems that come with that.

In late July, Tristan Winters interviewed a Dogecoin core developer, “langerhans” about this vulnerability and immediate solutions.⁸⁰⁶ According to langerhans:

A low hashrate is a threat for every Proof of Work based coin that doesn't implement special measures to mitigate possible attacks.

Dogecoin was brought to the market with an “expiration date” as the block reward schedule was made for about one year. That is basically the reason why we were already looking for solutions for quite some time.

The problem is that many of the solutions are either still highly theoretical or are deemed to be in an “Alpha” or “Beta” state. Some have technological issues, some have “political” issues.

After the venture of Litecoin's creator into the Dogecoin subreddit, it seems that the implementation of the so called auxiliary proof of work is the most discussed one right now. While my recent reddit post about this may have seemingly implied differently, I'm not against this concept from the technical perspective.

Yet, we still want to make sure that if this is considered to be the option to go with, there are no oversights of any concerns with it.

On August 3, 2014, the Dogecoin development team announced upcoming support for Auxiliary proof of work (AuxPoW), which enables merged mining.⁸⁰⁷

It bears mentioning that Dogecoin has not been attacked by any ASIC farm or pool. And while Dogecoin's security was becoming increasingly more vulnerable every two months, if pools do begin to adopt AuxPoW then this will likely extend the endurance of Dogecoin; likely at the expense of decentralization.⁸⁰⁸ With that said, so long as proof-of-work is still used in the manner it is today, the longevity of any chain is probably self-terminating.⁸⁰⁹

Compounding this tenuous hashrate vulnerability issue is the July 2014 launch of Dogeparty, a fork of Counterparty that uses Dogecoin as the backbone.⁸¹⁰ As noted in the 5th option above, Counterparty is a “2.0” platform that resides on top of the Bitcoin blockchain and enables users to create and exchange assets such as financial instruments. The problem however is that, as mentioned in chapter 14, Bitcoin miners are not incentivized to “burn” more capital or create more hashrate to protect these instruments. There is no financial incentive within the protocol

to reward miners for protecting Counterparty-based assets. As a result, these coins may be vulnerable to attack.

The same concerns are amplified with Dogeparty because it uses Dogecoin as its foundation. If Dogecoin sustains a successful 51% attack from a pool or farm, there could be a systemic failure – a cascading domino effect – by which interconnected instruments on Dogeparty are no longer accessible because the underlying network has been compromised. At the time of this writing it is unclear if or when this could occur.

Can this happen to Bitcoin?

One common refrain that some Bitcoin advocates have stated in the past is that Bitcoin does not have a similar incentives issue. As I have described in numerous articles and papers, this is false.

For instance, below is data from the Litecoin hashrate statistics database at Bitinfo Charts.⁸¹¹ The numbers expressed represent the collective hashing power of the Litecoin network:

- 576.8 megahash/s on November 25, 2012
- 572.62 megahash/s on November 26, 2012
- 578.92 megahash/s on November 27, 2012
- 687.47 megahash/s on November 28, 2012
- ——— Bitcoin Halving Day ———
- 1.11 gigahash/s on November 29, 2012
- 1.28 gigahash/s on November 30, 2012
- 1.14 gigahash/s on December 1, 2012
- 834.75 megahash/s on December 2, 2012

What we see here is that some (marginal) miners that were previously hashing on the Bitcoin network left and began providing their labor on a competing network (Litecoin) that was temporarily more profitable to them (or at least, what they may have seen as future profitability relative to their costs).

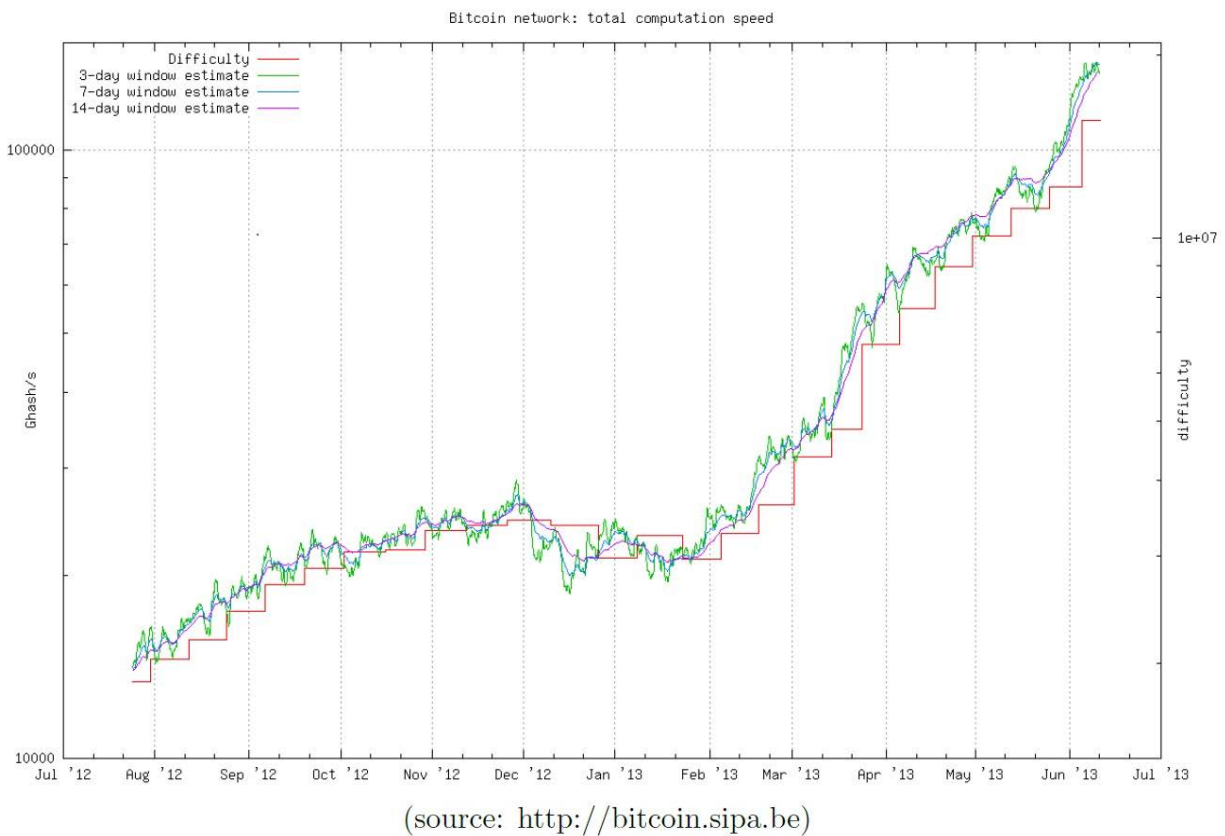
These were likely slower GPU-based miners as FPGAs were increasingly being acquired and used by larger Bitcoin mining farms. Remember, while there were some proprietary ASICs that were developed and used in this time frame, they were not available to the public at-large — the first ASICs that were sold to the public (from Avalon) did not come online till the end of January / beginning of February the following year in 2013.

Below are the corresponding dates on the Bitcoin network using the same database:⁸¹²

- 24.65 terahash/s on November 25, 2012
- 26.52 terahash/s on November 26, 2012

- 25.29 terahash/s on November 27, 2012
- 29.47 terahash/s on November 28, 2012
- ——— Bitcoin Halving Day ———
- 28.2 terahash/s on November 29, 2012
- 21.71 terahash/s on November 30, 2012
- 28.31 terahash/s on December 1, 2012
- 24.19 terahash/s on December 2, 2012

Below is the visualized network hashrate for the Bitcoin network following its first halving day on November 28, 2012:



The following two months, from December 2012 through January 2013, the hashrate stayed flat and in some weeks even declined.

There were at least three reasons why the network did not decline precipitously like Dogecoin:

- Despite the fact that very little real commerce actually takes place on the Bitcoin network, there was some amount that did in 2012 and does today (primarily gambling and trading of illicit wares). Thus there was external demand for the tokens beyond miners and tippers.

- The token prices rose creating appreciation expectations. The price rose from \$12.35 on November 28, 2012 to \$20.41 on January 31, 2012.⁸¹³ If miners believe and expect the price to increase in value, they may be willing to operate at a short-term loss
- The first batch of ASICs from Avalon shipped and arrived to their customers at the very end of January.⁸¹⁴ These provided roughly 2-4 orders of magnitude per watt in performance than the top competing FPGAs and GPUs. This is equivalent of miners being given sticks of dynamite instead of pick axes to tunnel through mountains.

While more research will be conducted and published in the following months before the next Bitcoin halving day (estimated to occur probably before August 2016), the Bitcoin network faces a similar existential hurdle, though perhaps less stark once more ASIC processes hit similar node fabrication limitations.⁸¹⁵ In the next couple of years there will no longer be performance gains measured in orders of magnitude. Since most participants do not like paying transaction fees, incentivizing miners to stay and provide security will likely be problematic for the same income reduction issues. This scenario will likely be revisited by many others in the coming years.

Nothing personal

From a marketing perspective Dogecoin has done more to bring fun and excitement to this sub-segment of digital currencies than most other efforts (remember, USD can also be digitized and encrypted). In turn it brought in a new diverse demographic base to blockchain technology, namely women. While some of the more outlandish gimmicks will likely not be enough to on-ramp the necessary token demand which in turn leads to token appreciation, this project has not gone unnoticed.

For instance, in early May 2014 I had coffee with a bank manager in the San Francisco financial district. As we were wrapping up he asked me to explain Dogecoin. I mentioned that what sets doge apart from the rest was its community was much more open towards self-ridicule, self-parody, less elitist and most importantly, women actually attended meetups.

He quickly surmised, “Oh, so it’s the wingman currency. It’s the friend you bring to the bar who is willing to look goofy to help you out.”

That is probably a fair enough assessment and it will likely need a wingman to survive.

Chapter 16: Potential alternatives and solutions

Now that we have discussed a host of opportunities and challenges within the Bitcoin ecosystem, this chapter will look at some of the alternative platforms currently under development.

For example, can Bitcoin be used as the connectivity between the world's financial systems?

In theory, yes. But so could dozens of other competing platforms that have lower operating costs.

In July 2014, Greg Brockman, CTO of Stripe, provided an overview of the current financial system and how there are numerous systems whose back ends could tie into Bitcoin.⁸¹⁶ This is possible, but unlikely for the reasons stated in the previous chapters.

For instance, Brockman states that:

This would not, of course, be the first global payments network. One obvious comparison is with PayPal. The fundamental advantage a Bitcoin gateway ecosystem has over PayPal is that it's open. Any closed network will, by nature, be deprived of structural pressures that force it to improve. A third-party can't improve a closed network; if they really want to, they first have to try to replicate the network itself from scratch. In contrast, the Bitcoin space is already seeing rapid iteration and compounding improvements.

This is incorrect. The evolution of Bitcoin's network has moved from openness to siloed, trusted entities that use Bitcoin in name only (BINO). In all likelihood, firms such as Coinbase (which seeks to be the PayPal of Bitcoin) are internally using the same hardware layout that companies such as PayPal do: a couple of secured computers and not tens of thousands scattered around globally because it is cost prohibitive to do so. For Coinbase, the actual network functionality (security and transactions vis-à-vis the blockchain) is instead outsourced to a handful of mining pools.

Bitcoin, the protocol, is not experiencing any rapid iterations or improvements, the alts are but none of those improvements are being integrated back into Bitcoin itself due to a number of issues mentioned throughout this book such as the lack of resources to fund such integration and special interest groups pushing against such features (e.g., OP_RETURN 80 byte size or Zerocash/zkSNARK privacy features).

Consequently, PayPal has a distinct advantage over Bitcoin in two areas:

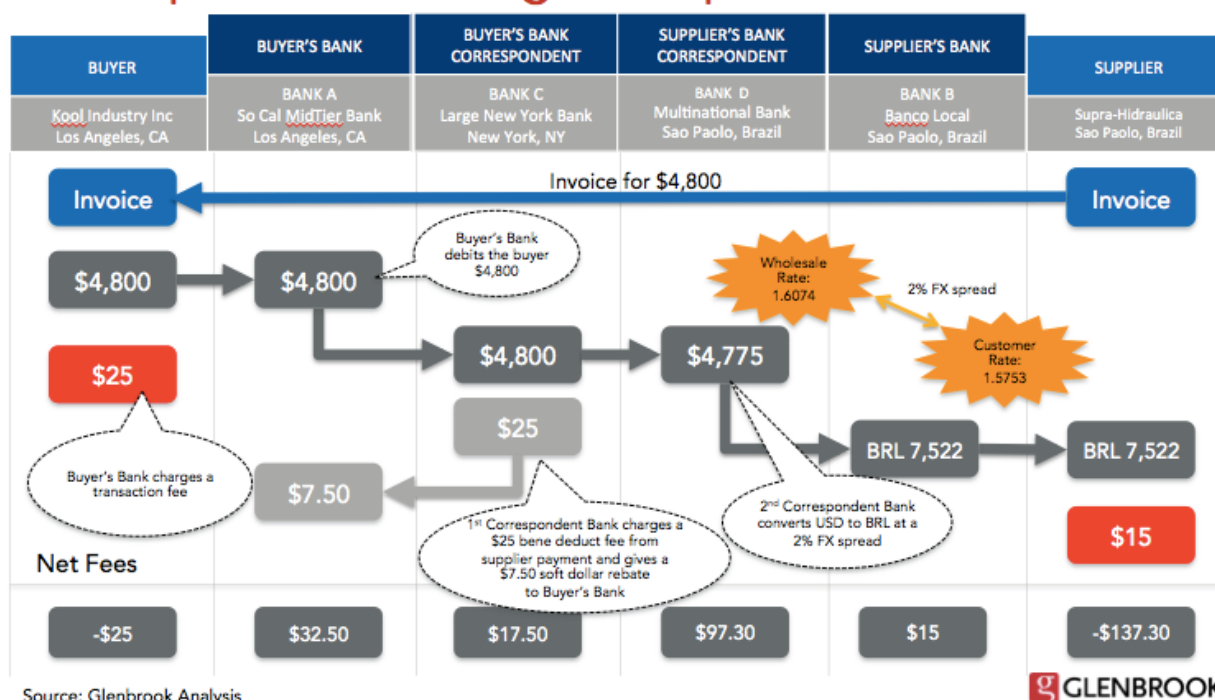
- 1) It owns its hardware and thus it cannot be easily replicated without large quantities of capital (it can withstand competitive pressure), see chapter 7.

- 2) The marginal costs for moving a transaction are virtually trivial compared with Bitcoin's cost of \$40.

Again, from a technological perspective all a company like PayPal fundamentally needs is one secure server to host a database in which the ledger entry for its customers is updated in milliseconds (much faster than 10 minutes). There is no competition. Bitcoin, again, is being marketed for an area it is not competitive at, retail payments or SWIFT-like functionality, when in fact its competitive advantage is in distributing trust. PayPal customers are provided customer service (such as fraud protection or in the event of hacking, compensation). Because Bitcoin cannot natively provide these functions, other trusted parties providing these services have to raise their operational costs to compete with PayPal, ultimately pricing themselves out of the market.

For instance, in May 2014, Erin McCune, Managing Partner at Glenbrook Partners, explained how there is no such thing as an “international wire” or global clearing house – rather there is an amalgam of international banking relationships that are collectively described as “international wires” as shown below:

Correspondent Banking: Example



While Bitcoin and its progeny could theoretically provide a backbone to these correspondent banks, other choices are much more competitive. For instance, Ripple, the protocol, is essentially a digitized form of Hawala.⁸¹⁷ It is able to provide a similar function to that which SWIFT provides – such as message routing including tying these Correspondent Banks together – yet at a significantly lower capital requirements than Bitcoin.⁸¹⁸ While many Bitcoin adopters

are dissatisfied with this, claiming that Ripple Labs (the sponsor company of Ripple) is not a decentralized institution, the first half of this book clearly shows that Bitcoin suffers from the same type of theoretical vulnerabilities that Ripple Labs could. Furthermore, because it has clear governance and a corporate sponsor that can actually pay contributors real salaries, the Ripple Labs team is able to avoid several public goods problems in the development of the Ripple protocol and ecosystem that bedevil Bitcoin.

What is the trade-off in doing so? David Schwartz is an early Bitcoin adopter and now Chief Cryptographer at Ripple Labs. Upon launching their service last spring, Schwartz, in May 2013 explained their decisions to decentralize certain aspects of the organization and code:⁸¹⁹

The tradeoff with Bitcoin's decision to go open source so early is that community input to shape the design was minimal. Where was my chance to argue against the block reward schedule before Satoshi set it in stone? Where was your chance to argue against the use of base 58 for the accounts? Where was the chance to argue for a different format for the transaction language? Where was the chance for public participation in the choice of ECDSA curves? Bitcoin was presented to the public as a done deal.

Ironically, by keeping the source closed, we keep public participation in the design open. Ripple benefited quite a bit from this decision. We made some fundamental design changes that might have been impossible to do once the system was open to different stakeholders. Essentially, Ripple is still where Bitcoin was before the source was opened -- except Ripple was open to the public for use, analysis, and comment while design changes could still easily be made while Bitcoin was not.

[...]

I don't think we can do one without the other. We've made the source code open to several different outside groups for auditing purposes. But as soon as the source code is widely available, people will almost certainly start running validators on the network. At that point, any changes to the transaction processing have to be agreed upon. Once you decentralize a system, or it decentralizes itself, there's no going back. We don't want it to be easy for one party to control it once anyone can run the source.

By the end of September 2013, rippled (the equivalent of bitcoind) was officially open-sourced.⁸²⁰ In an alternate world, Satoshi Nakamoto could have released and ran Bitcoin as testnet for the first year, giving him the flexibility to make the core changes that Schwartz hypothesized. To do so today on mainnet, especially as it relates to static bitcoin rewards or with questionable ECDSA curves (secp256k1, the Koblitz curve may not be secure) would likely divide the community because of the large financial gains and losses from these core changes.⁸²¹ Furthermore, once an organization is decentralized, it is also hard to remove those “bad apples” who may be a detriment to the users and utility of the network.⁸²²

In July 2014 L.M. Goodman put forth the argument that this is incorrect terminology to begin with, that, as Inigo Montoya might say, most advocates keep using that word – decentralization – not realizing what they think it means:⁸²³

Bitcoin is decentralized in the sense that no participant or set of participants is explicitly given a specific role in the protocol.

However, the distribution of power within Bitcoin is currently extremely unbalanced! A handful of miners represent the vast majority of the hashing power. It would suffice that 2 or 3 miners be compromised (or decide to collude) to deal a devastating blow to the security of the network.

A coalition of 100, reputable, non profit organizations located all around the world would certainly be less likely to collude or become compromised than two or three mining pool operators. This “centralized” solution would actually have a much safer distribution of power than Bitcoin currently has. Yet, it would carry the stigma of being “centralized”.

Bitcoin does not eliminate trust – that is just marketing. In this case, the less reliant on trust a user is, the better, but trust is just a cost and a compromise, like anything else. Math problems (e.g., brute forcing SHA256) does not make Bitcoin “trustless” because users are still trusting miners not to collude. Or in other words, the safety of Bitcoin relies as much on game theory as it does on cryptography.

Again, this is not an endorsement of a particular company or solution but merely an illustration. The advantage Bitcoin may have had at the beginning in 2009 (its *raison d'être*) was the cost oversight for identity management: there was none. Yet this cost has grown significantly as all venture-backed firms that handle exchanges, transactions and holdings will likely be required to fulfill costly Know Your Customer (KYC) and Anti-Money Laundering (AML) compliance which will bring the cost structure up to equilibrium with existing competitors, if not more.⁸²⁴

It is unclear what the legal requirements and compliance costs will be in markets such as The Philippines or Mexico discussed below, but there is a possibility that the costs could rise if policy makers implement similar regulations like the New York BitLicense. Will Bitcoin as a platform remain competitive in that overseas environment? This is an unknown. What is known however is that the cost of connecting the disparate systems such as Alipay, APCA, ELV, SEPA and NACHA together will not be a trivial, inexpensive endeavor and one that as a consequence of Bitcoin's cost structure could likely remove itself from the pool of long-term competitors.

Incidentally, on July 31, 2014, Stripe announced that it was an investor in a new start-up called Stellar, which uses a consensus ledger mechanism and gateway system that Ripple (the protocol) does.⁸²⁵ Stellar is co-founded by Jed McCaleb, who also co-founded Ripple Labs in 2012 but left a year later.⁸²⁶

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).

In March when I published *Great Chain of Numbers*, there were roughly 30 developers and founders working on 8 projects and the team have each subsequently increased in depth and breadth.⁸²⁷ 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 Lighthouse or some kind of Kickstarter project in which certain milestones and deadlines are publicly listed.⁸²⁸

Another way, and one in which several projects have opted to go, is through a type of crowdfunded IPO vis-à-vis bitcoins. Three 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).⁸²⁹ 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.⁸³⁰
- Ethereum: for one month starting on July 22, 2014, the Ethereum team launched its "ether sale" or Genesis sale by which outside developers and speculators could exchange bitcoins for ether (ETH).⁸³¹ Ether is used by the network to run the computational steps in a contracts that are exchanged and processed on the Ethereum blockchain. At the time of this writing, they have sold over 22.3 million ether, roughly equivalent to 11,150 bitcoins.
- 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 existing monetary stock contracted by 0.01%).⁸³² 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.

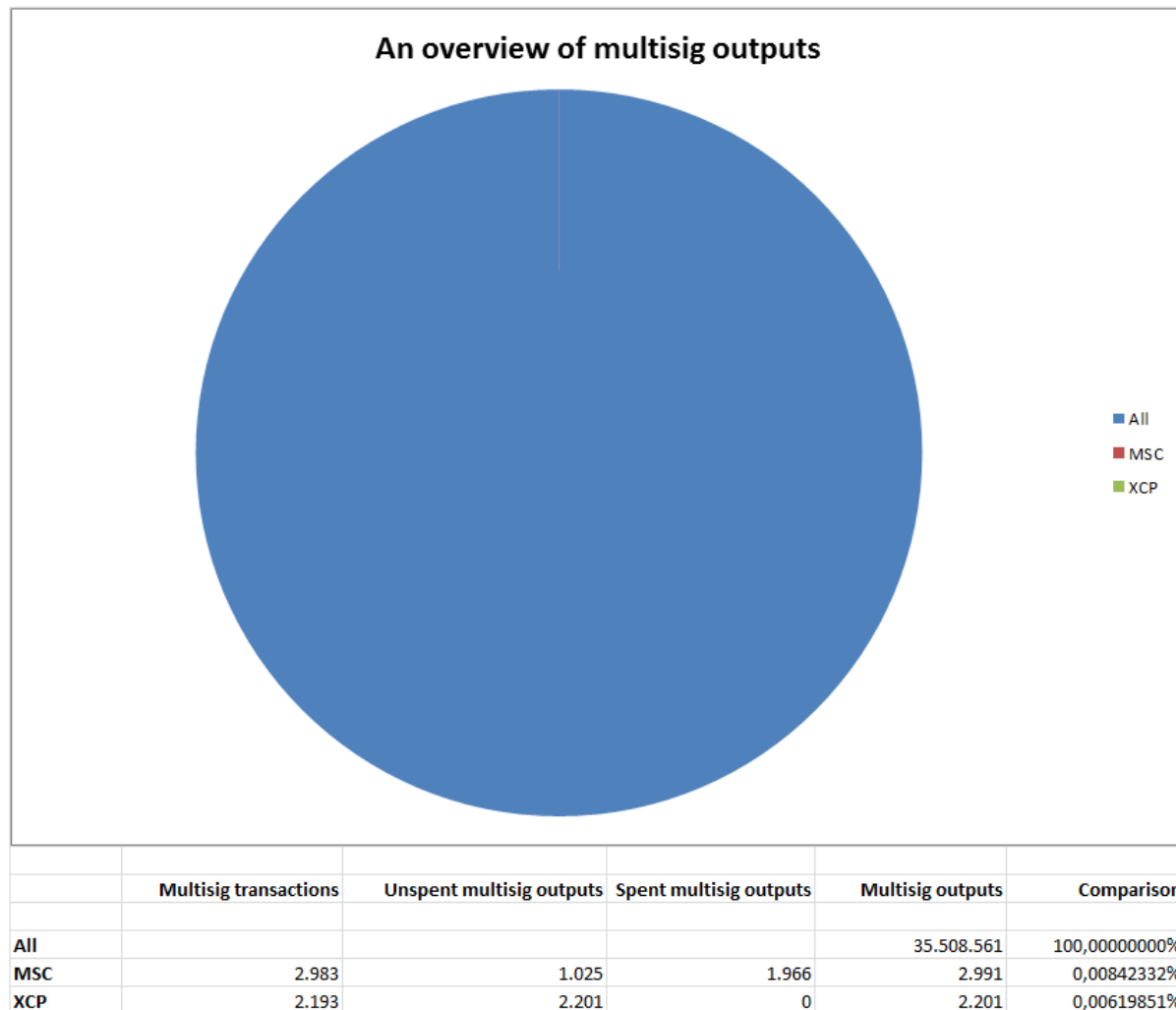
While this is not an endorsement of this particular fundraising effort, it does show you at least one method for raising development funds. In addition, Ripple Labs, the sponsor of Ripple, went a different route and has received \$9 million in funding from both venture capital and angel investors as well as wholesale of XRP (the native token of the Ripple network) over the past two years.

Real bloat?

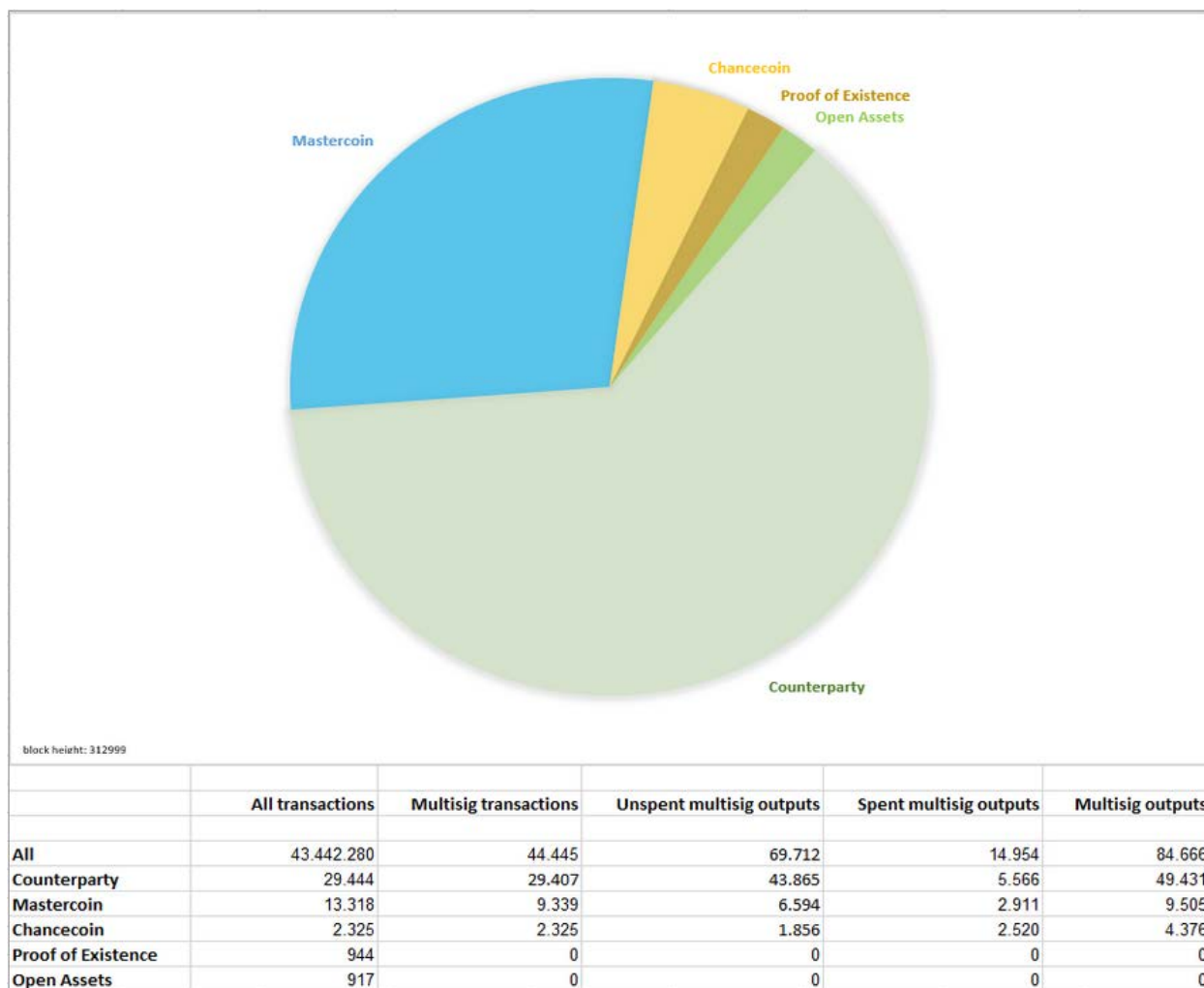
One of the common complaints that some Bitcoin adopters have towards the 2.0 platforms that reside on top of the Bitcoin blockchain, such as Mastercoin, Colored Coins and Counterparty is that in order to interface with Bitcoin, these protocols effectively clutter up the blockchain with “bloat” – multisignature 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.⁸³³



At the time, there were not 35 million multisig outputs, but rather 35 million total transactions.



I contacted the original author of this first survey conducted in March and he provided the updated chart above.⁸³⁴ Chancecoin (CHA) is a protocol and coin used to bet on dice rolls and other gambling games in a decentralized casino.⁸³⁵

What this survey shows is that over the past four months there has been a 13.4x increase in the amount of multisig transactions for Counterparty (XCP) and roughly a 3.1x increase in the amount of multisig transactions for Mastercoin. Furthermore, MSC, XCP and CHA combined now account for about 70% of all multisig outputs but compared to all transactions, MSC, XCP and CHA account for 0.1% of all transactions on the Bitcoin blockchain.

One other notable increase is that the total of unspent outputs in March 2014 was 9,819,223 and as of late July 2014 this number has increased to 12,444,288 (at block height 312,999). What this means is that the number of script hash (P2SH) and null data (OP_RETURN) transactions have grown significantly and will likely continue to do so in the near future.

And while chapter 14 discussed the disproportional security that these projects operate under (piggybacking off token inflation) it is unclear when similar native solutions can or will be built into the blockchain or if these solutions will withstand legal scrutiny over the coming 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 cryptolledger can provide. The following is a list of 84 uses compiled by Antonis Polemitis from Ledra Capital:⁸³⁶

Alternate Uses for a Cryptolledger

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)

Source: Ledra Capital

Can Bitcoin be used to track and manage all of these use-cases? Not currently, though eventually that could change with solutions like Blockstream, PeerNova and Salpas. The stated purpose of “2.0” platforms (NXT, Ethereum, Mastercoin, Counterparty, colored coins, Invictus, Ripple) is to do so natively. However most of these, like the covenants of Bitcoin, have thus far been overpromised and underdelivered (i.e., vaporware). Or maybe some are just too early.

Several other potential use-cases that have received notable coverage this past year:

- Real estate title tracking which has many additional benefits in developing countries as seen in chapter 5 and later chapter 17
- Office automation to track and verify receipts and orders with vendors without a need to worry about bloating as the cryptolledger would be internal
- HMOs and health providers can share medical records in an m-of-n manner, multisignature transactions could prevent and mitigate abuse
- While readers are encouraged to seek legal counsel, there may be opportunities in crowdequity and content rewards through programs like Koinify, Coinpowers and LTBCoin described in the next chapter.⁸³⁷

For perspective I spoke with Vitalik Buterin, founder and creator of Ethereum a “2.0” platform that as noted above, used a crowdfunding method to fund its internal development. He has previously written about some of the same challenges discussed in chapter 3, including block reward halvings.⁸³⁸ In his exchange with me he predicts that:⁸³⁹

I think that by around 2030, when fees and not mining revenue start to dominate, Bitcoin's security is going to start being substantially more wobbly than it is today. Situations where one transaction pays a very large fee and then miners all try to fight for it rather than mining on top of each other's blocks are quite likely. That's one of the main reasons why I gave ether an infinite supply.

Ethereum has an initial allocation of ether which is sold or directly granted to pay for development. This is a highly imperfect solution, since the allocation is centralized, but it is good enough; advanced governance mechanisms like futarchy may be needed to truly solve that particular problem in a properly decentralized way.

In terms of motivations and reasons for why he decided to build a new ledger in the first place:

Bitcoin is actually two things at the same time. First, it is a decentralized currency, and second it is a blockchain. Many people focus on the first aspect; however, in reality the blockchain is usable for a lot more - including contracts, name registries, decentralized organizations, and dozens of other features that we have not thought of.

There have been a few attempts to make platforms on top of Bitcoin that have that functionality, but all were limited in various respects - they all tried to add a limited number of "features" to a Bitcoin-like system, rather than being properly generalized and allowing people to build whatever building blocks they wanted. The intent behind Ethereum was to fix that problem.

While promising, it is unclear at this time whether or not these features will fulfill mass consumer demand that cannot be fulfilled today by other existing platforms. For instance, if there was a large profit margin to be made issuing and exchanging contracts in a decentralized

manner, wouldn't existing contract providers already be building these systems? For balance, some advocates are quick to point out that the legal framework does not allow these systems to work as-stated, the next chapter will discuss the challenges of protecting property (e.g., digital bearer bonds) on an unrecognized decentralized platform. Consequently, in the event that the legal framework is resolved, nothing prevents for-profit companies could fork the code and provide competing services as happened in the free open source (FOSS) movement in the 1990s which is an issue detailed earlier in chapter 7.

For perspective, in the five months since I wrote my previous book, in terms of production code shipped: Ripple and Counterparty have advanced the furthest followed by NXT, Bitshares (from Invictus) and Mastercoin (in that order). They all are significantly further along in development than Ethereum, which is not scheduled to be launched for another 6-9 months at the minimum. Open-Transactions continues to remain a work in progress. And again, this is not an endorsement of these projects or their coins.

Competition does not disappear in an open market

One of the memes propagating on Twitter, reddit and Bitcoin Talk is the coming death of alts or alternative coins. It has been historically true that most proof-of-work-based alts never live past their second or third "halvingday" – and the new "Blockchain 2.0" solution seems to provide technical incentives for why alt designers may be interested in working within one existing system instead of building entirely new protocols which compete with Bitcoin directly.⁸⁴⁰

As noted in chapter 2, alts will also probably continue to exist for at least two reasons:

- 1) Scarce labor
- 2) Depreciating capital goods

There are few people capable of building a secure blockchain and because Bitcoin operates as a charity organization (socializing labor, privatizing gains) there is no one to pay the developers (yet). Perhaps the new Blockstream (sidechains) project or Coinbase or Bitpay will be the Red Hat of this space, maybe none of them will.⁸⁴¹ But currently, the only chains that pay their developers are alts. Thus capable labor continues to go where market rewards are.

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

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 proposed a theoretical FastCoin5, with “block intervals is 5 seconds and transaction confirmation (for a reversal probability of 0.1%) is below 25 seconds.”⁸⁴²

For comparison, on average:

- GeistGeld had **15 second** blocks (but many orphans)⁸⁴³
- Bitcoin has **10 minute** blocks (max 7 tx per second)
- Litecoin has **2.5 minute** 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

While these block timings can be arbitrarily changed with a trivial edit in the code base, there is a balancing act in terms of orphans. GeistGeld failed in part because it was uneconomical for miners to protect the network when they were unable to be rewarded due to high orphan rates (e.g., working on and propagating blocks that have no parent in the longest tree).

SKU and supply chain management

According to *Gartner*, supply chain management software revenue will reach \$10 billion in 2014, can blockchains be used in this segment?⁸⁴⁴ In July 2014 I spoke with Srinivasan Sriram and Zaki Manian, co-founders of a new startup in Palo Alto called SkuChain.⁸⁴⁵

They have focused on building a blockchain-based solution using its core competitive advantage: creating transparency in supply chains.⁸⁴⁶ And they have done so by identifying three areas of “pain” which SkuChain is trying to resolve.

The first area is the Letter-of-credit (LC) to Bill-of-Lading (BL) workflow where wholesale buyers issue an LC through a bank on which manufacturers get a working loan and then attach a BL to the shipment that when cleared through customs or shipment transit point triggers an automatic payment transaction based on the terms of the LC.

According to Sriram,

“When Alice wants to buy something from Bob, she gets an LC from a bank and sends it to Bob. Bob goes into his bank and can now get a loan against it. Bob then builds and ships the widgets. The shipping documents include a Bill of Lading that transfers title of the goods from Bob to the Carrier and then from the Carrier to Alice. Once Alice receives the shipment and signs the Bill of Lading the monies are released from Alice’s bank to Bob’s bank and to Bob.”

Thus as part of their development process, they foresee a time in which a smart contract sitting on the SkuChain with the right kind of multisignatures in place, could make this process frictionless. In addition the same contract could be used to split payments along the supply chain to the suppliers who shipped raw materials to Bob.⁸⁴⁷

The second area, or pain point, is in shipments that are slated for retail and go through a wholesale to distributor process. Under current conditions tracking the end product is very difficult especially when there are unitization steps in-between where large quantities are packed for unit retail.

According to Manian,

“One reason why they haven’t created centralized supply chains in the wholesale to distributor to retail space is because the chain is very fragmented and it would be very difficult and expensive to even contemplate such a thing. Also, there is no real need for manufacturers to know much about the downstream activity, they just want to sell their raw materials.

The original manufacturer whose products are sold at Alice’s Pharmacy, doesn’t want/need to know about Bob the wholesaler or Dan the distributor but only Evan (the consumer). They don’t want to build a database or manage identities.”

According to their development plan, with SkuChain, rather than building integrated and synchronized databases that can be cost prohibitive to maintain, every person down from the manufacturer has the keys because the distributor receives the SkuChain keys along with the package and can re-generate additional keys in different units, the total being equal to the original quantity. In theory, the technology is self-referential and the package proves its own validity.

For example, a distributor receiving a package of 100 bottles would be able to take the SkuChain label from the tamper-proof package and subdivide it into 100 units and create 100 new wallets which say “proof of 1 bottle.” The consumer can see the originating path through the subdivision step to the original manufacturer, originated and signed by Pfizer’s trusted signature.

This provides protection against double-spending, guarantees the product has not been diluted (e.g., copied), and there will not be any more bottles from Pfizer than Pfizer produced, since each bottle can self-validate its path to the originating manufacturer.

Sriram thinks that the cryptographic protection against double spending that public/private key/wallets provided by the blockchain technology, “offers a unique opportunity to transform shipping labels into tracking vouchers that can ensure that end-retail products have clear provenance. From pharmaceuticals to milk powder and luxury goods such a tracking system would prove to be invaluable saving billions of dollars and more importantly providing farm to table assurance guaranteed by the blockchain.”

The third and final area is in the retail Consumer Packaged Goods (CPG) segment where the ubiquitous bar code is the means by which SKU pricing and identification is done.

The SkuChain would augment these barcodes with Unique Hierarchical deterministic addresses to provide one-to-one marketing channels between brand and consumer. This can provide both large groups like Procter & Gamble and small locally produced coffee-roasters a simple trusted way to build a direct relationship with the end-consumers of their product regardless of the distribution channel through which the product was delivered.

Thus based on SkuChain's current model the flow looks as follows:

From manufacturer -> to distributor -> to consumer using their patent-pending ability to generate a large number of HD addresses and move value between them at will.

At the end of July they deployed their technology as a dry run through a project called Coinblaster.⁸⁴⁸ CoinBlaster itself went on to win first prize at a July 'hackadoge' event in San Francisco.⁸⁴⁹

Their team also identified a low-hanging fruit entry strategy: SkuChain label stickers that shippers can stick to their cartons. This lets distributors and retailers look up the secret key using a mobile app and ensure that the original shipment of say 1,000 milligram of a drug can only be split into 10 x 100 milligram packets, and the 11th one will not be able to get a valid SkuChain label. This lets the manufacturer control the whole chain without having to build complex systems integrating all the distributors throughout the supply chain.

They are not selling any tokens as this is a non-monetary application of blockchain technology. In addition, eventually SkuChain will be built as a separate custom blockchain, but for now it will likely use the Dogecoin ledger. According to Sriram, "Dogecoin was temporarily chosen due to its low transaction fees and fast confirmations. Bitshares seems to have a lot of what we are looking for in their custom chain and they might fork it when it becomes available."

Whether or not existing systems such as SAP could also be used to build a similarly transparent platform is an area for future entrepreneurs to assess. For instance, there are some existing databases that tracks these types of inputs and outputs for specific industries. Producers of the raw material have existing ways to target sales down through the entire distribution chain based on a wide variety of criteria at each level. Knowing about their downstream is how they sell their raw materials – large producers typically sell to every level of the chain depending on volume. Can a blockchain be inserted in this process to provide better quality control? Furthermore, if consumers are able to validate against it, does this expose any sort of logistic or production information to competitors? Supply chain management systems today make heavy use of EDI and large retailers like Walmart take it one step further with proprietary systems that sit atop EDI.⁸⁵⁰ Perhaps blockchains could be added to another quality control layer in this process.

This idea was earlier explored by a team of German researchers in, *Towards Risk Scoring of Bitcoin Transactions*.⁸⁵¹ By conducting their audit of Bitcoin they saw potential use for the blockchain as a means for providing transparency:

On the upside, however, recipients of payments could apply ethical standards on what money they accept. This is best comparable to the Kimberly Process Certification Scheme, a set of international resolutions established with the aim to suspend the trade of blood diamonds, which are mined in war zones and sold to finance arms. One might wonder how well certain industries fared if the money they accept could be traced back with the ease offered by Bitcoin. Although market participants still use Bitcoin like a fungible good, being more selective in what one accepts stands to reason. At least those who have a brand or reputation to lose have every reasons to be afraid of negative publicity linking their profits to violence, with evidence publicly accessible in the block chain.

The Kimberly Process was established in 2003 and was set up “to ensure that diamond purchases were not financing violence by rebel movements and their allies seeking to undermine legitimate governments.”⁸⁵² Blockchains are one candidate for providing accountability in this segment.

International Payments

I also spoke with Marco Montes Neri, founder of Saldo MX, an international payments platform.⁸⁵³ Neri is originally from Mexico and saw a pain point that had a number of frictions: migrant workers from Mexico working in the US who wanted to pay for a variety of bills back home. While they could use existing companies like Western Union, as noted in this book, such remittance options can be costly as funds have to be converted from dollars and into pesos. Mexicans working in the US remit around \$22 billion a year, thus shaving off a few percent can provide more savings for their families back home.⁸⁵⁴

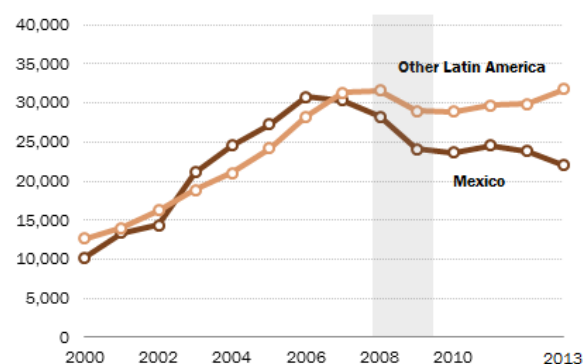
He did this by using existing closed-loop infrastructure: users can pay their bills in Mexico directly from the US. According to Montes Neri:

A remittance is by definition a sum of money sent to an individual or a place. Its intrinsic inability to recognize the purpose of the money created numerous Know-Your-

FIGURE 1

Total Remittances Received in Latin America and Mexico, 2000-2013

In millions, 2013 U.S. dollars



Notes: Shading indicates U.S. recession. 2013 are World Bank estimates. "Other Latin America" comprises Argentina, Bolivia, Chile, Colombia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, Honduras, Nicaragua, Panama, Paraguay, Peru, Uruguay and Venezuela. Remittance flows for 2005-2013 use a different methodology than 2000-2004; for more details see text box.

Source: World Bank Annual Remittances Data Inflows, Oct. 2013

<http://go.worldbank.org/092X1CHH0>

PEW RESEARCH CENTER

Customer (KYC) procedures. Saldo is moving away from the traditional remittance paradigm by understanding the destination and frequency of international money transfers. We use a low cost, secure network of payments on Ripple and bring an innovative way to use gateways (on- ramp and off-ramp points). The telecoms in this instance are part of the gateway.

And how does he handle the edge-based interfaces?

Saldo basically creates a distributed network of mobile agents for the cash-in process instead of using expensive networks of payments and eliminates the need of cashing out completely. We launched this with 10 agents on the ground in San Jose, California and they provide the ability for thousands of underbanked Mexicans in the area to pay phone bills, utilities, cable or insurance back in México. And by limiting the amount of money the agents move fulfills FinCEN AML regulations.

As he noted, there is no cash-out (it is pre-paid), it uses a trusted network (the phone companies already handle the KYC) and the size limit for such payments is limited to no more than \$2,000 daily, thus removing some of the legal costs that would otherwise be passed on to customers.

For balance, in June 2014 I also spoke with Ron Hose, CEO and co-founder of Coins.ph, the leading Bitcoin exchange in The Philippines.⁸⁵⁵

According to Hose the largest pain point for a large segment of the population is sending and receiving money abroad. With about \$25 billion a year the Philippines is the 3rd largest recipient of remittances – roughly half the size of its gross domestic exports.⁸⁵⁶ And these funds are predominantly going to people who do not have bank accounts and thus have to pick money up at retail locations like Western Union and consequently pay an average of 9% in fees.⁸⁵⁷

“The reason they pay this 9%,” explained Hose, “is because they don’t have a bank account and likely will never have a bank account because they do not have enough savings. Banks have a cost structure (location, tellers, rent) and if you do not have sufficient savings on the first day when you open an account, the bank is already losing money. This pain point is an area where mobile banking and bitcoin can help out. For instance, if a relative abroad sends money to you and you have to pay a transaction fee to a retail location, then that is equivalent in 3-4 days of income that you paid just to pick up your money.”

He also noted that the key to finding use-cases with Bitcoin is,

It must solve a real problem; there has to be something that is painful enough to convert, somewhere there is enough friction. The thing about emerging markets is that pain exists – you don’t have a bank account or you have to pay 9% to transfer money to your family – so it is much easier to make that leap.

Because current decentralized systems have logistical challenges competing with incumbent credit card processors such as speed, confirmations and usually cost, Bitcoin entrepreneurs are typically 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 purportedly provide services to the underbanked.⁸⁵⁸

Yet accepting bitcoins does not necessarily translate to actual bitcoin payments. For instance, on July 9, 2014 I contacted Automattic, the parent company of WordPress and asked if they would comment on how many bitcoins they had received since they first began accepting them. The response I received in return was, “We will not disclose that type of information since we keep our financial information private, as well as any information as it relates to our users.” In contrast, in September 2013, Rick Falkvinge contacted the same company and asked the same question, their response was, “a couple of hundred dollars worth, so far.”⁸⁵⁹ What this likely means is that *ceteris paribus*, they simply have not received many bitcoins. As shown by the charts analyzing blockchain behavior, this lack of purchases is common in the bitcoin space and is likely one of the reasons why BitPay stopped reporting transactional volume after fall of 2013.⁸⁶⁰ Perhaps this will change if and when exchanges and ATMs are built in these 60 countries but such services require an infrastructure that may not exist in some of these regions.

In Goldman Sachs report this past spring, they note that using the Bitcoin network today, retail merchants, online merchants and remittance consumers purportedly could accrue \$210 billion of savings.⁸⁶¹ Though, to be clear, unlike UBS’ report, the Goldman Sachs report does not take into account the actual transaction costs of using the network (i.e., 1% fee).⁸⁶² 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 uses the daily transaction volume divided by daily money supply.⁸⁶³ Thus again, on paper Bitcoin appears disruptive yet when these unseen costs are accounted for, it may actually be more expensive than existing systems.

While it is unclear what the impact BitLicense regulations will have on the adoption and continued development of altplatforms or even Bitcoin itself, the next chapter discusses the legal opportunities and challenges of working in this fledgling space.

Chapter 17: Legal specialization

What then is a protocol like Bitcoin especially good at? The world has seen virtual currencies (Beenz and Flooz), cryptographic currencies (DigiCash) and numerous commodity-standards (gold, silver, copper).⁸⁶⁴ And even if the “currency” aspect of bitcoin finds niches, according to preliminary research from Neil Gandal and Hanna Halaburda, it is unlikely that network effects alone will create a winner-takes-all scenario relative to other cryptocurrencies.⁸⁶⁵

Instead, the core innovation is the blockchain, which may be competitive at managing distributed trustlessness (a topic also broached by a recent OECD working paper).⁸⁶⁶ This space has also spurred the development of creative tools including a bevy of HDM wallets as well as authentication services (like up-and-coming Lastwall).⁸⁶⁷⁸⁶⁸ This chapter will discuss the opportunities for legal professionals in this new space as well as the challenges that entrepreneurs face whilst building projects and companies.

For perspective I spoke with several attorneys including James Duchenne, co-founder of Satoshi Legal and founder of SEiAN Rewards.⁸⁶⁹ According to him,

“For me, using bitcoin is a matter of choice. You can choose to trust in the laws crafted by people and their empowered third parties, or the laws of consensus algorithms. So, bitcoin is not a completely trustless system, as some would advocate, but rather it allows the possibility to shift trust from the status quo to an algorithm, the security provided by miners, the reliability of nodes and the confidence of the underlying system's economic viability.

I also view bitcoin as being like the “Benjamin Button” of technology. It started its life as a currency and is currently backtracking to fulfill its promise as a distributed consensus network. Thus, it was born an adult, fought like one and is now growing towards its adolescence and *raison de vivre*. Perhaps, if it were the other way around, descriptions of it having no intrinsic value wouldn't be heard.

In terms of use, I tend to view bitcoin as an “algorithmic-enforced” private contract assigning value amongst its users (in so far as price discovery exists and it doesn't contravene the laws of a relevant jurisdiction). Unfortunately, it currently sucks at that function due to its volatility. However, the point is that it is able to be the product, the registered agent, the legal system and the enforcer. Thus, implementations like coloring coins to represent an element (i.e. share, assets etc.) are kind of silly, since transacting in those “rights” must be replicated with paper work to comply with existing law.

Lastly, some of the big hurdles in using bitcoin's consensus network are education, trust and liability, especially if it's to be used by the legal profession. Would an attorney, an accountant or a registrar use the blockchain as counterparty for the verification and authentication of a document or for other recording keeping purposes? They can, but

it's unlikely it'll happen anytime soon. Who bears the risk if something goes wrong with bitcoin? Is it malpractice? Alternatively, someone can offer this service, keep copies of the records and bear that risk. Then why use the blockchain for this purpose? I can, however, entertain the thought of the consensus network being used in self-enforced private contracts for ownership and dissemination of digital intellectual property. While this is the promise of the consensus network, we have yet to see successful real world sustainable applications and examples.”

What else can this distributed network be used for? What are some of these possibilities that Duchenne is referring to? For instance, in some places like Greece (which does not have a computerized central land title registry system), titles are held in different localities and law firms which makes the dispute over who owns a certain house complicated.⁸⁷⁰ For buyers and sellers this can result in expensive due diligence and fact-finding processes.

Yet, all things being equal, this notary niche is probably a bit easier, cheaper and less lawsuit prone for solutions with high infrastructure costs like Bitcoin because legalese is more semantical than the “currency” questions where uncertainty lies in many jurisdictions. For instance, in the Greek case above, a blockchain could store the metadata, the hash or even the entire land title itself.

Entrepreneurs could build companies around Proof-of-existence and Bistamped-like services such as these or perhaps, countries, communities and NGOs could use assurance contracts to fund the network through what Mike Hearn is trying to do with Lighthouse.⁸⁷¹ Or maybe similar volunteer initiatives like NodeShares and “Adopt-a-node” can be done on the mining side as well (e.g., an intentional non-profit mining farm).⁸⁷²

Attorney Pamela Morgan, founder of Empowered Law, thinks that:⁸⁷³

“Beyond currency, there are many uses for bitcoin technology. For example, we could create global jury pools for private dispute resolution. Participants could either provide value to the network through services, such as serving as a jury member or by paying for the service. Users of the service would have access to a more diverse, and possibly skilled, pool for dispute resolution which should result in improved outcomes. Jurors could be chosen randomly and elect to serve or not, thereby helping to prevent coercion or jury tampering. While a similar service could exist outside of the blockchain, the transparency provided by a public voting ledger would likely be the simplest and most easily implemented method.”

However, according to Preston Byrne, perhaps this could still run into other hurdles:

“Bitcoin is tremendously expensive to operate, capable of transmitting only very basic data, and even then only does so unidirectionally. It's basically ARPANET with the ability to fork - which it should do, and soon, if it is to have any chance of long-term survival.

You can do virtually anything you want with a blockchain - much as you can do anything you want with software. The issue is that you have to structure it properly so that the blockchain creates the real-world impact you want in direct conjunction with the digital asset you want to transfer.

Problem is, just 'colouring' a coin as one asset or another achieves practically nothing unless you can also present data which matches the token or contract and demonstrates evidence of ownership. Most of the proposals for virtual assets or title registration do not address this issue adequately, if they do so at all."

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. 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?"⁸⁷⁴



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. 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.⁸⁷⁵ 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 cryptolledger 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 cryptolledger 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 cryptolledger with a traditional ledger system.⁸⁷⁶ Banks could inexpensively reduce their exposure and increase their awareness of sudden or unexpected liabilities on their balance sheets, and furthermore, the cryptolledger 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.

Real risks

While in the long-run there will likely be new opportunities that open up, below are real, present risks involving the cryptocurrency world, especially with those individuals developing appcoins, crowdfunding and crowdequity platforms. For instance, section III of the Jumpstart Our Business Startups (JOBS) Act has *not* been written up let alone implemented.⁸⁷⁷

As a Swiss friend in finance likes to remind me: Rule #1 of Bitcoin: do not believe any news about Bitcoin -- always do your own research. And in this case, talk to an attorney.

In the event of lawsuits, not everyone has enough money to live abroad and permanently hang out in Panama, Switzerland or Japan – thus if it sounds too good to be true, it probably is.

I spoke to several attorneys about specific risks under this umbrella such as:

1) Securities are legal constructs and require legal structuring to be valid and binding obligations of their issuers.

As Preston Byrne, put it bluntly: "virtually nobody has done this correctly. To date I have not seen a single crypto-security that has been properly structured." Purchasers of securities issued on a cryptolledger may find that what they think they possess is in fact nothing of the sort - for example, a "cryptoequity" may purport to represent an ownership interest in a company, but will only be so if it is recognized as such in the jurisdiction of the issuer's incorporation. Extensive due diligence and legal advice are essential before entering into any such investment.

According to Austin Brister, a Houston-based attorney, "Aside from the validity concerns, most of the foreign crypto-startups I follow should realize that they will likely be subject to U.S. Security laws, whether they like it or not. For example, even though the SEC has taken a more and more "foreign friendly" position over the last few years, U.S. securities laws can and do frequently govern non-U.S. issuers of securities. This means that, even if these startups did pack up and move to Sweden, they still may be subject to many securities rules administered by the SEC, including prospectus disclosures, periodic reporting requirements, and all the various protections such as insider trading, tipping, fraud, etc. For most of these startups, the fact that they have established a foreign home base will, at best, allow them to qualify as a "foreign private issuer." However, this isn't a complete "U.S. Securities Shelter" or loophole, but rather simply allows "foreign private issuers" to qualify for reduced reporting and disclosure requirements.

Of course startups could potentially seek to remove themselves sufficiently from the United States capital markets to not be subject to its various securities laws. Certainly, *Morrison v. National Australia Bank* and its progeny indicate growing resistance by US courts to exercise their extraterritorial jurisdiction in dealing with US federal securities laws. However, many of the startups I have talked to specifically plan to target the US markets, and have considered the move overseas merely as some fictitious SEC loophole."

Similarly, James Duchenne, comments that, "an analogy that I've heard for the issuance of tokens to fund and, subsequently use in, a project is like buying game credits to play in a game; if the game disappears, the credits are useless. Thus the only thing to worry about, they contend, is misrepresentation and non-performance. However, it's not that simple and following *SEC v. Shavers*, promoters must be extremely careful as to how they structure, issue, offer and approach their fund raising efforts, especially where in substance the scheme can be seen as a common enterprise with the expectation of profits. As to issuing "shares of stock" in an undertaking (and worst, labeling it as such) in crypto-currency without proper compliance in the relevant jurisdiction will likely bring the wrath of local governmental agencies (and those that exert extraterritorial jurisdictions), so it's not a good idea for a promoter or an investor to get involved in these."

While it varies upon jurisdiction, the Howey test is one definition of a security under current US federal law.⁸⁷⁸

2) Government bodies like the SEC, CFTC and FinCEN will likely prosecute those who violate the “accredited investor” statutes.⁸⁷⁹

As Byrne candidly put it, “to my knowledge, every pre-sale that has hit the market is or should have been subject to these statutes or jurisdiction-appropriate public offering rules. To my knowledge, again, not a single one has actually complied.” Each jurisdiction has different requirements for users to meet, and failure to do so could result in fines and perhaps worse. Bob might think issuing a securities contract in a foreign country (like Switzerland) might mitigate this risk, but if Swiss legal formalities are not complied with and/or any of the buyers turn out to be US citizens, then the SEC may step in. As shown by the SatoshiDice case, this is unlikely to change anytime soon.⁸⁸⁰ Firms like SWARM and Moolah (and their “Pie” fundraiser) should take note.⁸⁸¹

Duchenne concurrently notes that, “playing in “securities” on exchanges like Havelock is like entering a virtual game of Russian roulette after having digested volumes of inadequate prospectus-like information. Bloated with this “intelligent” data and what passes for news on the Internet, users go around thinking they’re buying “shares” in the next Facebook. That is, until Neo & Bee happens.”

3) Bar associations and their members (attorneys) could and likely will prosecute organizations and developers for “unauthorized practice of law” (UPL).⁸⁸² While this may sound anti-competitive, they have decades of both statutory and case-law to back them.

As one NYC-based attorney I spoke with noted, “There are always exceptions to the anti-trust laws such as bar associations -- and usually the only people that ever challenge it are bad lawyers. More than likely you will get slapped with unauthorized practice if you try to do lawyerly things or give advice. Unfortunately most people such as developers do not know anything about legal stuff so this could end badly for them.”

Pamela Morgan, explained that, “Companies outside of the Bitcoin ecosystem - like Legal Zoom - continue to face similar UPL lawsuits. Sometimes they win.⁸⁸³ They are basically paving the way to certainty, one way or the other, for these types of businesses. Though the industry could fight to change the laws if companies like Legal Zoom lose the UPL cases, the more likely outcome, at least in the short term, is that start-ups in the space would become less attractive to investment due to increased legal risks. Regardless UPL lawsuits present a real risk to those seeking to provide code based legal solutions to the public.”

Continuing she notes, “Many of the organizations competing in the space have not completed business organization paperwork, thereby exposing the owners to unlimited civil liability. Meaning the owners personal assets could be used to satisfy the debts of the organization. While it may not be easy to uncover the identities of the owners of these

companies, given the right motivation (such as a government seeking taxes, another organization seeking money damages, etc.) it can be done."

Brister thinks that, "It's important to note that, in practice, these laws focus almost entirely on the protection of the ordinary consumer. Companies like Legal Zoom are becoming more and more safe for the ordinary consumer, because the entire population is becoming more and more "do it yourself" centered, and is much more familiar with the risks and challenges associated with playing the "pro se internet lawyer." But this is a poor analogy for cryptocurrencies, blockchain technologies and so-called "smart contracts," because the average consumer is light years away from understanding crypto technologies, and appreciating the various risks. In other words, just because Legal Zoom can argue that the average person can safely fill in the blanks for a pre-drafted DIY Last Will and Testament, doesn't mean that the average person is safe in navigating the intricacies and risks associated with converting their affairs into complex algorithms, managing their assets over irreversible P2P systems, and coding their seemingly simple agreements into the proper syntax, operators, and cryptographic protocols. Can it be done? Sure. But I believe we are a long way out. However, I don't believe bar associations will be keen to computer programmers drafting and negotiating smart contracts without being licensed to practice law, which establishes the character, fitness and competence required to step in the shoes of another person and represent them in their legal affairs."

4) These same protocols and ledgers currently have no way to indemnify users since they often lack legal personality and cash-flow, and have no assets. Accordingly, recovery in the event that a given altcoin or appcoin "startup" network fails could turn out to be extremely difficult in practice. Consequently if for example, an altcoin or appcoin "startup" does have funds, they may be able to indemnify specific users (namely exchanges) through corporate insurance (a bond). If you plan to go down this route be sure to try and get such assurance on paper, that is standard operating procedure and this space is no exception.

Concluding, Brister explained that, "Consumer protection laws can be far reaching and quite unforgiving. Ordinary businesses do just fine in navigating these laws, even if they don't realize it, because they can adjust their interactions with consumers in "real-time" in order to be reasonable, well-centered, and act in good faith in dealing with consumers. However, the problem with smart contracts, decentralized autonomous organizations, and the like, is that they are hard-wired to act in one way, whether it makes sense or not. Unforeseeable circumstances practically always present themselves to businesses of all types, and by definition, these circumstances cannot be foreseen or planned for. These systems need to adequately plan for this possibility, and be prepared to be properly insured or adequately bonded in the event things go wrong, and customers are hurt. Similarly, consumers should be aware that they are not dealing with living breathing people, but rather a machine subject only to 0's and 1's."

In addition, one problem with integrating blockchains and their functionality (e.g., smart contracts) into existing financial institutions is that the protocols and ledgers have to go

through each of those companies internal compliance channels which takes many months and perhaps years. For instance if something like a blockchain passed compliance checks, it would only be useful if their counterparties also had blockchains, which would mean going through other compliance venues -- yet blockchains currently do not add much value to the back end (yet) of the organizations, Citi and Goldman Sachs do not counterfeit one another.

Maybe something like Secure Asset Exchange on the NXT platform will become more commonplace once the legal issues are resolved.⁸⁸⁴ But remember there are already dozens of trading platforms used by financial professionals today thus not only do these new smart contract-based systems compete with one another, but also seasoned incumbents. And not just incumbents that build trading platforms.

For instance, according to company filings Ingenico, VeriFone and Pax Technology collectively spent \$92 million on research and development in the first half of 2010 a figure that nearly doubled to \$174 million by the second half of 2013.⁸⁸⁵ These are the top three public payment terminal providers (for point-of-sale) and highlight that existing players are not sitting idle.

Therefore while blockchains could act as an intermediary in a back office for clearing and settlement or for derivatives intermediation, it may not be able to efficiently do so in a competitive environment let alone in a retail setting.

Efforts like Common Accord, Codius and Bithalo may change this equilibrium.⁸⁸⁶

I contacted Primavera De Filippi, a legal researcher at Harvard's Berkman Center for Internet & Society and a co-leader of the Common Accord initiative. In her upcoming paper *Legal Framework For Crypto-Ledger Transactions*, she explains the challenges of self-enforceability versus legal enforceability of smart contracts:⁸⁸⁷

Yet, many people forget that these applications are meant to operate in a world that is regulated by traditional rules of law. While smart contracts are increasingly able to handle complex deal logics, many kinds of transactions do - eventually - have to interface with the "real world". It is at those "choke points" that the legal system will ultimately have a say in the context of a breach.

In this regard, one important question is to determine whether smart contracts are in fact actionable in the real world. While they can be regarded, at their core, as a written contract drafted in a computer language, it is not clear - at this date - whether their code is "legally binding" upon the parties interacting with these contracts.

This is a critical issue because the provisions of a smart-contract are self-enforceable only to the extent that they account for all possible deviations from the agreed-upon terms - e.g. by implementing a complex system of collaterals, which might considerably increase the complexity of these contracts. Were they enforceable under the law, smart-contracts could be drafted in a much simpler manner - e.g. by only incorporating

a basic set of conditions into the code and subsequently relying on the legal system in order to enforce these conditions, in the event of a breach. Legal enforceability would essentially allow for only the main-case set to be handled by smart-contracts, leaving the edge-case set to be handled by the courts.

Most importantly, in many real-world situations, contracts are performed without the need to be enforced by law, as the threat of one party invoking the legal system is sufficient for the other party to comply with the contracted terms. In order to be as effective as their traditional counterparts, smart contracts must therefore also be actionable in the real world. This might, of course, require them to comply with all the standard formalities required for a court to enforce a contract under the law.

The solution she proposes to bridge this chasm is what underpins Common Accord, the creation of a “global template system of codified legal text.” Such a framework already exists for commercial transactions and procurement processes called International Commercial Terms or Incoterms. Common Accord is a project that researchers, attorneys and entrepreneurs may be interested in pursuing in the future. In the meantime be sure to contact an experienced legal professional before pursuing any of the aforementioned options.

Cryptosecurities

Throughout this past spring I received a number of emails from individuals looking to leverage the technical capabilities of colored coins and metacoins to issue shares of stock. One such correspondence included the following from “Mark”:⁸⁸⁸

I think a good use case is for stocks: so long as it's for Class A common stock, no dividends, it's a very uniform asset, already digitally-issued. If Google treasury (the issuer of Google stock) colored a coin, they are the final arbiter of whether a share is a share, and I would trust them as the issuer of the coin. But what about proxies, splits, ugh...

Best, best use case is for foreign stocks to be registered this way: it's still really cumbersome for a non-Brazilian investor, for example, to buy Petrobras on Brazil's Bovespa market.

While the technical constraints of creating a distributed system to transfer financial instruments could conceivably be decentralized, whether or not that these kind of companies are willing to try and adopt this method is another matter entirely — as are the legal issues of exchanging a security to different qualified investors. What is the cost-benefit for a company like Google to do so?

Consequently, on July 30, 2014, Patrick Byrne, CEO of Overstock created a new site to explore, “how a public company could issue a “cryptosecurity” to potential investors.”⁸⁸⁹ And that one

of the platforms his team was looking at to provide the ability to issue stocks on was Counterparty.

In the same news story, Keith Miller, an attorney with Perkins Coie (which represents around 50 companies in the digital currency space) explained that, “I find it very difficult to believe that they won’t have to get some sort of registration statement on file that the SEC would have to approve—and I suspect there would be lots of comments back and forth.”

This skeptical view was also articulated by Preston Byrne (no relation to Patrick), who explained in an email exchange that:⁸⁹⁰

“I think it extremely unlikely that Counterparty will ever be used to transfer securities, for the following reasons:

- *first*, to paraphrase Dr. Byrne, shares are utterly dependent on government mandarins, and with good reason. Being things in action, the ultimate guarantor of their value is the possibility of real-world enforcement against their issuers in the event of a default or making distributions on events such as an insolvency. Basing such instruments on a blockchain will frustrate that possibility;
- *second*, the objective of the capital markets is for companies to raise capital - which, for the foreseeable future at least, the main markets are likely to be a far more effective means of doing so;
- *third*, a fully-decentralised alternative will, as Bitcoin, be vulnerable to network failure in a way that a bricks-and-mortar institution is not;
- *fourth*, the issuance of securities is difficult for a reason - we have these regulations to protect people from, in the words of *SEC v Howey*, "the countless and variable schemes devised by those who seek the use of the money of others on the promise of profits." Although libertarians among us will argue that they should be free to choose for themselves from what and from whom they need government protection, the overwhelming evidence from centuries of securities fraud shows that, given the chance, unscrupulous people can, will, and do convince unsuspecting members of the public to part with their money with unsubstantiated promises of high returns, or simply by mismanaging the funds with which they have been entrusted. Lowering barriers to entry in the manner Dr. Byrne describes on a decentralised platform like Counterparty is likely to encourage this mischief, and cause harm to the investing public to such a degree as to easily outweigh the benefits;
- *fifth*, corporates will want to ensure their securities are not traded in contravention of applicable law - for example, not being traded into and out of sanctioned countries such as North Korea - which the Counterparty vision is expressly designed to circumvent; and

- *sixth*, Counterparty is untested - there may be security holes of which we are not yet aware, only one of which would be sufficient to introduce the possibility of substantial losses for its users.

“Any corporate of consequence will therefore have almost no incentive to use Counterparty to list. In the short-term, it seems likely that the platform will be used by fringe crypto-equity issuers who are willing to sell what they purport to be financial instruments over the blockchain without complying with the necessary formalities. Although this may seem an acceptable solution for cryptocurrency enthusiasts, anyone issuing or investing in such products does so at their peril - it is all but certain that these issuances contravene the accredited investor statutes and public offering rules, and the likelihood of obtaining adequate remedies against a purely blockchain-based enterprise in the case of fraud or default is low if not non-existent.”

Preston Byrne concluded by opining that, “There are numerous ways to use blockchains to democratise access to finance. Crypto-equity is not one of them.”

Legal realities

Part of the current narrative popular on social media such as Reddit and Twitter is that Bitcoin’s cryptographic code, being nigh-unbreakable by law enforcement and other judicial authority, will itself act as a form of “law” transcending all jurisdictions. Two notable examples being that of Mircea Popescu of MPex who asserted Bitcoin’s sovereignty in response to an SEC investigation as well as Trendon Shavers (‘pirate40’) who was charged by the SEC for running a \$4.5 million Ponzi scheme through a firm called Bitcoin Savings & Trust.⁸⁹¹ In fact, due to the numerous scams and thefts that continue to occur with these types of investments, in May the SEC issued an investor alert related to bitcoin and other virtual currencies.⁸⁹²

Yet, in reality, the edges of the network still interact with physically sovereign entities – and Bitcoin is not a sovereign. Just like the “s” in “https” does not make a user less immune to legal sanction, so does ECDSA not absolve illegal conduct by users of the blockchain.

For example, below is a part of an interview between Juan Llanos, executive vice president of Bitreserve and David Landsman, Executive Director of the National Money Transmitters Association (NMTA):⁸⁹³

JL: I understand you have been in touch with Bitcoin industry members. What have those discussions been like? How do their approaches and strategies compare to yours or the NMTA’s?

DL: Most Bitcoiners I have spoken to are not aware of their legal environment, or in a state of deep denial. It is not only about the federal and state legalities I mentioned above. They lack of awareness of the direct culpability society attaches to the Bitcoin dealer, if it later turns out that his Bitcoin customer dealt in drugs, terror, human smuggling, copyright infringement, hacking, or any type of criminal activity. How could

you have known, you say? You are not responsible, you say? Well, it is your responsibility, they say, to develop a credible 'Know-Your-Customer' program, one that is 'reasonably designed' to prevent, detect and report illegal money that moves through, or is in any way facilitated by, your company.

This is not an endorsement of any particular policy but rather is a report on what is actually going on versus what some advocates hoped would go on.

In accounting there is a principle called "substance over form" which is used to calculate the financial reality of an entity instead of just the legal form of the transaction. In other words, it is used to characterize transactions: although the parties may adopt different legal terminology or other descriptions to try to characterize their transactions as a gift, or a sale of a product, or some other thing, a regulator will classify a transaction in accordance with the function that transaction carries out. This is roughly equivalent to "the spirit of the law" and not necessarily the letter of the law.

For instance, while each jurisdiction has its own set of standards, the sale of cryptocurrency tokens in a pre-sale context is often described by its promoter as a sale of a software product, when in fact the law will probably look at the transaction as an investment contract which is subject to public offering rules. Although given the newness of the technology there may not be a direct precedent dealing with cryptocurrency tokens in existing case law, the overall regulatory code and controls may be likely to classify each pre-selling transaction as a sale of securities – and the purported description of these tokens as software products may not stand up to regulatory scrutiny.

This point is raised not to endorse or oppose specific laws or policy, but consider for the moment the problem if a large pre-sale takes place and subsequently regulatory intervention results in a regulatory injunction in the form of an asset freeze and a cease-and-desist order. What would happen if, suddenly, the SEC or a similar authority brought proceedings against the individuals or entity operating the pre-sale? Would the platform the pre-sale was designed to fund be doomed? What liability would the pre-sale's promoters incur? And would it be likely that a pre-sale model – one which has been prevalent to date in the cryptocurrency space – would continue to be viable if regulatory sanction were actually undertaken? These questions are what

Another hypothetical example, Bob's bank in the UK creates a contract (or smart contract) that links the performance of UK gilts (Treasury bonds) to a cryptoledger with the intent to sell to individuals in countries with strict capital controls such as Vietnam. While there may not be a regulation in Vietnam that explicitly prevents or forbids its residents from buying this specific type of contract, the overall regulatory code and controls suggests that this type of contract would probably not stand up to a lawsuit from the Vietnamese government.

Consider for the moment the possibility that Bob's bank built up a large client base in Vietnam including Alice, a high net-worth individual. What would happen if her smart contract was

stolen as happens with bitcoins? How could she rectify this situation with the knowledge that the Vietnamese regulatory framework does not permit such exchange?

Or as Dan Kervick explained in March 2014:⁸⁹⁴

Conventional digital payment platforms continue to evolve, and will eventually be able to accomplish all that Bitcoin achieves, but without the risks that come from using a clandestine payment system that can't be easily and directly regulated and in which contracts can't be legally upheld and disputes legally resolved without a lot of time-consuming and cost-adding investigative headaches. The very existence of a system of market exchange based on private property rights presupposes and depends on a legal system that can efficiently assign and uphold those rights. A market system and a legal system are two faces of one and the same animal.

Kervick's view was not popular with many Bitcoin advocates, but it is arguably an accurate prediction of how these cryptocurrency and cryptolledger systems will interact with real world jurisdictions.⁸⁹⁵

For instance, on July 17, 2014 the New York State Department of Financial Services (NYDFS) announced its proposed regulations of virtual currencies in what is called a "BitLicense."⁸⁹⁶ While this book has briefly discussed the proposed regulatory framework, these regulations will not be finalized until later this fall.

James Duchenne recently explored several of these twenty-one sections currently outlined in the NYDFS draft.⁸⁹⁷ Noting:

Now, the biggest danger to the start up scene is not the paperwork and oversight of BitLicensees it aims to generate but Part 200.8 (a), its capital requirements. This is, in effect, a bond commensurate with the risk of conducting business and will vary between BitLicensees. Where a centralized repository of private keys is envisaged, I think this is appropriate as is the case in the finance industry (and also in other industries, for example, EPA facility remediation licence bond). However, where a BitLicensee doesn't have control of a customer's private keys, that requirement is logically limited to safeguard against platform malfunctions. This is not easy to quantify. Take for example hardware wallets, such as Trezor, where a defective product could also lead to significant loss of funds and a replacement of the device wouldn't be appropriate as restitution. While parallels can be drawn with cash in a normal wallet, due to the potential quantum of losses and the technological expertise required in hardware digital currency wallets, it is not farfetched to see damages being sought from a company if the loss was foreseeable from a best practice industry point of view. In this instance, it is unsure whether the quantum of the capital requirements could be adequately calculated or that it would even be effective.

These capital requirements will actually serve as a barrier to entry that other competing altplatforms must hurdle over to compete in. The fact that startups such as Pebble (not the watch company), Coinaaa, Stellar and Hyperledger and any other coin-issuing platform may need to raise large sums of funds to meet capital requirements effectively limits the playing field to Bitcoin and the coins that have launched thus far.⁸⁹⁸ This is not to say that the existing coins will necessarily be grandfathered in and excused of such requirements.

Continuing Duchenne notes that:

The effects of Parts 200.3 and 200.21 are skewed towards current financial industry participants, operating digital currency ventures and also raise some questions regarding consumer use. First, in a level playing field all businesses, whether or not they are banks, should be made to comply with the rules. Where compliance with the rules already exists under another legislative scheme, it follows that these won't have to be reconsidered although a gap-analysis, as a minimum, should be provided. On the other hand, currently operating digital currency ventures may benefit of an average of between 45 days and 120 days of continued operation (maximum time for the Superintendant to consider licensing – though this can be varied). This is nearly 4 ½ months of operation whereas a new entrant won't be allowed to operate for the same time frame and generate revenue. Part 200.3 (c)(2) allows consumers to “solely” utilize Virtual Currency for the purchase or sale of goods or services. Does this prevent peer-to-peer bitcoin lending, bitcoin investment directly in companies, participating in derivatives market and/or holding bitcoin as a speculative currency investment? It is argued that this rule may have to stand up against a bevy of other legislative provisions, precedents and even the concept of money as free speech. Time will tell.

Again, readers should consult with an experienced attorney before embarking on specific entrepreneurial activities in this space. Yet if Duchenne's interpretation is correct, that could mean that start-ups should launch as soon as possible as their grace period is drastically shortened after this law comes into effect.

Current participants may not like any or all of these regulations. Still, as Antonis Polemitis recently pointed out, the auto industry survived Red Flag laws (also called the Locomotive Act) and, for its part, Bitcoin could survive BitLicense as well.⁸⁹⁹ Red Flag laws were enacted in the UK and US in the late 19th century that required drivers to wave red flags to warn pedestrians and bystanders that the vehicle was approaching.

Whether or not Bitcoin and its descendants will be able to competitively maneuver will be a question that can only be answered several years down the road. If history is any guide, BitTorrent may have lost substantial market share over the past decade (down from a peak of 60% to 7%) but it continues to exist despite both regulations and well-capitalized competitors.⁹⁰⁰ Perhaps Bitcoin will be positioned somewhere between the two precedents.

Chapter 18: 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 despite its numerous warts some perceive it as good enough.

Throughout this study we have learned that all but five of the Bitcoin core developers are effectively 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 contributors are conservative in adding new features. Consequently it appears there is a market-mismatch which can be capitalized on: 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 throughout the book, there are numerous incentives that are being overlooked in discussions regarding challenges within the ecosystem such as a lack of financial incentives for attracting scarce talent to work the core protocol. One solution is for mining farms and pools to hire core developers yet this voids the separation of powers, the multipartite system that exists. Consequently pursuing this will likely trend towards collusion and cartelization at the expense of decentralization.

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. While this is not an endorsement of their services, firms such as Ripple Labs and Stellar are likely better positioned in that they are the custodian of a protocol creating a known chain-of-command (e.g., clear governance) and are only able to extract value from the network from the native token (e.g., XRP, stellar) which provides an incentive to manage and create value to the network (i.e., skin in the game). In addition, a proof-of-stake system along with consensus ledgers (Ripple and Stellar protocols), are increasingly ideal candidates for distributing trust as they require significantly less capital to securely operate.

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. Consequently, because of the variance rewards that miner's face which drives economies of scale leading to centralization of farms and pools, the network is vulnerable to additional collusion from an oligopoly of transaction providers in the coming months and years; it technically happens today through peering agreements.

Two of the underutilized capabilities that could be used to incentivize continued participation once block rewards lessen are merged mining and atomic transactions. Tying the two

technologies together may provide new functionality to the ecosystem for experimentation; yet neither solves the deepening centralization issue.

Thereupon special interest groups will continue to exert pressure to include (or not include) certain features into the Bitcoin blockchain. Lobbying and politicking and even cyber bullying on social media will likely increase due to a “public goods” issue described in various dimensions. For instance, “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 phenomenon (e.g., inflation) by giving speeches and announcements (“Whip Inflation” by Ford and Carter). However, economic indicators are not a cartoon character. Similarly, attempts to “jawbone” the cryptocurrency marketplace regarding altcoins will not work because 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.

Furthermore, Bitcoin will not fail simply because scarce resources (e.g., human capital) are attracted to other competing projects. The automobile, train, shipping and aerospace industries did not collapse because of an influx of competitors. This would be akin to saying the Linux community should rally behind one and only one Linux distribution. Distributions have come and gone, in fact, Slackware was created in 1993 and is the oldest remaining distribution. Yet despite a multitude of competitive forces and consumers using many different distributions, Linux in the form of Android, is now a widely used tool on smartphones and some tablets – not just servers.⁹⁰¹ The idea was bigger than the first-mover (or second, or third).

Consequently, 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.⁹⁰²

In terms of on-ramping utility, edge providers such as Coinbase and BitPay and trading platforms like Kraken, Atlas ATS and Bitfinex provide new functionality beyond simple exchanges, creating new utility to the ecosystem and could conceivably act as digital currency clearing houses if absorbed into existing financial institutions.

Lastly, these tools, like any database, are agnostic and open-source, enabling new parties irrespective of ideology to utilize them. Consequently, enterprise-oriented well-capitalized organizations could eventually deploy a variety of cryptoledgers which are used internally and externally for a sundry of motives (as noted by the potential 84 uses-cases).

Moving forward

As more professional research is conducted on Bitcoin, arguably the more it seems as if Satoshi Nakamoto may not have fully understood what he was inadvertently doing. If nothing else, he

has given the world a visual aid – a terrarium – on what a deflationary economy looks like in near-real time and how it would – generally speaking – not be pleasant to live in. To be fair, it is unclear if he could have foreseen all of the issues that Sams, Dillinger, Levin, Ametrano, Hanley and Babbitt – among many others cited – have discussed throughout, but the inelastic supply and sticky wage issue is something that suggests he probably had certain philosophical leanings. Or maybe he was trying to see if such a system would work too and just did not know. We may never know and in retrospect that is no longer important as the code itself has turned into a ship of Theseus.⁹⁰³

How does this impact your own future decisions as a developer, entrepreneur, investor, educator, attorney or policy maker?

In 1995, Warren Buffett's longtime business partner, Charlie Munger, gave a speech at Harvard discussing the psychology of human misjudgement.⁹⁰⁴ The abridged version in short: when people get financially invested in something, they get emotionally invested, which leads to bias (e.g. confirmation bias) and then misjudgment, and in financial matters that tends to lead to losses. Today there is an entire field of study called behavioral finance – a subset of behavioral economics – which chronicles and analyzes this phenomenon: why market participants with relevant up-to-date information still make systematic errors including overconfidence, unrealistic optimism and hubris. This includes investors of Enron, WorldCom, Kodak and most recently RIM and Nokia.

Consequently with Bitcoin, the world has seen speculative euphoria before and it is impossible to predict when this could stop – especially when you have such large emotional buy-in from passionate adopters.

BitLicenses may become common place globally in the next few years and according to this narrative, existing financial institutions will get involved, bidding up the token to new highs and shortly thereafter, mainstream adoption as a medium-of-exchange will take place. That could happen, in fact, the first part of that theory may play out as seasoned Wall Street traders look for new ways to practice their arbitrage acumen. But the latter is unlikely to for the reasons detailed in this study. Or in other words, investment firms could trade ETFs and continue to treat the token as a commodity, yet aside from a few niches, it will not be used as a currency because it does not have competitive attributes as one. Though this may not matter because it could be the only game in town through what is in effect, a licensed monopoly.

Skeptics could always be wrong, maybe this is all a replay of the Xerox 'Memo of the Month.'⁹⁰⁵ Perhaps the currency or commodity aspect of bitcoin will grow beyond the niches of remittances (in corridors such as Southeast Asia), day trading and black markets.⁹⁰⁶ Or maybe, the current Cambrian explosion in altcoins repeats what Akinobu Kuroda elucidated of 18th century Bengal, where Dacca residents had 52 kinds of coins of different weights and measurements in circulation, each with a specific "circuit" (layered market) and use-case that

fluctuated cyclically during the year.⁹⁰⁷ Or conversely, perhaps BitLicenses will effectively insulate Bitcoin from these competitive altcoins.⁹⁰⁸

It is impossible to predict the future or to know *a priori* what the market will eventually adopt. And conceivably the concerns raised in this study are not necessarily show stoppers but mere bumps in the road. In fact, the age of Bitcoin may have just been given prosthetic legs at the expense of other cryptoledgers and distributed applications. Time will tell on this front.

About the author



Tim Swanson is a graduate of Texas A&M University and worked in East Asia for more than six years. He is the author of [Great Wall of Numbers: Business Opportunities & Challenges in China](#) and [Great Chain of Numbers: A Guide to Smart Contracts, Smart Property and Trustless Asset Management](#).

He can be reached at: tswanson@gmail.com

Keep up to date with further information at: www.OfNumbers.com and Twitter: [@ofnumbers](https://twitter.com/ofnumbers)

Endnotes

- ¹ [Bitcoin: a Money-like Informational Commodity](#) by Jan Bergstra and Peter Weijland
- ² [Formalising the Bitcoin protocol: Making it a bit better](#) by W.J.B. Beukema
- ³ Personal correspondence, July 29, 2014. I would like to thank Dave Babbitt for his insights and clarification of these points.
- ⁴ [The 8 identities of Bitcoin](#) by William Mouyagar
- ⁵ 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). Similarly I remove the space between “block” and “chain.”
- ⁶ The author, Satoshi Nakamoto (a pseudonym), states early in the 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](#)
- ⁷ [Bitcoin is Worse is Better](#) by Gwern Branwen
- ⁸ [The History of ACH Payments](#) from Piracle
- ⁹ See [How do bitcoin transactions work?](#) from *CoinDesk* and [How the Bitcoin protocol actually works](#) by Michael Nielsen
- ¹⁰ 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
- ¹¹ 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.
- ¹² 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 and [Why can't Diffie-Hellman be used for signing?](#) from StackExchange
- ¹³ I would like to thank Stephan Kinsella for describing and clarifying this point.
- ¹⁴ [Rivalrous goods](#)
- ¹⁵ [Wet code and dry](#) by Nick Szabo
- ¹⁶ 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.
- ¹⁷ As one reviewer noted, “My first attempt at trying to reconcile the underlying workings of the protocol with legal systems ended in a simple observation. In the eyes of the Bitcoin protocol ownership is conflated with possession. In ordinary society we make a distinction and have created a society that revolve around property rights. This makes it difficult to impose an existing legal structure to Bitcoin directly. As the Bitcoin ecosystem has evolved to contain more third party providers, its current usage actually brings it much closer to concepts that are more familiar to the existing legal systems with people possessing rights over Bitcoins. However the legal definitions concerning the underlying protocol remains difficult to pin down. In order to come up with a legal framework that will endure it is necessary in my opinion to get to grips with the way that the Bitcoin protocol enforces the contracts that take place within the Bitcoin network rather than entirely on the way it is currently used.”
- ¹⁸ This is sometimes spelled seignorage but means the same thing. See [Seignorage](#) from About.com
- ¹⁹ 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 and Peter Weijland
- ²⁰ [The Marginal Cost of Cryptocurrency](#) by Robert Sams
- ²¹ [Marginal revenue and marginal cost](#) from Khan Academy

-
- ²² 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.
- ²³ 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 cryptolodger, see [Turing complete language vs non-Turing complete \(Ethereum vs Bitcoin\)](#)
- ²⁴ 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*
- ²⁵ [Washing virtual money](#) from *The Economist*
- ²⁶ See [tweet](#) from Adam Back; and also [The estimated number of hashes of work in the blockchain just passed 2^80](#) by Peter Wuille
- ²⁷ 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](#). 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
- ²⁸ Or a species of the genus “double-spend attack. 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
- ²⁹ 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
- ³⁰ See [Bitcoin Mining Explained Like You’re Five: Part 2 – Mechanics](#) by Chris Pacia and [The Marginal Cost of Cryptocurrency](#) by Robert Sams
- ³¹ This effectively means that there could be billions of contracts, not just 21 million.
- ³² [The Rewards For A Bitcoin Miner](#) by Dave Hudson
- ³³ [The Bitcoin Central Bank’s Perfect Monetary Policy](#) by Pierre Rochard
- ³⁴ 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*, [Bitcoin Startup Xapo Sets \\$40 Million Fundraising Record](#) from *Bloomberg* and [Bitcoin Security Firm BitGo Raises \\$12 Million](#) from *The New York Times*
- ³⁵ The numbers vary according to source, as of this writing [Bitinfocharts](#) lists 25 GB.
- ³⁶ [Fake gold bars turn up in Manhattan](#) from *MyFoxNY*
- ³⁷ While he did not coin the term, Heinlein popularized it in his novel, *The Moon is a Harsh Mistress*
- ³⁸ This price fluctuates, see [Bitcoin – A Jack of All Trades is the Master of None](#) by Ken Griffith
- ³⁹ [Why the payment card system works the way it does – and why Bitcoin isn’t going to replace it any time soon](#) by Richard Gendal Brown
- ⁴⁰ [Birth of the Chaordic Age](#) by Dee Hock
- ⁴¹ For another discussion on debit cards see [The sad truth: XAPO international debit card vs. most European debit cards](#) and also [Why are bitcoins always compared to credit cards? One is an asset instrument, the other a debt instrument](#). from reddit

⁴² I would like to thank Robert Sams for his feedback clarifying the strict versus extended definition of seigniorage in this section.

⁴³ Research presented by Kay Hamacher, Stefan Katzenbeisser in December 2011 suggests that at that time, bitcoins were actually “elastic” in that they could be used as money substitutes. At the time of the presentation, the market value of a bitcoin was \$3. See [Bitcoin - An Analysis \[28C3\]](#)

⁴⁴ [Dispelling some myths about Bitcoin, from a Bitcoin fan](#) from L.M. Goodman

⁴⁵ From definition of [CAP theorem](#)

⁴⁶ [HyperDex](#) by Sirer *et. al.* and [Datomic](#)

⁴⁷ [Academics Spy Weaknesses in Bitcoin’s Foundations](#) from *Technology Review*

⁴⁸ [How ArtForz changed the history of Bitcoin mining](#) by Tim Swanson

⁴⁹ As noted in [Bitcoin: Cryptographic Texture](#) by Tomáš Rosa “[T]his was the intent as the PoW is nothing but a cryptanalytic problem that we believe there is no better way to solve it than using a brute force.”

⁵⁰ See Hashcash.org and [Episode #77](#) from *Let’s Talk Bitcoin*. Last year Back published a [brief autobiography](#) on BitcoinTalk.

⁵¹ Pool chart as of August 3, 2014: <http://bitcoinchain.com/pools>

⁵² See [Re: \[ANN\]\[XCP\] Counterparty Protocol, Client and Coin \(built on Bitcoin\) - Official](#)

⁵³ 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

⁵⁴ 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.](#)

⁵⁵ Tweet permalink: <https://twitter.com/jgarzik/status/429058872725102593>

⁵⁶ 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*

⁵⁷ [Episode 99](#) of *Let’s Talk Bitcoin*

⁵⁸ One reviewer thought that “mining warfare incentives” would accurately describe these scenarios.

⁵⁹ [Selfish Mining: A 25% Attack Against the Bitcoin Network](#) by Vitalik Buterin

⁶⁰ 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 the fall of 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*

⁶¹ [Majority is not Enough: Bitcoin Mining is Vulnerable](#) by Ittay Eyal & Emin Gun Sirer and [Selfish Mining: A 25% Attack Against the Bitcoin Network](#) by Vitalik Buterin

⁶² Microtransactions is an arbitrary term, why not “microish” transactions? See [The Mental Accounting Barrier to Micropayments](#) by Nick Szabo and [The Case Against Micropayments](#) by Clay Shirky. Jeff Garzik has a demonstration that purportedly reaches 100 per second. See his [tweet](#).

⁶³ See [Transaction fees](#)

⁶⁴ 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.

⁶⁵ [Permalink](#) to Gavin Andresen’s comment.

⁶⁶ [Gavin Andresen: Rising Transaction Fees Could Price Poor Out of Bitcoin](#) from *CoinDesk*

⁶⁷ [4 New Bitcoin Features Revealed by Core Developer Mike Hearn](#) from *Cryptocoins News*

⁶⁸ 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).”

⁶⁹ [New Study: Low Bitcoin Transaction Fees Unsustainable](#) from *CoinDesk*

⁷⁰ Image from [The Tragedy of the Commons](#) from Penn State

⁷¹ 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 trustless Merkle tree, then there may be 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 investment banks 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.

⁷² [Bitcoin Core Development Falling Behind, Warns BitcoinJ's Mike Hearn](#) from *CoinDesk* and [Mike Hearn: Underfunding is Leaving Bitcoin Development in Crisis](#) from *CoinDesk*

⁷³ [Mike Hearn: Underfunding is Leaving Bitcoin Development in Crisis](#) from *CoinDesk*

⁷⁴ [Unilateral Statement Regarding Mt. Gox from 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*

⁷⁵ 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.

⁷⁶ [Bitcoin Raises Washington Profile, to Silicon Valley's Dismay](#) from *Bloomberg*

⁷⁷ According to [Investopedia](#): “A postulated antithesis to fragility where high-impact events or shocks can be beneficial. Anti-fragility is a concept developed by professor, former trader and former hedge fund manager Nassim Nicholas Taleb. Taleb coined the term “anti-fragility” because he thought the existing words used to describe the opposite of “fragility,” such as “robustness,” were inaccurate. Anti-fragility goes beyond robustness; it means that something does not merely withstand a shock but actually improves because of it.”

⁷⁸ [Banning, Dumping and Attacks on Mining: Could Bitcoin be Hijacked?](#) from *CoinDesk*. Greg Maxwell has mentioned this issue several times, that when Bitcoin breaks, he has to fix it – it is not anti-fragile.

⁷⁹ Reminiscent to the quote Henry Kissinger purportedly said, “Who do I call if I want to call Europe?” See [The audacity of bitcoin](#) by John Normand and [Kissinger says calling Europe quote not likely his](#) from *The Associated Press*

⁸⁰ 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.

⁸¹ 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

⁸² [CrowdCurity](#), [Eris](#) and [Lighthouse](#)

⁸³ One notable piece outside of academia is [Markets, Institutions and Currencies – A New Method of Social Incentivization](#) by Vitalik Buterin

⁸⁴ [Coinometrics](#)

⁸⁵ Personal correspondence, March 26, 2014

⁸⁶ See [Auroracoin - Forked and Game Over](#) on Bitcoin Talk and [comments](#) on *Hacker News*

⁸⁷ It should be noted that only if that size cannot meet all current demand, which is not the case today.

⁸⁸ [Nash equilibrium](#) – N players making the best decision available to them while knowing the decisions of all other players, who are also making the best decision they have available.

⁸⁹ [The Bitcoin mining game](#) by Nicolas Houy

⁹⁰ 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*

⁹¹ 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?](#)

⁹² I would like to thank Jonathan Levin for clarifying this issue for me.

⁹³ [Creating a decentralised payment network: A study of Bitcoin](#) by Jonathan Levin

⁹⁴ [Back-of-the-envelope calculations for marginal cost of transactions](#) by Gavin Andresen

⁹⁵ [Dr. Bitcoin E02: The Unproven Hypothesis](#) by Paul Rausch

⁹⁶ [Mike Hearn on Coming Bitcoin Protocol Updates](#) from *Money & Tech*

⁹⁷ [Creating a decentralised payment network: A study of Bitcoin](#) by Jonathan Levin

⁹⁸ [Bitcoin Transaction Fees To Be Slashed Tenfold](#) from *CoinDesk*

⁹⁹ [Whatever happened to the 10X reduction in transaction fees? I'm still paying \\$.06 a transaction. If we want this to be of use to the poor, this is something that needs to be fixed.](#) from reddit

¹⁰⁰ [Bitcoin, Ethereum and Pigou: the economics of transaction fees](#) by Robert Sams

¹⁰¹ [Pigou tax](#) – A tax to compensate for costs incurred by others.

¹⁰² [On Transaction Fees, And The Fallacy of Market-Based Solutions](#) by Vitalik Buterin

¹⁰³ [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.

¹⁰⁴ [Tezos: A Self-Amending Crypto-Ledger Position Paper](#) by L.M. Goodman

¹⁰⁵ I have discussed some of these educations in a presentation given on April 27, 2014 ([video](#)) ([slides](#))

¹⁰⁶ 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.

¹⁰⁷ [Episode 99](#) of *Let's Talk Bitcoin*. Adam Back proposed a few a potential solution to this issue and several other hurdles discussed in the book, although it could lead towards more centralization down the road. This announcement was made on April 8 and no new information has been made publicly available.

¹⁰⁸ Over the past four months, a significant amount of public debate has taken place between developers such as Peter Todd, Adam Back, Alex Mizrahi, Andrew Miller and Greg Maxwell over the advantages and disadvantages of sidechain technology. On the one hand it does provide new extensibility but on the other it likely enhances and/or incentivizes more centralization. See [Why do people think that side-chains are going to be secure?](#) by Alex Mizrahi and this [long twitter debate](#).

¹⁰⁹ [Even faster block-chains with DECOR protocol](#) and [DECOR+](#) by Sergio Lerner

¹¹⁰ [Stress Test Prepares VisaNet for the Most Wonderful Time of the Year](#) from Visa

¹¹¹ [Gartner: AWS Now Five Times The Size Of Other Cloud Vendors Combined](#) from *readwrite*

¹¹² [Dispelling some myths about Bitcoin, from a Bitcoin fan](#) by L.M. Goodman

¹¹³ Chart via: <https://blockchain.info/charts/hash-rate> and for more mining pool, network, and exchange analysis see, [Neighbourhood Pool Watch Bitcoin](#)

¹¹⁴ [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.”

¹¹⁵ 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](#)

¹¹⁶ Vitalik Buterin [labels it](#) a prototype, stating: “As *Let's Talk Bitcoin's* Daniel Larimer [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?”

¹¹⁷ 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?

¹¹⁸ 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](#))

¹¹⁹ See [The Shareholder vs. Stakeholder Debate reconsidered](#) by Rüdiger W. Waldkirch and [How to Bureaucratize the Corporate World](#) by Ben O'Neill

¹²⁰ The ratios were probably higher the first several years because of the amount of “cons” and “scams” that were pervasive. Venture capital and angel funding could reduce this as they bring professionalism to the market. 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*

¹²¹ [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

¹²² [The Marginal Cost of Cryptocurrency](#) by Robert Sams

¹²³ JP Koning discusses these *moneyness* aspects including capital accumulation at [Moneyness](#)

¹²⁴ Jeff Garzick [suggests](#) that “Blockchain tech is a new type of [eventual consistency](#) database.”

¹²⁵ 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

¹²⁶ [Developers Battle Over Bitcoin Block Chain](#) from *CoinDesk* and reddit [comments](#)

¹²⁷ 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 1/30th 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.”

¹²⁸ See [Association of Licensed Automobile Manufacturers](#)

¹²⁹ 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

¹³⁰ 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.

-
- ¹³¹ See [An Introduction to BIP70](#) by Kevin Greene and [Coinbase Adds Bitcoin Payment Protocol For Safer Transactions](#) from *CoinDesk*
- ¹³² This comment has since been removed from the forum by the user.
- ¹³³ Not to reuse the same reference, but this is also 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*
- ¹³⁴ If all pool operators were contactable, does not petitioning their opinion and vote amount to little more than lobbying, 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).
- ¹³⁵ [E77 – The Adam Back Interview](#) from *Let’s Talk Bitcoin* and [Re: \[Bitcoin-development\] Tree-chains preliminary summary](#) by Peter Todd
- ¹³⁶ Currently capital expenditures represent the bulk of costs (e.g., chip advancement is very expensive) and consequently CAPEX costs dominate the OPEX costs.
- ¹³⁷ In the economic sense, a more accurate term is “traded,” in the thermodynamic sense, nothing is destroyed. The exergy is essentially “converted” from the thermodynamic viewpoint and the security is more like “traded” from the economic viewpoint.
- ¹³⁸ My thanks to Robert Sams of [Cryptonomics](#) for pointing this out.
- ¹³⁹ This issue dovetails into more complex discussions involving legal tender laws. Enacting monetary and fiscal policies by fiat has its own series of drawbacks (i.e., interest rates can arbitrarily be set by committee, but these can create time-preference distortions).
- ¹⁴⁰ [The Marginal Cost of Cryptocurrency](#) by Robert Sams
- ¹⁴¹ For more about the economic inputs and outputs of mining on the Bitcoin network see, [Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms](#) by David Evans
- ¹⁴² Amortized costs, by definition, are fixed and are therefore irrelevant to the decision to turn the machine on or off (those costs are only considered when deciding to invest in a new machine or not). Before setting up, professional miners will look at calculations for recouping their operating costs and upfront investments (such as hardware, physical plant and real estate).
- ¹⁴³ More specifically, bitcoin price is a function of supply, current demand in the economy, and future demand discounted to present value.
- ¹⁴⁴ [Facebook Has Spent \\$210 Million on Oregon Data Center](#) from *Data Center Knowledge* and [Large Crack Found in Dam Supporting Quincy Data Center Cluster](#) from *Data Center Knowledge*
- ¹⁴⁵ [ASICs and Decentralization FAQ](#) by Andrew Poelstra
- ¹⁴⁶ Or in other words, network difficulty is an arbitrary metric in and of itself. The probability of success refers to an attacker amassing more than 50% of the hashrate (e.g., 51% attack). You could burn enormous amounts of electricity with CPUs yet fail to generate any meaningful hashrate to attack the network. An ASIC may be able to generate more hashrate than a single CPU but quantity is not the same as quality. One way to measure the quality of the security for a decentralized network is whether or not there are an increasing or decreasing amount of nodes. In this case, centralization of the hashrate has taken place leading to a qualitatively less secure network (due to less decentralization).
- ¹⁴⁷ One reviewer wrote in response to Poelstra’s paper: “this equating of decentralization with security is naïve. Bitcoins have huge theft problems. How many dollars have been stolen traversing Mastercard or Visa payment systems? It happens, but it’s a small fraction of dollars that go through. And that theft is not actually in the system itself. Nobody has ever attacked Visa and hacked through a transaction.”
- ¹⁴⁸ [\[ANN\] High-speed Bitcoin Relay Network](#) by Matt Corallo and [The Future of Bitcoin: Corporate Mines and Network Peering?](#) from *Data Center Knowledge*
- ¹⁴⁹ Personal correspondence, April 8, 2014. See also, [Bitcoin Hurdles: the Public Goods Costs of Securing a Decentralized Seigniorage Network which Incentivizes Alternatives and Centralization](#) and [Bitcoin Block Propagation](#) Speeds by Ittay Eyal and Emin Sirer
- ¹⁵⁰ [Bitcoin mining profitability calculator](#) from BitcoinX
- ¹⁵¹ [Hash Rate Headaches](#) by Dave Hudson
- ¹⁵² [Megawatts Of Mining](#) by Dave Hudson
- ¹⁵³ [Bitcoin network: computation speed growth](#)

-
- ¹⁵⁴ [Reward halving is approaching fast due to sustained difficulty increase: we are already 103 days early if one starts counting since the last halving](#) from reddit
- ¹⁵⁵ Personal correspondence, June 25, 2014
- ¹⁵⁶ [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.
- ¹⁵⁷ This figure could increase due to numerous undisclosed hardware purchases by private parties including enterprises and investors in this space
- ¹⁵⁸ Data for Figure 1 came from: [CoinDesk BPI](#), [BitInfoCharts – Litecoin](#), [BitInfoCharts – Namecoin](#). Note that Namecoin prices generally track Bitcoin at a 0.005 ratio. The weighted token average is a rough estimate and may be off by a standard deviation.
- ¹⁵⁹ One of many instances include [comment](#) #3 from cypherdoc2 on reddit
- ¹⁶⁰ This comment received a lot of criticism, primarily along the lines of how a PoS allegedly cannot provide consensus and Ripple can, but requires some trust and only in a distributed fashion. These issues will likely continue being discussed in future papers, suffice to say that if these systems are vulnerable there should be an economic incentive for them to be hacked. See [Proof-of-stake](#), [Ripple protocol](#)
- ¹⁶¹ Technically speaking, it is like that their (variable) electricity costs that matter significantly more because hardware costs are fixed (e.g., electricity typically costs about 98% of the total cost of mining). The amortized cost of the hardware usually only enters the calculation before the miner buys the system.
- ¹⁶² [Bitcoin Miner Taps Dad's Power Plant in Virtual-Money Hunt: Tech](#) from *Bloomberg*
- ¹⁶³ One reviewer noted that, "There may also be an element of the sunk costs fallacy applying – irrational behavior arising from a psychological aversion to realizing that the amounts they had invested in their mining hardware are now worthless, the shutting down of which would constitute realizing the loss."
- ¹⁶⁴ I would like to thank Jonathan Levin for pointing this out.
- ¹⁶⁵ [The ZeroAccess Botnet – Mining and Fraud for Massive Financial Gain](#) by James Wyke
- ¹⁶⁶ [Gaming Company Fined \\$1M for Turning Customers Into Secret Bitcoin Army](#) from *Wired*
- ¹⁶⁷ [Symantec takes on one of largest botnets in history](#) from *c/net*
- ¹⁶⁸ Fred Trotter, estimates that since January 2009, the mining process of Bitcoin has consumed 150,000 megawatt hours of electricity, which is equivalent to a year's worth of electricity for about 14,000 average U.S. homes. See [Malignant computation](#) from *O'Reilly* and [Bitcoin Miner Taps Dad's Power Plant in Virtual-Money Hunt: Tech](#) from *Bloomberg*
- ¹⁶⁹ [GPU Roaring? You May Be Infected With a Bitcoin Trojan Says Symantec](#) from *Daily Tech*, [World's most dangerous botnet mines Bitcoins](#) from *The Inquirer*, [Security researchers kill Kelihos again after Bitcoin crime spree](#) from *ArsTechnica*, [Cybercriminals Unleash Bitcoin-Mining Malware](#) from TrendMicro, [More users, more attacks: Kaspersky Lab stats show a surge in Bitcoin cybercrime](#) from Kaspersky, [Bitcoin Botnet Mining](#) from Symantec, [IAMA a malware coder and botnet operator, AMA](#) from reddit and [Have there been reports of botnets mining Bitcoin / crypto-currencies?](#) from StackExchange
- ¹⁷⁰ [Botcoin: Monetizing Stolen Cycles](#) by Huang et. al. Another paper from the same team discusses the differences between "light" and "dark" mining pools, [Poster: Botcoin – Bitcoin-Mining by Botnets](#)
- ¹⁷¹ [Microsoft Destroys Bitcoin Mining Botnet Sefnit](#) from *CoinDesk*
- ¹⁷² FPGAs and ASICs are credited for pushing out small botnet operations which still require a certain amount of working capital to maintain which could not be covered with increasingly less competitive hashrate from CPUs nodes. See [Bitcoin & Gresham's Law - the economic inevitability of Collapse](#) by Philipp Güring & Ian Grigg and [A Botnet herder mining Bitcoin](#) from Zooko Wilcox-O'Hearn
- ¹⁷³ [Facebook Breaks Up Cryptocurrency Mining Botnet 'Lecpetex'](#) by *CoinDesk*
- ¹⁷⁴ [How Hackers Hid a Money-Mining Botnet in the Clouds of Amazon and Others](#) from *Wired*
- ¹⁷⁵ Personal correspondence with two mining startups in China.
- ¹⁷⁶ As Jonathan Levin pointed out at an event in Australia, "Because Bitcoin mining is software to be run on computers, there's been a great incentive to invent malware that essentially hijacks computers in order to perform an activity." See [Bitcoin and the obscurity of the blockchain](#) from *CIO*
- ¹⁷⁷ [CoinLab's Alydian files for bankruptcy and reveals debt of over \\$3.6m](#) from *CoinDesk*
- ¹⁷⁸ [A Non-Outsourceable Puzzle to Prevent Hosted Mining](#) by Andrew Miller
- ¹⁷⁹ [Towards Risk Scoring of Bitcoin Transactions](#) by Malte Möser, Rainer Böhme, and Dominic Breuke
- ¹⁸⁰ [US Government Bans Professor for Mining Bitcoin with A Supercomputer](#) from *Bitcoin Magazine*

¹⁸¹ The [Dogecoin defense force](#) is one such group.

¹⁸² Satoshi stated several times that he wrote the code first beginning sometime in mid-2007 and then later wrote the whitepaper to describe it, see the last comment on November 9th, [Re: Bitcoin P2P e-cash paper](#). See also, [What is the Carbon Footprint of a Bitcoin?](#) from *CoinDesk*

¹⁸³ This depends strongly on how investors expect the price to behave in the future and this in turn will determine the ratio of capital expenditure to operating expenditure. It should also be noted that there are only 2 years left in which 1.3 million bitcoins will be created. It will halve again in 2016.

¹⁸⁴ The comparison with MasterCard is not entirely apple's to apple's because it is just processing transactions and not acting as a type of seigniorage entity. There is a lot more that goes into a Visa transaction than their overt energy costs. There are also additional layers in bitcoin but much less. Again, in Mastercard case, they only get transaction cost and energy expended by all the support layers, see [How Merchant Processing Works](#) from IPPAY. Furthermore, MasterCard [spent](#) \$299 million on their capital expenditures in 2013.

¹⁸⁵ As ASICs increase the hash/watt efficiencies, they may run into the limits of [Koomey's law](#).

¹⁸⁶ [E77 – The Adam Back Interview](#) from *Let's Talk Bitcoin* and [Re: \[Bitcoin-development\] Tree-chains preliminary summary](#) by Peter Todd

¹⁸⁷ [\[ANN\] High-speed Bitcoin Relay Network](#) by Matt Corallo and [The Future of Bitcoin: Corporate Mines and Network Peering?](#) from *Data Center Knowledge*

¹⁸⁸ One reviewer noted that "The real mining is done by ASICs, searching for hashes. The blockchain management is done by normal CPU's, they verify the new blocks, calculate which hash-patterns the miners have to search for, and communicate with the Bitcoin network. The blockchain management likely needs good bandwidth and good connectivity, but the communication between blockchain management and the mining hardware should take something like 100 bytes every 10 minutes, a case could be argued that it could work great over protocols like Dtex-P or old GSM-Data or perhaps even Acoustic coupler's. Thus in practice it could be one server in a well-connected datacenter e.g. in Europe or the US, and a place with cheap energy for the miners with at least IP connectivity, it does not need to be broadband. The requirements for the blockchain management might change, but the requirements for the communication between blockchain management and mining should remain stable, independent of the amount of transactions on the bitcoin network."

¹⁸⁹ In doing so this would lead to numerous social engineering issues including regulatory oversight.

¹⁹⁰ Feathercoin had a major problem in the spring of 2013, many large mining pools abandoned it (almost all at once) after the block rewards halved ("halvingday") and as a result the difficulty rating remained very high. During the subsequent month very few blocks were able to be processed because the remaining pools did not have the necessary hashrate to cycle through them, reducing the network to a relative crawl. This hashrate overhang ultimately was solved with a hardfork in the code. A similar decrease, though not nearly as severe, took place with the Bitcoin network in the fall of 2012. Following "halvingday" on November 28, the network remained stagnant. It was not until the new ASIC miners were turned on (first from Avalon) that the hashrate began its upward ascent once more. See Section 2.3 in [CryptoNote v 2.0](#) by Nicolas van Saberhagen (likely a pseudonym)

¹⁹¹ The Bitcoin network, on average, processes roughly 0.7 transaction per second over the past year versus 2,000 per second with Visa.

¹⁹² Robert Sams has written about a number of these issues on [Cryptonomics](#), the quote comes from personal correspondence, April 18, 2014

¹⁹³ One reviewer does not see decentralization as binary. In this instance, once 51% of the hashrate is secured by honest miners, the remainder of the hashrate – for security purposes – is deadweight.

¹⁹⁴ Arguably the most important tool for miners and mining operators is a mining profitability calculator which helps estimate operating costs and revenue generation. One popular version is the [Bitcoin](#) calculator.

¹⁹⁵ These are lower bound estimates based on a weighted token over the corresponding time frame. The actual number is likely higher.

¹⁹⁶ These exceptions are 1) botnets, 2) hobbyists, 3) education & research, 4) political actors, 5) "honest" miners who are speculating that the price will increase whereupon their costs are paid for. Four of these are discussed in [Learning from Bitcoin's past to improve its future](#)

¹⁹⁷ My thanks to David Merfield for concisely describing this phenomenon.

¹⁹⁸ This creates centralization issues which in turn leads to social engineering issues (such as regulations, taxes, and vulnerabilities to organized criminals).

¹⁹⁹ A block reward halving creates a dilemma for miners. In a nutshell they are being asked to continue providing the same amount of labor for half the wages. As a consequence, many will leave and focus on other more profitable jobs (such as altcoins). This was illustrated best with what has happened to Dogecoin throughout 2014.

²⁰⁰ If it looked like something like that (a large jump in prices) were happening, the Bitcoin network would be dramatically “oversecured” and miners would likely switch to an altcoin with a much lower inflation rate.

²⁰¹ [Bitcoin mining firm CoinTerra signs multi-megawatt datacentre deal](#) from *ComputerWeekly*

²⁰² [Bitcoin Hardware Player BitFury Enters Cloud Mining With 20MW Data Center](#) from *Data Center Knowledge*

²⁰³ Google | [Data Centers Finland](#), see also [DCD industry census 2013: Data center power](#) from Datacenter Dyanmics

²⁰⁴ See [BFSB Finland](#) and [Bitcoin sysselsätter i Kimito](#)

²⁰⁵ [BitFury Announces Hosted Mining Services](#) from *Venture Beat*, [BitFury Announces Hosted Mining Services for Business Customers](#) from *CoinDesk* and [Bitcoin Startup BitFury’s CEO Earlier Repped ‘Notorious Market’ Ex.ua](#) from *The Wall Street Journal*

²⁰⁶ [Will Industrial Mining Become the Next Big Bitcoin Investment Sector?](#) from *CoinDesk*

²⁰⁷ [Bitcoin Infrastructure May Grow by \\$600M in Second Half of 2014](#) from *Data Center Knowledge*

²⁰⁸ NRE stands for [non-recurring engineering](#). See [Bitcoin and The Age of Bespoke Silicon](#) by Michael Taylor

²⁰⁹ [Design of Ion-Implanted MOSFET’s with Very Small Physical Dimensions](#) by Dennard *et. al.*

²¹⁰ [SP10 Dawson - Mid June Batch](#) from Spondoolies

²¹¹ [SP30 Yukon September Batch 2](#) from Spondoolies

²¹² There is no such thing as “free” electricity only cheaper or more abundant. Solar panels (which are also depreciating capital goods) still require upfront costs which are amortized over their lifetime (usually 10-20 years). And the (unseen) knock-on effects of pollution and emissions from the creation of those solar panels needs to be quantified – the supply chain to create these tools which tap into renewable energy needs to be accounted for in such a calculation.

²¹³ [ASICs and Decentralization FAQ](#) by Andrew Poelstra

²¹⁴ See [Dennard scaling](#), [Kooomey’s Law](#) and [Ultimate physical limits to computation](#) by Seth Lloyd

²¹⁵ This is not a complaint about capital savings. One argument could be made that savings creates reserve demand for a currency. Yet in practice, virtually no one spends the token treating it much like a commodity or collectible like a stamp. Thus the term “cryptocurrency” is debatable and in practice it is more akin to a commodity, see [Bitcoin: a Money-like Informational Commodity](#) by Jan Bergstra and Peter Weijland

²¹⁶ This figure is generated by the following: 656250 bitcoins mined each year following the block halving multiplied by \$1 million per token. As of 2012, the nominal GDP of Switzerland \$631 billion.

²¹⁷ See [Regulatory capture](#). There are several proof-of-stake systems under development, yet thus far they have all failed key vulnerability tests leading to some kind of centralization verification process. See also [What Are Bitcoin Nodes and Why Do We Need Them?](#) by Daniel Cawrey

²¹⁸ [Malignant computation](#) by Fred Trotter

²¹⁹ Disclosure: I do not own any litecoins nor do I maintain or operate any mining machine of any kind today.

²²⁰ According to one statistical analysis, from between its April 2012 announcement through August 28, 2013, Satoshi Dice-related transactions accounted for 52.3% of all bitcoin transactions. See [Re: Satoshi Dice -- Statistical Analysis](#) from Bitcoin Talk and [A Fistful of Bitcoins: Characterizing Payments Among Men with No Names](#) by Meiklejohn *et al.*

²²¹ [Google to Increase Finance in Finland Data Center](#) from *WiredRE*

²²² [Sea-Cooled Data Center Heats Homes in Helsinki](#) from *Data Center Knowledge* and [Helsinki data centre to heat homes](#) from *The Guardian*

²²³ [CoinSummit Day Two: Mining Superpowers and the 51% Challenge](#) from *CoinDesk*

²²⁴ [Before you buy that new miner ...](#) from reddit

²²⁵ Thanks to Jonathan Levin for helping crystalize the distinction between the two.

²²⁶ Personal correspondence, see [Comment of the day: Mining Rewards](#) by Tim Swanson

²²⁷ [An Order-of-Magnitude Estimate of the Relative Sustainability of the Bitcoin Network](#) by Hass McCook

²²⁸ Personal correspondence, July 11, 2014

²²⁹ [What is the Carbon Footprint of a Bitcoin?](#) from *CoinDesk* and [SolarCoin](#)

²³⁰ [Decentralised Currencies Are Probably Impossible](#) by Ben Laurie

²³¹ [Tezos: A Self-Amending Crypto-Ledger Position Paper](#) by L.M. Goodman

²³² What is happening in Europe with solar power may be the inverse of what has been happening with hashrate. See: [How to lose half a trillion euros](#) from *The Economist*

²³³ [China Tightens Grip on Rare Minerals](#) from The New York Times

²³⁴ [Molycorp Announces Start-Up of Heavy Rare Earth Concentrate Operations at Mountain Pass, Calif.](#) from *Business Wire*

²³⁵ See [World Payments Report 2013](#) from CapGemini and related [comment](#) from “usthing.” Note: ‘usthing’ calculation assumes that miners are not compensated by seigniorage, but only by fees which is discussed later in Chapter 3.

²³⁶ [Bitcoin: Questions, Answers, and Analysis of Legal Issues](#) from Congressional Research Service

²³⁷ Ibid

²³⁸ [Why I want Bitcoin to die in a fire](#) by Charles Stross.

²³⁹ For an explanation see [Economic profit vs accounting profit](#) from Khan Academy

²⁴⁰ 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 arbitrated 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.

²⁴¹ [Cost Per Transaction](#) from Blockchain.info

²⁴² An economic profit takes into consideration the opportunity costs of a venture and not just the profit/loss statement calculated by accounting profit. See [Economic profit vs accounting profit](#)

²⁴³ [Different proof-of-work mechanisms and several altcoins that have been hit with a 51% attack](#) by Tim Swanson

²⁴⁴ See [Peter Todd Joins Viacoin Development Team as Chief Scientist](#) from *CoinDesk*, [Tree-chains](#), [Permacoin \(video\)](#), [Proof-of-Activity](#) from Bentov et. al.

²⁴⁵ Proof-of-Idle ([video](#))

²⁴⁶ One reviewer hypothesized that in the future, if one of the exchanges such as Coinbase, Circle or BitPay establishes a *de facto* monopoly via vertical integration and BitLicenses, they could effectively “control” prices much like De Beers “controls” diamonds.

²⁴⁷ [Floating Fees for 0.10](#) by Gavin Andresen

²⁴⁸ [Can Bitcoin Be Stable Long Term?](#) from *Bloomberg*

²⁴⁹ Peter Todd’s [tweet](#)

²⁵⁰ [BitPay's New Plan: Free, Unlimited, Forever.](#) by Tony Gallippi

²⁵¹ [Think Fees On Normal ATMs Are Expensive? Check Out What It Costs To Use A Bitcoin ATM](#) from *Business Insider*

²⁵² [Amazon: How and why did Amazon get into the cloud computing business?](#) by Werner Vogels

²⁵³ [Amazon’s cloud price war with Google is starting to hurt](#) from *Quartz*

²⁵⁴ Thanks to Dan O’Prey for pointing this out to me. See [Amazon Glacier Pricing](#)

²⁵⁵ [Amazon S3 SLA](#)

²⁵⁶ [Bitcoin: Cryptographic Texture](#) by Tomáš Rosa

²⁵⁷ As a friend aptly stated: centralized systems have incredible efficiency but require extraordinary cooperation among stake holders to deploy. Decentralization is opposite end of the continuum where efficiency is traded for ad-hoc coordination between players and boot-strapping. The question for this era is not what is the most decentralized solution possible but solutions are decentralized enough to self-catalyze into solving real problems at scale.

²⁵⁸ [Creating a decentralised payment network: A study of Bitcoin](#) by Jonathan Levin

²⁵⁹ [How a floating blocksize limit inevitably leads towards centralization](#) from *Bitcoin Talk*

²⁶⁰ Personal correspondence, June 30, 2014

²⁶¹ [Re: rpietila Altcoin Observer](#) by Ray Dillinger

²⁶² [Target credit card hack: What you need to know](#) from *CNN/Money*

²⁶³ [Anonymous Byzantine Consensus from Moderately-Hard Puzzles: A Model for Bitcoin](#) by Andrew Miller and Joseph LaViola

²⁶⁴ [Near Zero Bitcoin Transaction Fees Cannot Last Forever](#) by Kerem Kaskaloglu

²⁶⁵ [Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake](#) by Bentov et. al.

²⁶⁶ [China gives green light for three private banks](#) from *Reuters* and [Weibo's mobile wallet will soon allow friends to send money to each other](#) from *Tech In Asia*

²⁶⁷ [Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms](#) by David Evans

²⁶⁸ [Gavin Andresen: Rising Transaction Fees Could Price Poor Out of Bitcoin](#) from *CoinDesk*

²⁶⁹ [VisaNet fact sheet](#) and [Why the payment card system works the way it does – and why Bitcoin isn't going to replace it any time soon](#) by Richard Brown

²⁷⁰ [Tezos: A Self-Amending Crypto-Ledger Position Paper](#) by L.M. Goodman

²⁷¹ While companies like Mastercard and Visa have several centralized nodes, the network is somewhat decentralized as banks send transactions in from their merchants and Mastercard routes them to the member bank, then ships the responses back. This means that Mastercard has incentive to cut costs and manage quality.

²⁷² [Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake](#) by Bentov, *et. al.*

²⁷³ [Why bitcoin won't disrupt digital transactions](#) by Felix Simon

²⁷⁴ A fun thought experiment involving neutrino detector comes from Peter Todd, see [The end of bitcoin is nigh! \(Again\)](#) and [Neutrino communication arrangement](#) patent

²⁷⁵ See [Creating a decentralised payment network: A study of Bitcoin](#) by Jonathan Levin

²⁷⁶ Transactional volume is an unnecessary illustration in this examination. It was used solely to illustrate how the cost of maintaining the network is relatively high despite relatively little transactional action. The bulk of the security is simply for the store of value function. The transactional volume could fall, yet the demand for tokens could rise. If the token value rose, the cost for securing those tokens rises proportionally with it irrespective of transactional volume. Nothing is “left over” from the burning process. Or in other words, the value of a token is function of current or eventual economic demand. Yet, the network hashrate burns the other side of that -- the value of the token equals the cost (of some kind of burn) on the other side to secure it.

²⁷⁷ [Why the payment card system works the way it does – and why Bitcoin isn't going to replace it any time soon](#) by Richard Brown, [Here's How Visa and MasterCard Actually Make Money](#) from *The Motley Fool* and [Paying With Plastic](#) by David Evans and Richard Schmalensee

²⁷⁸ Personal correspondence, May 9, 2014. See also, [Quantifying the Value of Bitcoin](#) by Cal Abel

²⁷⁹ According to David Evans, “With unpredictable, or suboptimal, prices there would be less incentive to make sunk cost investments in forming firms and buying computer capacity. In that case we would expect processing to be conducted by underemployed laborers.”

²⁸⁰ Personal correspondence, May 9, 2014. For Babbitt's calculations see his [spreadsheet](#) on Bitcoin Mining

²⁸¹ Personal correspondence, May 9, 2014. This is based on a baseline electricity cost of 10 cents per kilowatt hour (kWh) which works out to 16,200,000 kilowatts per day. The Hoover Dam produces 49,920,000 kilowatts per day, so roughly 1/4 the output of the Hoover Dam. In practice, according to him it is likely double this amount as many people are mining at a loss or stealing electricity (or ignoring the electrical component entirely).

²⁸² Personal correspondence, May 7, 2014.

²⁸³ Implementing sidechains and merged mining for example. See [Episode #99](#) from *Let's Talk Bitcoin*

²⁸⁴ Mike Hearn has proposed using Tor as an authentication mechanism for the network. Miners currently do not know if they are connected to the “right” Bitcoin network. Their connection could be spoofed by a Sybil attack and thus Hearn's proposal could mitigate some of those risks. See [Mike Hearn on Coming Bitcoin Protocol Updates](#) from *Money & Tech* and [4 New Bitcoin Features Revealed by Core Developer Mike Hearn](#) from *Cryptocoins News*

²⁸⁵ Depending on the time of year and quantity, rates in Saudi Arabia can run from \$0.03 to as low as \$0.01 (wholesale commercial) – however the hot summers make the location less ideal for mining due to the increasingly important cooling requirements. One Chinese reviewer mentioned that in 2012 a team in China conducted a cost/benefit analysis of building a mining pool in Mongolia and came to the conclusion that within 5 years it could likely become a prime location due to its cooler climate and relatively cheap access to energy resources.

²⁸⁶ Thanks to Robert Sams for this keen insight; spending kWh, a scarce resource, makes a Sybil attack (among others) costly.

²⁸⁷ Personal correspondence, May 7, 2014.

²⁸⁸ Ibid

²⁸⁹ When block rewards halve, this could create network performance issues. If half the labor force leaves, then the network may have less security that can only be incentivized through transaction fees. Nicolas Houy has modeled how the fee requirements would necessarily need to increase for the network to maintain the same level that existed prior to the halving, [The Bitcoin mining game](#)

²⁹⁰ [Pantera Launches BitIndex to Track Bitcoin](#) from *CoinDesk*

²⁹¹ In their terms: “It is underweighted because of the arbitrary nature of some bitcoin flows.”

²⁹² [Naked Statistics: Stripping the Dread from the Data](#) by Charles Wheelan, p. 53

²⁹³ The FIFA World Cup was ranked in the top 10 throughout the summer of 2014 but this in itself does not necessarily mean it will lead to additional long-term football adoption in Brazil. See [Popular pages](#)

²⁹⁴ If you can imagine Leonardo da Vinci dreaming up the concept of a botnet with nothing to work with but actual humans, you essentially have Mechanical Turk.

²⁹⁵ [Belkin in "astroturfing" furore](#) from *bit-tech*

²⁹⁶ [Want fans? Hire a social media 'click farm'](#) from *USA Today*

²⁹⁷ [Naked Statistics: Stripping the Dread from the Data](#) by Charles Wheelan, p. 74-75

²⁹⁸ [Private China Meeting Unites Bitcoin Mining Industry Leaders](#) from *CoinDesk* and [GHash Commits to 40% Hashrate Cap at Bitcoin Mining Summit](#) from *CoinDesk*

²⁹⁹ [Some \(sad\) numbers on how Linux desktop adoption is going](#) by Adam Williamson and [NetMarketshare](#)

³⁰⁰ [My Wallet Number Of Users](#), [My Wallet Number of Transactions per day](#) and [My Wallet Transaction Volume](#). See also [My Wallet transaction volume](#) on Bitcoinpulse

³⁰¹ [Blockchain Releases New Android Wallet App To Put Bitcoin Into Everyone's Hands](#) from *TechCrunch*

³⁰² [Bitcoin's failed Coup of Wall Street](#) by Brett King

³⁰³ [Number of Transactions Per Day](#)

³⁰⁴ [Bitcoin Days Destroyed](#)

³⁰⁵ [Leverage point](#)

³⁰⁶ [180,000 BTC from Mt.Gox-associated accounts on the move ... but by whom?](#) from BitcoinX

³⁰⁷ [Total Transaction Fees](#)

³⁰⁸ [Cost Per Transaction](#)

³⁰⁹ [Total Volume Output](#) see also the [cumulative TVO](#) on Bitcoinpulse

³¹⁰ [The Space Shuttle Decision](#) from NASA

³¹¹ See [Subscriptions by day](#) from reddit

³¹² [Coinbase charts](#)

³¹³ See Brian Armstrong's [tweet](#)

³¹⁴ [CheapAir.com Tops \\$1.5 Million in Bitcoin Sales, Offers Free Trip to London to a Lucky Member of the Bitcoin Community](#) from Coinbase

³¹⁵ [Bitnodes](#) 60 day window

³¹⁶ Future researchers could attempt to do a time lapse map of bitcoin nodes on a Mercator projection, similar to what Hans Rosling does at [Gapminder](#). It could also be used on other chains such as Litecoin and Dogecoin.

³¹⁷ [Can You Name a Successful Cleantech Company?](#) from *Green Tech Media* and [13 biggest moments in cleantech in 2013](#) from *GigaOm*

³¹⁸ The actual full list of variables is unavailable at the time of this writing, the link on his document does not resolve to a domain (it cannot be clicked).

³¹⁹ In terms of cell phone penetration and internet access in developing countries: “Internet access in the developing world was 20.5% in 2011, with mobile internet services surging; 29% of Arab states population is estimated to use the internet, although the spread is wide, correlating with per capita income. Cell phone subscriptions worldwide hit 6 billion in 2011, with 600 million new subscriptions that year, mostly in the developing world; as of 2011, there were 778 developing world cell phone subscriptions per thousand people.” See [Security in a Goldfish Bowl](#) by Brian Hanley

³²⁰ While the bulk of this book is comprised of research conducted this past spring, the editing and updating of all portions did not begin until mid-July 2014. \$634.48 was the high and \$564.37 was the low market price during the month of July, see [Bitcoin Price Index](#) from *CoinDesk*

³²¹ [Argentine debt restructuring](#) and [Argentine Debt Feud Finds Much Fault, Few Fixes](#) from *The Wall Street Journal*

³²² According to research from Kay Hamacher and Stefan Katzenbeisser, bitcoins are treated as a type of luxury good (held but not spent). See [Bitcoin - An Analysis \[28C3\]](#)

³²³ [Bitcoin Series 24: The Mega-Master Blockchain List](#) from Ledra Capital

³²⁴ [Chinese Banks don't know how to act appropriately, because Bitcoin is too tiny](#) by Weiwu Zhang

³²⁵ As of May 6, 2014, according to [Blockchain.info](#), miners received 0.31% of their revenue from transactions, the remaining balance came in the form of block rewards (seigniorage).

³²⁶ Its official name is the [Golden Shield Project](#)

³²⁷ See [Determining Electrical Cost of Bitcoin Mining](#) by Ruben Alexander and [The Average Price of Electricity, Country by Country](#) from The Energy Collective

³²⁸ Ignoring cooling requirements and management overhead another infrastructure issue is that this build-out needs approximately a \$100,000 transformer for every 1 megawatt. See also [Bitcoin Miner Taps Dad's Power Plant in Virtual-Money Hunt: Tech](#) from *Bloomberg* and [The Other Bitcoin Power Struggle](#) from *Businessweek*

³²⁹ More than two-thirds of China's energy needs are met through coal-powered power plants. The World Coal Association [estimates](#) that 79% of China's electrical generation capacity comes from coal.

³³⁰ [The ZeroAccess Botnet – Mining and Fraud for Massive Financial Gain](#) by James Wyke and [Botcoin: Monetizing Stolen Cycles](#) by Huang *et. al.* Another paper from the same team discusses the differences between "light" and "dark" mining pools, [Poster: Botcoin – Bitcoin-Mining by Botnets](#)

³³¹ SMT stands for [surface-mount technology](#).

³³² F2Pool, also known as Discus Fish, operates one of the largest known pools in China and the world

³³³ KNC attracted unwanted attention in 2014 when following the release of pictures of its mining facility, it was discovered that customer investors ("investormers") learned how KNC was operating at their expense: KNC received funds from customers, built the systems and then used the machines first for an undisclosed amount of time, generating bitcoins and increasing the difficulty rate at the expense of the customer. This would be akin to the [primary dealer](#) in open-market operations which receive US Treasury funds first before everyone else. See [Bitcoin Miners Building 10 Megawatt Data Center in Sweden](#) from *Data Center Knowledge*

³³⁴ [A Non-Outsourceable Puzzle to Prevent Hosted Mining](#) by Andrew Miller and [CoinLab's Alydian files for bankruptcy and reveals debt of over \\$3.6m](#) from *CoinDesk*

³³⁵ [Embattled CEO of Bitcoin miner firm: "We are as poor as church mice"](#) from *ArsTechnica* and [Bitcoin Mining Manufacturer HashFast Enters Chapter 11 Bankruptcy](#) from *CoinDesk*

³³⁶ Those gains in magnitude are no longer occurring. Jeff Garzik was one of the first users to receive the first batch of Avalon ASICs in January 2013. He recouped the cost of the order in less than a month. [Once upon a time in China, a package shipped](#) by Jeff Garzik, [The First Bitcoin ASICs are Hashing Away!](#) from *The Bitcoin Trader*, [AVALON ASIC has delivered first RIG \(68GH/s Confirmed\) 2nd out proof](#) from Bitcoin Talk and [Engineering the Bitcoin Gold Rush: An Interview with Yifu Guo, Creator of the First Purpose-Built Miner](#) from *Motherboard*

³³⁷ [CoinSummit Day Two: Mining Superpowers and the 51% Challenge](#) from *CoinDesk*

³³⁸ [Private China Meeting Unites Bitcoin Mining Industry Leaders](#) from *CoinDesk*

³³⁹ [China-Europe railway relaunches](#) from *China Daily*

³⁴⁰ [Kapronasia](#)

³⁴¹ [Writing China: 'Chomping at the Bitcoin,' Zennon Kapron](#) from *The Wall Street Journal*

³⁴² [How China's official bank card is used to smuggle money](#) from *Reuters* and [What Drives the Chinese Art Market? The Case of Elegant Bribery](#) by Jia Guo

³⁴³ [CoinSummit London 2014 - Bitcoin in China](#) from *Coinsummit*

³⁴⁴ [YesBTC](#) and [Bitcoin Banned by Alibaba's Taobao After China Tightens Rules](#) from *Bloomberg*

³⁴⁵ Here is the notice in [Chinese](#)

³⁴⁶ [Chinese Bitcoin Exchange FxBTC to Close Citing Central Bank Pressure](#) from *CoinDesk*

³⁴⁷ [F*CK CHINA! I'm holding!](#) on reddit and [China Banning BTC. Any thoughts for the soul especially the mind?](#) from Bitcoin Talk

³⁴⁸ [China Restricts Banks' Use of Bitcoin](#) from *The New York Times*

³⁴⁹ One story I was told by a close source in China is that during the winter of 2013-14, some bitcoin holders in China would hack into the Weibo accounts (similar to Twitter) of journalists and post fake government notices of upcoming regulations and bans. This would shock the market. The hackers would sell their coins before the hack and then after the Weibo account was restored and panic subsided, these same hackers would buy bitcoins at artificially lower rates.

³⁵⁰ [OKCoin's New Bitcoin and Litecoin Fees Cause a Stir on Social Media](#) from *CoinDesk*

³⁵¹ Tim Weithers, [Foreign Exchange – A practical guide to the Fx Markets](#), 2006, John Wiley and Sons, Hoboken, NJ. ISBN-13: 978-0-471-73203-7 pp 40.

³⁵² [Cryptocurrency Cat-and-Mouse games in China](#) by Tim Swanson

³⁵³ [Are the rumors true about China banning cryptocurrencies?](#) by Tim Swanson

354 This claim originated in the State of the Bitcoin 2014 report, see [tweet](#). See also, [The nitty gritty of money transfer operators \(MTOs\)](#) from the Federal Reserve Bank of Atlanta.

355 [Remittance Market: Ready and Waiting for its 'Skype' Moment](#) by Cognizant

356 [Why Bitcoin Faces an Uphill Battle in the Remittance Market](#) from *CoinDesk*

357 [ZipZap Raises \\$1.1 Million to Grow Global Bitcoin Payments Network](#) from *CoinDesk*

358 [Think Fees On Normal ATMs Are Expensive? Check Out What It Costs To Use A Bitcoin ATM](#) from *Business Insider*

359 Bitcoin ATMs are likely underutilized globally, many are probably unprofitable too, hence the lack of public announcement by ATM operators with large figures and margins.

360 [If Beijing is your landlord, what happens when the lease is up?](#) by *China Economic Review*

361 [China's nail houses: the homeowners who refuse to make way – in pictures](#) from *The Guardian*

362 [Fangdi](#)

363 Nick Szabo, the intellectual progenitor to these two concepts, has written extensively of each and I previously covered these in depth in [Great Chain of Numbers](#). See also [Unenumerated](#).

364 [How One Law Firm is Helping Bitcoin Startups Find Success](#) from *CoinDesk*

365 [YBEX](#)

366 [China's lust for scarce resources](#) by Weiwu Zhang

367 [As speculative fever rages, China bursts bean bubble](#) from *Reuters*

368 [Dang, The Wine Bubble Implodes \(It's China's Fault\)](#) from *Testosterone Pit*

369 Part of the contributing reasons for the “pop” is that there was a concerted government crackdown on “extravagance” which included wine as gifts or at parties. See [Why China's wine exchange is crashing: 110-proof grain alcohol all tastes much the same](#) from *Quartz*

370 [China bottle tech checks smash fake wine market](#) from *The West Australian*, [Mainland China Now #5 Export Market For US Wines, HK #3](#) from *Jing Daily* and [Wine Auctions Drop 19%, Chinese Demand Cools for Bordeaux](#) from *Bloomberg*

371 [China On Track To Be World's Biggest Cognac Consumer](#) from *Jing Daily* and [China Has Become A Very Important, Huge Market For Every Cognac Company](#) from *Jing Daily*

372 [Dang, The Wine Bubble Implodes \(It's China's Fault\)](#) from *Testosterone Pit*

373 [China bottle tech checks smash fake wine market](#) from *The West Australian*

374 [Bitcoin's Uncertain Future in China](#) by Lauren Gloudeman

375 [Bitcoin Mining Pool Ghash.io Is Unapologetic Over Risk Of Theoretical 51% Attack](#) from *Cryptocoins News*

376 Coinometrics used a different way to calculate the Ghash.IO hashrate, see [tweet](#)

377 [Coinometrics Briefing #1 - The 50% Club](#) from Coinometrics

378 [Litecoin Miners Urged to Leave Coinotron Pool Over 51% Threat](#) from *CoinDesk*

379 [51% Of The Network?](#) by Dave Hudson

380 [Why I just sold 50% of my bitcoins: GHash.IO](#) by Peter Todd

381 [Bitcoin is all about truth, part 2](#) from *IamSatoshi Networks*

382 [GHash Commits to 40% Hashrate Cap at Bitcoin Mining Summit](#) from *CoinDesk*

383 [What is a Finney attack?](#) from StackExchange

384 Consequently, the economics of cloud hashing may be currently skewed towards cleaning stolen coins, hence the pay-for-faucet. See [Interview with core developer, Peter Todd](#)

385 We also have to trust that GHash.io does not collude with 1 or 2 other pools in double-spending, artificially raising transaction fees, and so forth.

386 A sobering but realistic assessment of why farms join pools: [I own a large mining operation. I'll explain why I mine at ghash.io](#) by miner8765

387 [Hash Rate Headaches](#) by Dave Hudson

388 [The Gambler's Guide To Bitcoin Mining](#) by Dave Hudson

389 [How to Win the Lottery: Couple Profited From Quirk in Massachusetts Cash WinFall Game](#) from *ABC News*

390 Personal correspondence, June 13, 2014

391 [Bitcoin Stats Data Propagation](#)

392 [Creating a decentralised payment network: A study of Bitcoin](#) by Jonathan Levin

393 [Currency Stats](#) from Blockchain.info

394 Some vocal members on social media lashed out against GHash.io, one such post was: [To the "greedy" Ghash miners: Price is nosediving because of the pool majority we saw. WAS IT WORTH IT?](#) by Aviathor

395 [Bitcoin Pandemonium: The Ongoing Economic, Public, and Legal Debate over the Nature and Impact of Bitcoin](#) by Nicolas Wenker

396 [Re: Stupid newbie question about the nonce](#) by Meni Rosenfeld

397 See [How a floating blocksize limit inevitably leads towards centralization](#), [Re: \[Bitcoin-development\] Tree-chains preliminary summary](#) and [Let's Talk Bitcoin Episode 104](#)

398 [Two Phase Proof of Work \(2P-PoW\)](#)

399 [Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake](#)

400 See [Andrew Miller](#) and [Permacoin](#)

401 [Bitcoin Cooperative Proof-of-Stake](#)

402 [Delegated Proof of Stake](#)

403 [Blockpad: Improved Proof-of-work function with decentralization incentives](#)

404 See [On mining](#)

405 [ASICs and Decentralization FAQ](#) by Andrew Poelstra

406 [Bitcoin SF Devs Seminar: An Optimal Bitcoin Mining Strategy - Proof of Idle](#) and ([paper](#))

407 Regarding NXT see [Re: Bounty for successful nothing at stake attack?](#) by Vitalik Buterin

408 [Security](#) from XKCD

409 [Getblocktemplate BIP 23](#)

410 See [BitUndo](#) and also [this thread](#) on the Bitcoin developer mailing list.

411 [Mining Decentralisation: The Low Hanging Fruit](#) by Mike Hearn

412 ["Hash Rate Headaches"](#)

413 [Jeremy Allaire: Bitcoin Developers Need to 'Step Up'](#) from *CoinDesk*

414 Personal correspondence, July 6, 2014. See also his presentation ([slides](#)), "Crypto-Economic Design: A Proposed Agent-Based Modeling Effort"

415 [Certimix](#)

416 [LIMIO protocol](#)

417 [Re: Bitcoin P2P e-cash paper](#) by Satoshi Nakamoto

418 From [Chapter 7](#) in *Great Chain of Numbers*

419 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

420 [This Box Can Hold an Entire Netflix](#) from *Gizmodo*

421 [Uber Woos Drivers With \\$1,000 Bonuses in Tussle With Lyft](#) from *Bloomberg*

422 [Are Uber's latest price cuts sustainable?](#) from *Financial Times*

423 [Craigslis v. 3Taps](#)

424 For more on BitLicenses see [the overview](#) from law firm Katten Muchin Rosenman and the [press release](#) from the New York Department of Financial Services

425 [Corporate Social Responsibility 2013 Report](#) from Bank of America and [BitMinter](#)

426 [Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms](#) by David Evans

427 [Platform Monopolies](#) by Fred Wilson

428 [Intel puts new Arizona chip factory on back burner](#) from *c/net*

429 Another technology that became obsolete despite the large scale deployment and use of protocol was [X.25](#), which was replaced by less cumbersome protocols.

430 [PandoMonthly: Fireside Chat With Peter Thiel](#)

431 [New York Reveals BitLicense Framework for Bitcoin Businesses](#) from *CoinDesk*

432 This also creates legal certainty, as Gil Luria from WedBush explained, "It will make it possible for Bitcoin companies to function in a regulated way which most of them have been seeking out. It should help create the infrastructure to support the growth of the technology as new robust, liquid, US-based exchanges emerge." [New York Just Released Its Bitcoin License, And They're Going To Change The Face Of Digital Currencies In The US](#) from *Business Insider*

⁴³³ New York State Department of Financial Services [proposal](#): "Virtual Currency Business Activity" is defined as: (n) Virtual Currency Business Activity means the conduct of any one of the following types of activities involving New York or a New York Resident: (5) controlling, administering, or issuing a Virtual Currency."

⁴³⁴ If Bitcoin is the equivalent of an underdeveloped country perhaps its inelastic monetary policy has kept it from even reaching a Lewis Turning Point let alone a "middle income trap." See [China approaching the turning point, How to Avoid Middle Income Traps?](#) from The World Bank and [Middle-income Trap Holds Back Asia's Potential New Tiger Economies: 12 Things to Know](#) from Asian Development Bank

⁴³⁵ [Consumers Pay More When They Pay With Bitcoin](#) by Ben Edelman and [The "pain point" of payments in the developed world](#) by Tim Swanson

⁴³⁶ [New Data on Twitter's Users and Engagement](#) from RJMetrics

⁴³⁷ [Throw Your Life a Curve](#) from *Harvard Business Review*

⁴³⁸ [Google+ Reaches 50 Million User Mark in About 88 Days](#) by Paul Allen

⁴³⁹ [Animal Spirits with Chinese Characteristics](#) by Mark DeWeaver

⁴⁴⁰ [Tree Chains with Peter Todd](#) from *Let's Talk Bitcoin*

⁴⁴¹ [Introducing Factum Money](#) by Max Kaye and [DAOs Are Not Scary, Part 1: Self-Enforcing Contracts And Factum Law](#) by Vitalik Buterin

⁴⁴² [Bitcoin: a Money-like Informational Commodity](#) by Jan A. Bergstra and Peter Weijland

⁴⁴³ [How we got from 1 to 162 million websites on the internet](#) from Pingdom

⁴⁴⁴ See [BitLegal](#) for summaries on many jurisdictions.

⁴⁴⁵ [Achieving critical mass in social networks](#) by Chris Geddes. Thanks to Chris Turlica for this reference.

⁴⁴⁶ [Roger Ver, Memorydealers \[interview\] - The European Bitcoin Convention - 2013 Amsterdam](#)

⁴⁴⁷ If this is a sales cycle, is there a way for Jack Lemmon to "always be closing" as seen in *Glengarry Glen Ross*?

⁴⁴⁸ [Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms](#) by David S. Evans

⁴⁴⁹ [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*

⁴⁵⁰ [Insight: African tech startups aim to power growing economies](#) from *Reuters*

⁴⁵¹ [M-Pesa helps world's poorest go to the bank using mobile phones](#) from *CS Monitor*

⁴⁵² [The Future of Payments: 2014](#) from *Business Insider*

⁴⁵³ Subpoenas and testifying in front of various government committees raised the public's awareness of Bitcoin, yet conversion rates are still quite low. In contrast, these four companies have not been subpoenaed or received the same amount of publicity, but have expanded both market share and user base significantly. This may due to the "hype cycle," see [Is Bitcoin Over the Hill?](#) by Danny Bradbury

⁴⁵⁴ As of block 310,000, see [BitcoinRichList](#)

⁴⁵⁵ [Jonathan Levin of Coinometrics @ CoinSummit](#) from *Money & Tech*

⁴⁵⁶ One reviewer noted that "the claim that 98.08% of all addresses contain less than one Bitcoin is an extreme understatement. In fact it is impossible for more than 21 million distinct addresses to correspond to UTXOs containing 1 bitcoin, but there are 10^{48} addresses. So it will always be the case that at least $(100 - 10^{-38})\%$ of addresses contain less than one bitcoin."

⁴⁵⁷ [Some altcoin memes are more equal than others](#) by Izabella Kaminska

⁴⁵⁸ [927 People Own Half Of All Bitcoins](#) from *Business Insider* and [Forget the 1 percent. In the Bitcoin world, half the wealth belongs to the 0.1 percent.](#) from *The Washington Post*

⁴⁵⁹ [Rise of the Zombie Bitcoins](#) by John Ratcliff

⁴⁶⁰ Many thanks to Andrew Poelstra for clarifying this for me

⁴⁶¹ [Mike Hearn, Bitcoin Core Developer NBC2014](#) from Bitcoin Congress

⁴⁶² [Android Bitcoin wallet](#)

⁴⁶³ Personal correspondence, July 11, 2014

⁴⁶⁴ [Google Trends](#)

⁴⁶⁵ [Structure and Anonymity of the Bitcoin Transaction Graph](#) by Ober *et. al.*

⁴⁶⁶ [Thread of the day: List of all the known dead altcoins](#) by Tim Swanson

⁴⁶⁷ [Some altcoin memes are more equal than others](#) by Izabella Kaminska

⁴⁶⁸ [Bitcoin 101 - Why Bitcoin's Growth is Normal & The S-Curves You Could Never See](#) by James D'Angelo

⁴⁶⁹ [Re: The current Bitcoin economic model doesn't work](#) from Bitcoin Talk

⁴⁷⁰ [Hoarding, compulsive buying and reasons for saving](#) by Frost *et. al.*

⁴⁷¹ [ING: Future Bitcoin Protocol Should Include Central Bank Functions](#) from *CoinDesk*

⁴⁷² [Bitcoin's Deflationary Weirdness](#) by Dan Kervick

⁴⁷³ [Bitcoin: Questions, Answers, and Analysis of Legal Issues](#) from Congressional Research Service

⁴⁷⁴ How to determine an interest rate within the Bitcoin economy? Nicolas Wesner attempted to build a framework in his paper, "[The Time Value of a Digital Currency: Bitcoin Interest Rates Dynamics](#)." As a Swiss friend explained in a meeting recently, "Bob can fill in the covered [interest rate parity](#) formula and solve it. The forward exchange rate can be taken from a futures contracts traded on ICBIT. However, the formulas in Wesner's paper are based on some assumptions which do not necessarily hold. Bob could fill in the numbers for the covered interest rate parity and test it with a trading pair like EURUSD first. Sometimes the end result does not match up with reality, so in practice traders use it as an indicator. They assume the formula calculates the balanced value and that markets in the long run will drift towards the equilibrium. But the long run never comes and thus the equilibrium is always changing."

⁴⁷⁵ [The 'Bitcoin Consumer Price Index' Shows Massive Deflation](#) by Peter Coy

⁴⁷⁶ This line of reasoning credited to [Why Bitcoin Will Never Be a Currency—in 2 Charts](#) by Matthew O'Brein

⁴⁷⁷ The original [Apple II](#) was released on June 10, 1977; calculation using the [BLS inflation calculator](#)

⁴⁷⁸ One reviewer noted that, "you can't really have deflation in the case of a currency that's not a medium of exchange because if it wasn't used in transactions there wouldn't be any prices quoted in that currency and it therefore wouldn't be possible to speak of those prices falling."

⁴⁷⁹ Aswath Damodaran also discusses a market-based rate of return in [Bitcoin Q & A: Bubble or Breakthrough? Both! Cult or Currency? Both!](#)

⁴⁸⁰ [The Marginal Cost of Cryptocurrency](#) by Robert Sams and [Hayek Money](#) by Ferdinando Ametrano

⁴⁸¹ [Bitcoin a Fool's Gold Standard](#) by Edward Hadas

⁴⁸² [Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms](#) by David S. Evans

⁴⁸³ [Why Bitcoin's Volatility is Unique Among Commodities](#) from *CoinDesk* and [Lawsky's Office Starts Taking Applications for the 'BitLicense'](#) from *The Wall Street Journal*

⁴⁸⁴ [The audacity of bitcoin](#) by John Normand

⁴⁸⁵ [Re: Bitcoin P2P e-cash paper](#) by Ray Dillinger

⁴⁸⁶ [Your oldest, most outdated device](#) from *Yahoo!*

⁴⁸⁷ Deflation is usually more of a problem for the borrower rather than the lender. With deflation, the lender gets paid back an amount that is worth more than what he originally lent. Perhaps the problem is that if deflation is extreme, the default rate will be high.

⁴⁸⁸ One reviewer noted that in theory, "A lender should love a deflationary environment, assuming that default rates don't rise with it, and assuming that they keep the loan and its monthly installment payments in bitcoin. This logic holds true, however, when the loan or its payments are converted into fiat, non-deflationary currencies."

⁴⁸⁹ [Bitrated](#) is attempting to do so.

⁴⁹⁰ One reviewer suggested that "some illicit drugs such as cocaine and heroin can see similar distribution gains)."

⁴⁹¹ [The False Premises and Promises of Bitcoin](#) by Brian Hanley

⁴⁹² Personal correspondence, July 12, 2014; see [Inv and Sav Wallets: The Role of Financial Intermediaries in a Digital Currency](#) by Massimo Morini

⁴⁹³ Personal correspondence, July 15, 2014; see [The False Premises and Promises of Bitcoin](#) by Brian Hanley

⁴⁹⁴ The story that is oft repeated is that at some point, bitcoins will become worth so much that the original holders will cash out (assuming they still actually possess their coins, which they may have lost). Yet this has not empirically happened as seen with the 64x run-up last year.

⁴⁹⁵ Personal correspondence, July 31, 2014

⁴⁹⁶ [Rise of the Zombie Bitcoins](#) by John Ratcliff

⁴⁹⁷ [A History of Zombie Events](#) by John Ratcliff

⁴⁹⁸ [Quantitative Analysis of the Full Bitcoin Transaction Graph](#) by Dorit Ron and Adi Shamir

⁴⁹⁹ I would like to thank Chris Turlica for this turn-on-phrase

⁵⁰⁰ [Bitcoin's Deflationary Weirdness](#) by Dan Kervick

⁵⁰¹ [Bitcoin's deflation problem](#) from *The Economist*

⁵⁰² [Hayek Money: the Cryptocurrency Price Stability Solution](#) by Ferdinando Ametrano

⁵⁰³ [The Ascent of Money](#) by Niall Ferguson and the companion [PBS series](#)

⁵⁰⁴ [Shelling Out -- The Origins of Money](#) by Nick Szabo; see also [Rai stones](#)

⁵⁰⁵ [Money Matters: The Tally Stick System](#) from Unusual Historicals

⁵⁰⁶ [Debt: it's back to the future](#) by Gillian Tett

⁵⁰⁷ Leonardo Pisano Bigollo, better known as Fibonacci, created a number sequence called the [Fibonacci numbers](#) which helped transition Europe from Roman numerals to the Hindu-Arabic system.

⁵⁰⁸ In Brian Hanley's words describing a letter of credit: What started out by conning people became the basis of Western civilization, and then all of civilization – because it worked so well. It made huge amounts of money available by a brand new mechanism – the judgment of smart people who were not politicians. This had huge repercussions. Over time it made royal families beholden. It made it possible to get money in the present for a future promise to deliver – if the banker believed you. Banking was, in Silicon Valley-speak, “massively disruptive.” See [Beanie Babies or Bitcoins?](#)

⁵⁰⁹ [Bitcoin and Complexity Theory: Some Methodological Implications](#) by Marc Pilkington

⁵¹⁰ I would like to thank John Komkov for this thought experiment and reference.

⁵¹¹ It may be logistically difficult and very risky (since sending bitcoins are irreversible). See [Of course you can have fractional reserve Bitcoin banks](#) by John Carney

⁵¹² [BitVC](#)

⁵¹³ One reviewer does not think Huobi is heading in that direction. Noting, “What Huobi is doing is not likely to be fractional reserve banking. If they pay interest in bitcoin, and bitcoin goes up, they can't pay it in more bitcoin because that costs them a greater and greater amount of fiat currency. Only if bitcoin goes down predictably, and they convert it to fiat currency, then convert it back does that work. So where does it come from? If they transfer the bitcoins for trading on margin, what are they really doing? Are they just showing it online as numbers in an account and not really transferring it? That's an implementation of *virtual* bitcoin that might work within a single system. If Huobi enforces charges against the margin trading accounts, and those are virtual bitcoins the players are trading with, what are those players really trading? Are they buying bitcoin with bitcoin? Has Huobi implemented forward contracts on bitcoin? There's more to dig into here.”

⁵¹⁴ [Bitcoin Banking Will Be Boring](#) by Matt Levine

⁵¹⁵ I would like to thank Tyler Sorensen for making this droll observation.

⁵¹⁶ [The False Premises and Promises of Bitcoin](#) by Brian Hanley

⁵¹⁷ N. F. Hoggson, *Banking through the ages*. New York Dodd, Mead & Company, 1926

⁵¹⁸ BIS, "Basel III: A Global Regulatory Framework for More Resilient Banks and Banking Systems," ed. Basel, Switzerland: Bank for International Settlements, 2010.

⁵¹⁹ T. Tooke, *An Inquiry into the Currency Principle, the Connection of the Currency with Prices, and the Expediency of a Separation of Issue from Banking*. London: Longman, Brown, Green and Longmans, Paternoster - Row, 1844. <http://www.efm.bris.ac.uk/het/tooke/currency.htm>

⁵²⁰ (2012) (Accessed: Aug 15, 2013). Dree12. List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses. Available: <https://bitcointalk.org/index.php?topic=83794.0>

⁵²¹ J. Edwards. (2013, Nov 17) If Bitcoin Is So Secure, Why Have There Been Dozens of Bitcoin Bank Robberies And Millions In Losses? Business Insider. Available: <http://www.businessinsider.com/the-history-of-bitcoin-theft-2013-11>

⁵²² (2013) (Accessed: Nov 15). L. Mathews. \$4.1 million worth of Bitcoins goes missing as Chinese exchange GBL disappears. Available: <http://www.geek.com/news/4-1-million-worth-of-bitcoins-goes-missing-as-chinese-exchange-gbl-disappears-1576967/>

⁵²³ This comment comes from [Ben Coleman](#) on reddit. In an email exchange he explained that, “The invention of secondary markets would not necessarily require a centralized counterparty (though it would certainly help) but it would require the development of intensive contract enforcement. Some Bitcoin adopters will reply that “proof of existence” transactions deal with this risk, which is moderately true, but a secondary market will only occur when you and I both trust in a third party authority figure with the means to force us to pay each other per the terms of the contract.” Another thought provoking thread comes from [TheyCallMeRINO](#)

⁵²⁴ For balance, John Carney argues that [Of course you can have fractional reserve Bitcoin banks](#)

⁵²⁵ [Buyback Bitcoin After Checkout](#) from Coinbase

⁵²⁶ [Coinbase introduces instant buyback!](#) by coelomate

⁵²⁷ [Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms](#) by David Evans

⁵²⁸ [Bitcoin and volatility](#) by Chris Dixon

⁵²⁹ [Bitcoin's failed Coup of Wall Street](#) by Brett King

530 [Bitcoin Volatility – The 4 perspectives](#) by Radoslav Albrecht

531 [Digital Currency Deep Dive: Is Bitcoin Cheaper and More Efficient than Traditional Payments?](#) by David Evans

532 David Evans also discusses Coinbase in [The Great Bitcoin Debate In Six Points](#)

533 [Consumers Pay More When They Pay With Bitcoin](#) by Ben Edelman

534 [The 10 Most Promising Startups Building Stuff With Blockchain Technology](#) by Tim Swanson

535 [Creating a decentralised payment network: A study of Bitcoin](#) by Jonathan Levin

536 [Quantabytes](#)

537 [Is there a cure for China’s ailing healthcare system?](#) from *Prospect*

538 I wrote about this previously in [chapter 19](#) in *Great Wall of Numbers*. See also [Bribery serves as life-support for Chinese hospitals](#) from *Reuters*

539 [Occupational Employment and Wages, May 2013](#) from Bureau of Labor Statistics

540 [Bitcoin Foundation Holds \\$4 Million in Bitcoin, Spends \\$150,000 Each Month](#) from *CoinDesk*. I was also told that wages are paid based on a 30-day moving average of the market value.

541 [Blockr.io trivia](#)

542 The flowchart [How a Bitcoin transaction works](#) explains cryptographic hashes and nonces

543 [F2Pool](#)

544 [Back-of-the-envelope calculations for marginal cost of transactions](#) by Gavin Andresen

545 [These Three Graphs Prove That Bitcoin Is a Speculative Bubble](#) by Jason Kuznicki

546 [Why Bitcoin does not have a market cap](#) by Jonathan Levin

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

548 Robert Sams has also discussed some lower bound and upper bound estimates for the velocity of bitcoins, see [The velocity and dormancy of bitcoin](#)

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

550 [Testimony of Mark T. Williams](#) on April 2, 2014

551 According to Williams, “In 2009, annual volatility was approximately 160 percent. Using price data from 2010 forward from Mt Gox, Bitstamp and BTCe, annual volatility through 2014 was approximately 140 percent.”

552 Notable exceptions can be found in [The Most Profitable Small Businesses](#) from *Forbes*

553 [Investor Fred Wilson: Security and Hoarding Are Holding Back Bitcoin](#) from *CoinDesk*

554 See [Demand and supply statistics](#) from World Gold Council

555 Future value (FV) of a single sum, see [time value of money](#).

556 [The False Premises and Promises of Bitcoin](#) by Brian Hanley

557 Some have argued that it may be a collectible like a stamp, a beanie baby or “My Little Pony” figurine. See [Beanie Babies or Bitcoins?](#) by Brian Hanley

558 [BitBeat: Bitcoin Price – Curiously – Gets No Boost From Dell News](#) from *The Wall Street Journal*

559 [Shortage economy](#)

560 For balance there are some non-ideological proposals surrounding full reserve banking solutions from John Kay and Martin Wolf. See [Narrow Banking](#) by John Kay and [Strip private banks of their power to create money](#) by Martin Wolf

561 See also [Trilemma](#)

562 [The False Premises and Promises of Bitcoin](#) by Brian Hanley, [Hayek Money: The Cryptocurrency Price Stability Solution](#) by Ferdinando Ametrano and [Inv and Sav Wallets: The Role of Financial Intermediaries in a Digital Currency](#) by Massimo Morini

563 [Consumers Pay More When They Pay With Bitcoin](#) by Ben Edelman and [The Great Bitcoin Debate In Six Points](#) by David Evans

564 [Swiss Bank UBS: Banks Could ‘Absorb the Benefits’ of Bitcoin](#) by analyst4933

⁵⁶⁵ Bridgewater attempted to build a service similar to Bitreserve and LOCKS but were likely too early or perhaps this is not a scalable business. See [Mt.Gox fallout: Bridgewater is shutting down](#)

⁵⁶⁶ [SecondMarket \(BIT\)](#), [CampBX](#), [TruCoin](#), [Coinfloor](#), [Atlas ATS](#), [Kraken](#), [Coinsetter](#), [Vaurum](#), [itBit](#), [ICBIT](#), [LedgerX](#)

⁵⁶⁷ [Delta Financial Offers Interest-Bearing Bitcoin Accounts](#) from *CoinDesk* and [OKCoin Targets International Markets with Margin Trading Launch](#) from *CoinDesk*

⁵⁶⁸ [SecondMarket Seeks to Open Bitcoin Fund to Ordinary Investors](#) from *The Wall Street Journal* and [Winklevoss Bitcoin ETF to Trade on NASDAQ Under 'COIN' Symbol](#) from *CoinDesk*

⁵⁶⁹ Below is a list of embryonic solutions of projects being developed in this digital ecosystem (this is not an endorsement, nor do I hold no equity in them): API: Chain, Blockr, HelloBlock, BlockCypher, HiBitcoin; Analytics: Coinalytics, Coinometrics, Blocktrail, Quantabytes, Trade Block; KYC: CoinTrust, Block Score, Coin Comply; Decentralized cloud: Maidsafe, StackMonkey, decloud, Filecoin, Bitcloud, StorJ; Lending and Hedging: BTCJam, Bitreserve, Bitfinex, LOCKS, Bitbond; Peg: Netagio, Ripple Singapore, Digital Tangible Trust, GBI

⁵⁷⁰ [Eris project](#)

⁵⁷¹ [Ecuador Bans Bitcoin in Legislative Vote](#) from *CoinDesk*, [EU Banks Must Shun Bitcoin Until Rules in Place](#), [EBA Says](#) from *Bloomberg* and [One-on-One with Juan Llanos: On State-Run Currencies, NY's BitLicense and Bitcoin in Emerging Markets](#) from *Inside Bitcoin News*

⁵⁷² [Gov. Brown signs bills legalizing Bitcoins use, other legislation](#) from *Los Angeles Times* and the case [SEC v. Shavers and Bitcoin Savings and Trust](#)

⁵⁷³ [Bitcoin - An Analysis \[28C3\]](#) by Kay Hamacher and Stefan Katzenbeisser

⁵⁷⁴ The (-0.4) figure comes from [The Currency Transaction Tax: Rate and Revenue Estimates](#) by Rodney Schmidt

⁵⁷⁵ [Bitcoin and Beyond: The Possibilities and Pitfalls of Virtual Currencies](#) by David Andolfatto

⁵⁷⁶ [Federal Bank VP: Bitcoin Threat Means Banks Must 'Adapt or Die'](#) from *CoinDesk*

⁵⁷⁷ [SatoshiDICE.com - The World's Most Popular Bitcoin Game](#) by Erik Voorhees. On May 4, 2012 Stephen Gornick [calculated](#) that of the 42,152 total transaction on the blockchain, 21,076 transactions were wagers related to Satoshi Dice. This volume doubled within four days, as Gornick [posted](#) an update that 94,706 total transactions on the blockchain, 47,353 were wagers.

⁵⁷⁸ [Re: Satoshi Dice -- Statistical Analysis](#) by dooglus and [A Fistful of Bitcoins](#) by Meiklejohn *et al.*

⁵⁷⁹ Prior to emptying its wallet (the first time), on its then-summer 2012 height, Silk Road's public address (1DkyBEkt5S2GDtv7aQw6rQepAvnsRyHoYM) contained 5% of all mined bitcoins at that point. See [A Fistful of Bitcoins: Characterizing Payments Among Men with No Names](#) by Meiklejohn *et al.*

⁵⁸⁰ [Sealed Complaint 13 MAG 2328: United States of America v. Ross William Ulbricht](#) from the Federal Bureau of Investigation

⁵⁸¹ [Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace](#) by Nicolas Christin; see also [Bitcoin and the PPP Puzzle](#) by Paolo Tasca and Calebe De Roure

⁵⁸² Ross William Ulbricht is the alleged creator and owner of Silk Road, see [Silk Road, Shut Down in Fall, Had Digital Outpost in Pennsylvania](#) from *The New York Times*. Erik Voorhees is the founder of Satoshi Dice, he sold the company a year after its creation and the company is currently under investigation from the SEC. See [Bitcoin company acquisitions begin: Gambling site SatoshiDice sells for \\$11.5m \(126,315 BTC\)](#) from *CoinDesk* and [Gambling Website's Bitcoin-Denominated Stock Draws SEC Inquiry](#) from *Bloomberg*

⁵⁸³ A detailed analysis of transactional volume can be found in [A Fistful of Bitcoins: Characterizing Payments Among Men with No Names](#) by Meiklejohn *et al.* See also, [The Completely Insane Saga of CoinBet.cc](#) by Neil Sardesai

⁵⁸⁴ [Number of transactions per day](#) from Blockchain.info

⁵⁸⁵ In September 2013, Rick Falkvinge made the following analogy: "Money in gambling – at least instant gambling – is not in a lockdown cycle and does not contribute to the minimum size of the money supply. This becomes important as we look at the different economies making up bitcoin today. There are about 11.7 million bitcoin in circulation today. Out of these, a staggering 2 million bitcoin are gambled every year on the SatoshiDice site alone, and another, PrimeDice, 1.5 million. To put these numbers in perspective, if translated to the global economy, it would mean that people bet the entire production of the USA at one single betting site, and the entire production of Europe on another. But as we have seen, these numbers do not contribute to the money supply pool in any meaningful way in a functioning economy." Since its launch in May 2013, approximately 404,000 bitcoins have been wagered in over 748 million bets on PrimeDice. See [Bitcoin's Vast Overvaluation Appears Partially Caused By \(Usually\) Illegal Price-Fixing](#) by Rick Falkvinge

586 [Total-factor productivity](#); the latter have a certain *je ne sais quoi*.

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

588 Incidentally gambling has the nickname as “math tax” because it is a tax on people who are not proficient with statistics (49.5% odds means in the long-run, you will always lose to the house). This is derived from Ambrose Bierce’s quote, “Lottery: A tax on people who are bad at math.”

589 [That Which is Seen, and That Which is Not Seen](#) by Frederic Bastiat

590 [Gambling and speculation](#) by Shaheen Borna and James Lowry

591 Future research can look at risk-forward discounting and discounting due to inability to exchange large amounts of bitcoin without moving the market. There are only so many large holders “whales” that can exit the system.

592 I would like to thank Chris Turlica for this thought experiment.

593 [Flash Boys](#) by Michael Lewis

594 [Inv/Sav Wallets and the Role of Financial Intermediaries in a Digital Currency](#) by Morini Massimo

595 Luke Dashjr is volunteering when he writes code for Bitcoin and is paid by those who contract him.

596 [The False Premises and Promises of Bitcoin](#) by Brian Hanley

597 Bitcoin - An Opportunity for Investors by Pathfinder Capital (forthcoming)

598 [Former Neo & Bee Employees Release Damning Statement](#) from *CoinDesk*

599 Its customer base has been two-thirds female for over a decade, see [press release](#) from December 1, 2003.

[Overstock to Launch New Rewards Scheme for Bitcoin Buyers](#) from *CoinDesk*

600 [Bitcoin Needs Women](#) from *Motherboard*

601 [Overstock CEO Patrick Byrne Reports \\$1.6 Million in Bitcoin Sales](#) from *CoinDesk* and [Overstock Tops \\$1 Million in Sales Made With Bitcoin in 2 Months](#) from *Mashable*

602 [Patrick Byrne reddit AMA](#)

603 [\[170\] Cate Long on Puerto Rico finances & Patrick Byrne on Bitcoin in retail](#) from *Russia Today*

604 [Overstock.com just lost 1/5 of its stock value. Was Bitcoin a last-ditch attempt to save a dying company?](#) from *reddit*

605 [Bitcoin set to overtake PayPal in 2014](#) from *Cryptocoins News*

606 [The Future of Payments: 2014](#) from *Business Insider*; source for image is statista: [PayPal's total payment volume from 1st quarter 2010 to 2nd quarter 2014 \(in billion U.S. dollars\)](#)

607 [Realty Shares](#), [GBI](#), [Digital Tangible Trust](#), [Proof of Existence](#), [OriginStamp](#), [Lighthouse](#), [StackMonkey](#), [decloud](#), [Bitcloud](#), [StorJ](#), [Filecoin](#) and [MaidSafe](#)

608 [Deanonymisation of clients in Bitcoin P2P network](#) by Biryukov *et. al.* See also [Evaluating User Privacy in Bitcoin](#) by Androulaki *et. al.*

609 [Bitcoin Venture Investments](#) from *CoinDesk*

610 [Will Bitcoin Venture Capital Investment Reach \\$300m in 2014?](#) from *CoinDesk*

611 See [Annual B2C e-commerce sales in the United States from 2002 to 2013 \(in billion U.S. dollars\)](#) from Statista and [As world awaits Alibaba IPO, China's ecommerce spending grows to \\$74 billion in Q1](#) from *Tech In Asia*

612 [BitPesa](#), [BitPagos](#), [MaicoIn](#), [Coins.ph](#), [ZipZap](#), [Coincove](#) and [37Coins](#)

613 [Why Bitcoin Faces an Uphill Battle in the Remittance Market](#) from *CoinDesk*

614 A popular story about bitcoin-based remittances in Uganda story turned out to be false. See [Using Bitcoin To Send Money To Your Brother In Uganda Would Be Awesome, If It Actually Worked](#) from *Forbes*

615 Personal correspondence, June 2, 2014; see [Satoshi Legal](#)

616 [Google exec reiterates commitment to mobile payments](#) from *c/net* and [Will Apple Become The American Express of Mobile Payments?](#) from *PYMNTS*

617 [The Future of Payments: 2014](#) from *Business Insider*

618 [West Africa: Facts and Figures](#) from The World Bank

619 [Can Bitcoin Deliver on its Promise to the World's Unbanked?](#) by Jason Tyra

620 [Cash-Strapped MultiBit Developers to Charge Transaction Fee](#) from *CoinDesk*

621 [Once piracy havens, China's Internet video websites turn police](#) from *Reuters*

622 [Bitcoin Series 24: The Mega-Master Blockchain List](#) from Ledra Capital

623 [Startup Cities Institute](#)

624 See [Copay Team Broadcasts First BIP32 P2SH Multisig Transaction from Tucuman, Argentina](#) by Ryan Charles and [BitPay Releases Beta for Open-Source, Multi-Signature Bitcoin Wallet](#) from *CoinDesk*

⁶²⁵ [HelloBlock](#), [Blockr](#), [BlockCypher](#) and [Chain](#)

⁶²⁶ [Facebook's Ben Davenport Leaves for Bitcoin Startup BitGo](#) from *CoinDesk*

⁶²⁷ I would like to thank Richard Brown for this thought experiment.

⁶²⁸ [Plug and Play Tech Center](#), [500 Startups](#), [Boost VC](#), [CrossCoin Ventures](#), [Techstars](#), [YCombinator](#), [Seedcoin](#)

⁶²⁹ [Is Bitcoin Over the Hill?](#) by Danny Bradbury

⁶³⁰ John Wanamaker, was a merchant and one of the first pioneers in advertising and marketing. William Lever is the namesake of the modern brand line.

⁶³¹ Cryptocurrency may not be an accurate term for describing what bitcoins are. See [Bitcoin: a Money-like Informational Commodity](#) by Jan Bergstra and Peter Weijland

⁶³² [A Major Coinbase Milestone: 1 Million Consumer Wallets](#) from Coinbase

⁶³³ Coinbase began 2013 with 13,000 wallets and on February 27, 2014 announced it had reached 1 million. In contrast, Blockchain.info had roughly 13,000 wallets as of August 2013 and reached 1 million in January 2014. Thus 14 months versus 17 months. On April 14, 2014, Blockchain.info reached 1.5 million wallets, which are on-chain, yet it is unclear how many are active or have any bitcoins in them (similar uncertainties surround Coinbase wallets). Furthermore, Blockchain.info announced an implementation of [CoinJoin](#) ([SharedCoin](#)) on November 18, 2013 which coincided with a large increase in wallet creation. Though, it is unclear if wallet creation is instead linked to the increased popularity of Bitcoin in China, the height of which occurred in late November and early December.

⁶³⁴ One reviewer noted that, "Blockchain's wallets are just as centralized as any other. The blockchain is not structured to host wallets."

⁶³⁵ [A history of Bitcoin in one chart](#) by Jonathan Levin

⁶³⁶ [There are 38,399 addresses with a balance of exactly 50 BTCs. Most are dormant since 2009. I estimate 30-40% of all coins are gone.](#) by rutkdn

⁶³⁷ [Satoshi 's Fortune: a more accurate figure](#) by Sergio Lerner; see also [Chain Archaeology - Answers from the early blockchain](#) from Taras

⁶³⁸ [Chart from Bring Out Your Dead Bitcoins that is](#) by John Ratcliff

⁶³⁹ One reason for this is that the large miners cannot necessarily immediately sell coins in bulk without dramatically depressing the price of bitcoin; the market is sometimes too thin for them to sell their positions.

⁶⁴⁰ [Bring Out Your Dead Bitcoins that is](#) by John Ratcliff

⁶⁴¹ See [Blockchain Statistics for July 27, 2014](#) and [Rise of the Zombie Bitcoins](#) by John Ratcliff

⁶⁴² [Bitcoin Value Distribution by Age from January 2009 to May 16, 2014](#) by John Ratcliff ([raw data](#))

⁶⁴³ Personal correspondence, May 14, 2014

⁶⁴⁴ [Bitstamp Audit Proves it was Behind \\$147m Mystery Bitcoin Wallet](#) from *CoinDesk*

⁶⁴⁵ [Satoshi 's Fortune: a more accurate figure](#) by Sergio Lerner

⁶⁴⁶ Personal correspondence, May 16, 2014

⁶⁴⁷ [Show Me the Bitcoins](#) from *Technology Review*

⁶⁴⁸ I was given material in July from a mining farm that claims to have significant quantities of the popular script-based coins. Similarly, several of the large bitcoin mining farms and mining manufacturers have very large quantities of bitcoins because they receive the latest, best hashing equipment first; their profit margins are significantly wider than marginal participants.

⁶⁴⁹ Personal correspondence, May 5, 2014. See [Coinometrics](#)

⁶⁵⁰ Original announcement thread: [New Bitcoin Exchange \(mtgox.com\)](#)

⁶⁵¹ [How ArtForz changed the history of Bitcoin mining](#) by Tim Swanson

⁶⁵² [The ZeroAccess Botnet – Mining and Fraud for Massive Financial Gain](#) by James Wyke and [Microsoft: ZeroAccess botnet has been abandoned](#) from Threatpost

⁶⁵³ [Once upon a time in China, a package shipped](#) by Jeff Garzik, [The First Bitcoin ASICs are Hashing Away!](#) from *The Bitcoin Trader*, [AVALON ASIC has delivered first RIG \(68GH/s Confirmed\) 2nd out proof](#) from Bitcoin Talk and [Engineering the Bitcoin Gold Rush: An Interview with Yifu Guo, Creator of the First Purpose-Built Miner](#) from *Motherboard*

⁶⁵⁴ The economics of gravitating towards specialized hardware and in this case ASICs is described in [Bitcoin and The Age of Bespoke Silicon](#) by Michael Taylor

⁶⁵⁵ One reviewer noted an imperfect similarity between [primary dealers](#) and [open market operations](#) with ASICs manufacturers (assuming they mine too), likening them to the new central bank. "This is because they get the

hardware before others and thus reap the largest benefits. Especially, since the useful production window of a hardware is around 6 months or so, thus every day counts. Similarly, primary bond dealers receive funds first and therefore can spend the funds first.”

⁶⁵⁶ There are multiple competing technical terms to describe bitcoin, see [Bitcoin: a Money-like Informational Commodity](#) by Jan Bergstra and Peter Weijland

⁶⁵⁷ [List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses](#) from Bitcoin Talk. Note: on April 12, 2014 I contacted the creator of the list (dree12 by email) and have verified all but the Allinvain theft. I then contacted Allinvain on April 14, 2014 and the user said “I’m afraid there is nothing new. No coins have been recovered and the thief was not found. I’ve essentially given up.”

⁶⁵⁸ The user dree12 recently updated the previous list but as of this writing has not added the following: 5,800 PicoStocks; 96,000 Sheepmarketplace; 4,474 Silk Road 2; 335 Pony virus; 896 Flexcoin; 1,454 Vircorex; 950 Cryptorush; 1,295 BIPS; 484 Bitcash.cz; 7,500 James Howell’s laptop; 2,130 Proof-of-burn (Counterparty); 41,928 CryptoLocker ransomware.

⁶⁵⁹ A number of reviewers suggested using “rightful” owner instead of “legitimate” for this paper.

⁶⁶⁰ One reviewer provided a thought experiment of stolen coins. What if these coins have actually gone back into circulation and are being used actively in the criminal network and beyond, “this in a [quantity theory of money](#) sense or [Metcalf’s law](#) sense means that the network is more valuable. But it certainly detracts legitimacy that has to be earned in the eyes of people that enjoy well defined property rights or at least some concept of rightful ownership. Indeed play out the thought experiment that Coinbase was looted and those coins are now in the hands of some criminals that walk to the exchange and sell the coins. Even assuming that no one finds out about the heist for many hours, this would damage the network forever.”

⁶⁶¹ One reviewer noted that, “Tomorrow Satoshi Nakamoto could decide to start moving his bitcoins around. He could do that a year from now. Or ten years from now. And, it’s highly likely, that Satoshi probably has control over those keys. He was a thoughtful and careful person when it came to cryptography. I would say it’s quite likely he still controls those keys. What he plans to do with them, is unknown. While it’s interesting to note how many bitcoins may or may not be lost or gone, other than the uncertainty of it, it doesn’t really matter economically. It has been argued that the entire world-wide economy could operate on a single bitcoin, such is the power of mathematics and numbers with a whole lot of decimal places.”

⁶⁶² [Talking Bitcoin With the Winklevosses, Naval Ravikant, and BalajiSrinivasan](#) from *TechCrunch*

⁶⁶³ [\\$4.1m goes missing as Chinese bitcoin trading platform GBL vanishes](#) from *CoinDesk*

⁶⁶⁴ [CryptoDefense, the CryptoLocker Imitator, Makes Over \\$34,000 in One Month](#) from *Symantec*

⁶⁶⁵ In order to reclaim James Howell’s laptop and hard drive from the landfill this would take real world digging and “mining.” See [Missing: hard drive containing Bitcoins worth £4m in Newport landfill site](#) from *The Guardian* and [Digital Gold Rush: The Bitcoin Boom and Its Many Risks](#) from *Der Spiegel*

⁶⁶⁶ [Nakamoto’s Neighbor: My Hunt For Bitcoin’s Creator Led To A Paralyzed Crypto Genius](#) from *Forbes*

⁶⁶⁷ Stories on forums over the years include spouses and significant others who have taken computers out of spite and anger, never returning them. Some hard drives on these purportedly include hundreds of bitcoins each.

⁶⁶⁸ [Here’s why everyone should secure their Bitcoins properly](#), from Reddit

⁶⁶⁹ While many exchanges now have created purported “dark pool” or “dark liquidity” services (such as Prime from Trade Hill, prior to its closure), it is unknown how large these may be and likely that they are not using the term correctly; these should really just be called OTC markets. Other intermediary platforms may trade between these “dark pools” as well, including TruCoin. The pools exist to protect an institutions trading strategy from other participants and typically the sell side comes from large mining pools and merchant processors. In reality these are likely, hidden or reserve orders: implemented by exchanges and other marketplaces with the intent to allow traders to place larger orders discretely, in an attempt to avoid moving the market up or down. Thanks to Ken Abe for this clarification.

⁶⁷⁰ [CryptoLocker’s crimewave: A trail of millions in laundered Bitcoin](#) from *ZDnet*

⁶⁷¹ [Nearly 150 Breeds Of Bitcoin-Stealing Malware In The Wild, Researchers Say](#) from *Forbes*

⁶⁷² See also: [The Dark Economy Assessed](#) from *Coinometrics*

⁶⁷³ [Industrial Bitcoin Mine Employee Disappears After \\$190K in Alleged Theft, Fraud](#) from *CoinDesk*

⁶⁷⁴ [Bitcoin - An Analysis \[28C3\]](#) by Kay Hamacher and Stefan Katzenbeisser

⁶⁷⁵ [I just got hacked - any help is welcome! \(25,000 BTC stolen\)](#) by allinvain

⁶⁷⁶ [Investigating the allinvain heist](#) by GraphLab

⁶⁷⁷ [An Analysis of Anonymity in the Bitcoin System](#) by Fergal Reid and Martin Harrigan

⁶⁷⁸ This issue was highlighted in a passage from [Bitcoin trading website accused of defrauding thousands of customers](#) in the *Los Angeles Times*:

Because bitcoin is a decentralized currency without any real regulatory structure or way to reverse transactions, the currency is an attractive target for scammers, risk management analyst and former Federal Reserve Bank examiner Mark Williams said. “Right now in the bitcoin community, there’s no consumer protection,” he said. Williams said he wasn’t surprised to hear of companies allegedly scamming customers because many bitcoin users aren’t aware of the currency’s capacity for fraud. “You build a website, you put a piece of gold on it or a picture of a bitcoin and it gets people excited,” he said. “It’s like they check their brain at the door.”

⁶⁷⁹ One reviewer who had worked in Central Asia explained an opposite phenomenon: “A place like that is most like of the “fell off the truck” variety. It is how stolen food merchandise is converted into cash. Money laundromats are typically very nice stores in a good section of town. They sell high end merchandise. Sometimes the stores are successful businesses in themselves, often not.”

⁶⁸⁰ See [Basic Bitcoin security guide](#) from reddit. The same issue of creating and managing passwords bedevils altplatforms too: [Obtaining and offline securing ether for the upcoming Ethereum launch](#) by Andreas Brekken

⁶⁸¹ [Mind your wallet: why the underworld loves bitcoin](#) from Reuters

⁶⁸² [Mt. Gox files for bankruptcy, hit with lawsuit](#) from Reuters

⁶⁸³ [Mt. Gox Finds 200,000 Missing Bitcoin](#) from *The Wall Street Journal*

⁶⁸⁴ [Tokyo Police Formally Investigate Missing Bitcoin](#) from *The Wall Street Journal*

⁶⁸⁵ I would like to thank Petri Kajander for pointing this out.

⁶⁸⁶ [The Willy Report: proof of massive fraudulent trading activity at Mt. Gox, and how it has affected the price of Bitcoin](#)

⁶⁸⁷ [Bitcoin exchanges are more centralised than traditional exchanges. We can do so much better than this.](#) by Richard Brown

⁶⁸⁸ [Mind your wallet: why the underworld loves bitcoin](#) from Reuters

⁶⁸⁹ For discussion on Coinmarket.io see dozens of threads in the late 100s and early 200s: [CoinMarket.io | New, self-moderated support and news thread.](#)

⁶⁹⁰ [Scam exchange cryptorush implodes with epic drama \(support staff breaks ranks\)](#) from reddit

⁶⁹¹ [Cyprus police issues arrest warrant for bitcoin entrepreneur](#) from *Cyprus Mail*

⁶⁹² [Bitcoin trading website accused of defrauding thousands of customers](#) from *Los Angeles Times*

⁶⁹³ [Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk](#) by Tyler Moore and Nicolas Christin

⁶⁹⁴ Bitfoo is the international name for Bifubao. See [With Bifubao’s Wallet, Users Can Prove Funds via Cryptography](#) from *CoinDesk*

⁶⁹⁵ [Xapo Raises \\$20 Million for ‘Ultra-Secure’ Bitcoin Storage](#) from *CoinDesk* and [Introducing the Coinbase vault](#) (Coinbase does not offer insurance yet)

⁶⁹⁶ [Securing wallets by integrating a third-party Oracle](#) from CryptoCorp and [BitGo](#)

⁶⁹⁷ Even though m-of-n transactions has been supported since the acceptance of BIP 11 in 2011 and BIP 16 the following year, implementations of multisig has been slow going until recently due to lack of support from wallet software. This will likely change, yet as of this writing, no address on the Bitcoin Top 500 Rich List uses on-chain multisig.

⁶⁹⁸ [Armory Releases First Decentralized Multi-Signature Bitcoin Platform, Pledges \\$10,000 in Donation Matching Using New Simulfunding Features](#) from AccessWire

⁶⁹⁹ The usage of paper wallets raises an important question: if Bitcoin is supposed to be a new form of electronic cash, is not the usage of paper wallets (or notes) just a recreation of the old monetary order?

⁷⁰⁰ [Two-factor Bitcoin](#)

⁷⁰¹ Technically Jack Wang and his team at Bifubao/Bitfoo created the term “Wallet-as-a-service” first, for the Beijing Global Bitcoin Conference held in May 2014. See also [Wallet-as-a-Service is Here: The Coinkite API has launched!](#)

⁷⁰² Roger Ver, founder of Blockchain.info claims that the wallet is an “on-blockchain” solution yet it is still centralized – there is nothing on the blockchain that enables wallet functionality. See [Roger Ver on Blockchain’s Past, Present and Future](#) from *CoinDesk*

⁷⁰³ Personal correspondence, April 19, 2014. "The legal system is not entirely ill-equipped for cryptoledgers - particularly in relation to crime, where the law is fairly well-established," he says. "Blockchains pose more practical, rather than conceptual, problems. In terms of protecting and putting other parties on notice of property rights, new rules and transfer formalities would need to be established, with something like two-factor or three-factor authentication (or multisig) required for a valid transfer of certain types of crypto-titles. On the basis that some fraudulent transfers might still get through, however, the extent to which the market might tolerate wholly decentralised ledgers is an open question. I can't see the market - large or small - committing much by way of funds to a decentralised autonomous organization (DAO) which doesn't have a well-insured human corporate backdoor. Re-introducing some trust would, I suspect, be a price many would happily pay for the benefit of added accountability."

⁷⁰⁴ One reviewer noted that, "The conversion rates and metrics exist for many other industries and markets. But comparing them with Bitcoin would not necessarily be relevant at this stage because of the much higher barriers to entry (friction of access) in participating on the Bitcoin network."

⁷⁰⁵ Historically there are very few profitable exits for volunteer work or organizations. If this is the case in Bitcoin, one continual challenge will be monetarily incentivizing scarce talent like Bob to provide utility in the form of coding and debugging to the main codebase. And this is imperative for providing easy-to-use secure solutions for the average consumer. Failing that Bob will likely be motivated to build competing, profitable platforms of his own instead – after all why create enterprise-grade security features for free when someone else will pay for other features?

⁷⁰⁶ [Roger Ver, 'Bitcoin Jesus', Makes Largest Ever Bitcoin Donation of \\$1m](#) from *CoinDesk*

⁷⁰⁷ The "HODL" meme originally came from a Bitcoin Talk thread: [I AM HODLING](#)

⁷⁰⁸ [The Great Crash, 1929](#) and [A Short History of Financial Euphoria](#) by John Kenneth Galbraith

⁷⁰⁹ [The Essential Galbraith](#) by John Kenneth Galbraith

⁷¹⁰ I describe several others in this article (see the appendix as well): [Can Bitcoin change from a bubble economy into a growth economy?](#) Another notable one that touches on how some bitcoin adopters claim to be the "new landed gentry" ossifying into "old money"? Galbraith notes, "In all speculative episodes there is always an element of pride in discovering what is seemingly new and greatly rewarding in the way of financial instrument or investment opportunity. The individual or institution that does so is thought to be wonderfully ahead of the mob. This insight is then confirmed as others rush to exploit their own, only slightly later vision. This perception of something new and exceptional rewards the ego of the participant, as it is expected also to reward his or her pocketbook. And for a while it does." (p. 18 - 19)

⁷¹¹ [A Quick History of Cryptocurrencies BBTC — Before Bitcoin](#) by Ken Griffith and [Beenz](#)

⁷¹² [BitPay Now Processing \\$1 Million in Bitcoin Payments Every Day](#) by CoinDesk; see also this thread on reddit covering the proposal: [Why Target Must Accept Bitcoin Before Walmart Or Amazon](#)

⁷¹³ [The Feds Are Auctioning a Small Fortune in Silk Road Bitcoins](#) from *Wired*

⁷¹⁴ [Announcing Merchant Discounts: Pass Cost Savings on to Your Customers](#) from Coinbase

⁷¹⁵ See image of [Giant Poster of Mao Seizes Power in China](#)

⁷¹⁶ Myth, management of the unknown by Gianluca Miscione

⁷¹⁷ Professor Zittrain (Harvard Law School), echoing Gibson's definition of the cyberspace as a 'consensual hallucination', defined Bitcoin a 'collective hallucination'. See [What the heck is a Bitcoin?](#) at *MarketPlace*

⁷¹⁸ [Bitcoin and Complexity Theory: Some Methodological Implications](#) by Marc Pilkington

⁷¹⁹ I would like to thank John Komkov for highlighting this reference.

⁷²⁰ [Some altcoin memes are more equal than others](#) by Izabella Kaminska

⁷²¹ [Interesting posts to add to your reading stack](#) by Tim Swanson

⁷²² Tipping is just another redistribution wealth-transfer mechanism, a faucet and it is a poor market signaling mechanism. According to a paper by Lynn & McCall, "A study of diners concluded that only a very weak correlation exists between larger tips and better service. Customers in the study who rated their culinary experience as "excellent" still tipped anywhere within a broad range of 8% to 37% of the bill." See [Gratuities](#) from *The Economist*

⁷²³ [Number of transactions excluding popular addresses](#)

⁷²⁴ [State of Bitcoin Q2 2014 Report](#) from CoinDesk

⁷²⁵ [Bitcoin's failed Coup of Wall Street](#) by Brett King

⁷²⁶ Thanks to DB for his discussion on this. The corresponding image can be [viewed here](#).

⁷²⁷ I would like to thank Raffael Danielli for his discussion on this.

⁷²⁸ [The Renminbi as a Reserve Currency, Part 1](#) by Patrick Chovanec

⁷²⁹ [Accumulating foreign currency reserves](#) from Khan Academy

⁷³⁰ One reviewer noted that, “The big piece that is usually overlooked is perception of price and political stability, honesty of the government, and willingness of other nations to live under the rule of the fiat-issuing nation. If you settle in another nation’s currency, then you also agree to let that nation’s courts rule over your economy. Witness Argentina’s problems today. Nations that are perceived as corrupt, arbitrary, unfair to foreigners, or potentially unstable will not become significant settlement currencies for international trade. Thus, we see that the British pound remains a significant settlement currency despite the relatively small size of its economy. Britain is renowned for fairness of its courts, the government is stable, it is transparent. Bitcoin will never fulfill those needs. It has no courts. It has no government. It’s stability doesn’t exist. In other words, it is not a fiat currency.”

⁷³¹ [Trading the yuan: Yuawn](#) from *The Economist*

⁷³² [China New Credit Declines as Money-Supply Growth Decelerates](#) from *Bloomberg*

⁷³³ [China, U.S. to discuss yuan, monetary policy this week](#) from *Reuters*

⁷³⁴ [Bank of China Wins First Yuan Clearing Deal in Euro Area](#) from *Bloomberg* and [Top Forecaster Sees \\$4 Trillion Reason to Buy Yuan: China Credit](#) from *Bloomberg*

⁷³⁵ [The audacity of bitcoin](#) by John Normand

⁷³⁶ [Bitcoin Raises Washington Profile, to Silicon Valley’s Dismay](#) from *Bloomberg*

⁷³⁷ [Venture capital funds are shunning clean tech, but that could mean there are deals to be had](#) from *Quartz*

⁷³⁸ Data for image via [Ilan Gur](#) and [Danielle Fong](#)

⁷³⁹ [Why the Clean Tech Boom Went Bust](#) from *Wired* and [The Cleantech Crash](#) from *60 Minutes*

⁷⁴⁰ This may not be an apples to apples comparison because the majority of cleantech financing and business development was focused on government directed research which funneled scientists and entrepreneurs into chasing subsidies and tax breaks and not necessarily chasing novel innovations. They built and optimized their solutions and business models around these pillars.

⁷⁴¹ One common counterargument is that Dell does not accept RMB, that they accept credit card payments denominated in RMB. Yet the same logistical movement confronts bitcoin too, as Dell partnered with Coinbase and will simply just convert the bitcoins into fiat. See [Dell.com Partners With Coinbase to Become the Largest Ecommerce Merchant to Accept Bitcoin](#) from Coinbase

⁷⁴² [For Dell, Success In China Tells Tale Of Maturing Market](#) from *The Wall Street Journal*

⁷⁴³ A [strongman](#) is a political leader who rules by force and runs an authoritarian regime

⁷⁴⁴ L.M. Goodman explains that trust is still involved in the system from the first moment, as a user attempts to download a wallet from a trusted source; see [Dispelling some myths about Bitcoin, from a Bitcoin fan](#)

⁷⁴⁵ [Developers Battle Over Bitcoin Block Chain](#) from *CoinDesk*, [Is Double Spending Unconfirmed Transactions a Concern for Bitcoin?](#) from *CoinDesk* and [BitUndo](#)

⁷⁴⁶ [8 Million Vericoin Hack Prompts Hard Fork to Recover Funds](#) from *CoinDesk*

⁷⁴⁷ [The 9 Biggest Screwups in Bitcoin History](#) from *CoinDesk*

⁷⁴⁸ [Dr. Bitcoin E02: The Unproven Hypothesis](#) by Paul Rausch

⁷⁴⁹ [Some poor person just paid a 200BTC transaction fee to ASICminer.](#) from reddit

⁷⁵⁰ [It's Time For a Hard Bitcoin Fork](#) by Ittay Eyal and Emin Gün Sirer

⁷⁵¹ [Bitcoin News Sites & Dishonesty](#) by Tom Buttercoin

⁷⁵² [Cash for Coverage: Bribery of Journalists Around the World](#) by Bill Ristow

⁷⁵³ Some high profile Bitcoin conferences are very profitable, hence one of the reasons other adopters attempt to emulate their success.

⁷⁵⁴ I would like to thank Marshall Hayner and Jackson Palmer for suggesting this. [Coin Gorilla](#) is an early attempt at such a service.

⁷⁵⁵ [Is China’s housing bubble popping?](#) from *The Washington Post* and [Real Estate Tycoon Sees Titanic Moment for China’s Housing Market](#) from *The Wall Street Journal*

⁷⁵⁶ [Ponzis: The Science and Mystique of a Class of Financial Frauds](#) by Kaushik Basus at the World Bank

⁷⁵⁷ [BitPay Now Processing \\$1 Million in Bitcoin Payments Every Day](#) from *CoinDesk*

⁷⁵⁸ When reached for comment, an employ at BitPay explained that, “The amount of bitcoin varies but we do over \$1 million per day on average.” Personal correspondence: June 24, 2014

759 [Consumers Pay More When They Pay With Bitcoin](#) by Ben Edelman and [The Great Bitcoin Debate In Six Points](#)
by David Evans

760 [CryptoLocker's crimewave: A trail of millions in laundered Bitcoin](#) from *ZDnet*

761 [US researcher banned for mining Bitcoin using university supercomputers](#) from *PCWorld*

762 Senator Everett Dirksen allegedly said, "A billion here, a billion there, and pretty soon you're talking real money" – however according to The Dirksen Center, this may not be true; see ["A Billion Here, A Billion There..."](#)

763 One reviewer suggested that, "I would characterize this as a deficit between the cost of operation of the Bitcoin system and the realized valuation of new bitcoins."

764 [MasterCard Financials](#) from *The Wall Street Journal*

765 [Top secret Visa data center banks on security, even has moat](#) from *USA Today*

766 [Bitcoin Seen as Little Threat to Payment Firms](#) from *Bloomberg*

767 [To all of the deepbit whiners.](#) from Bitcoin Talk

768 [Salpas](#)

769 [Great Chain of Numbers](#) by Tim Swanson

770 [Script](#)

771 [Sanitizing Bitcoin: This Company Wants To Track 'Clean' Bitcoin Accounts](#) from *Forbes*

772 Personal correspondence, May 24, 2014

773 Personal correspondence, May 29, 2014

774 [BitUndo](#) and [Is Double Spending Unconfirmed Transactions a Concern for Bitcoin?](#) from *CoinDesk*

775 Personal correspondence, May 29, 2014. [Chromawallet](#); for example, see 0.134 BTC [here](#)

776 [How to make friends](#) by Preston Byrne

777 Personal correspondence, May 29, 2014. [Melotic](#) and [Bitfoo](#)

778 [Re: Decentralized Timestamp](#) by Ray Dillinger

779 [Colored coins now supporting dividends](#) from *Coinprism*

780 Attacher success probability [calculator](#)

781 This is not an endorsement of the idea but rather an explanation of what some developers have vocalized over the years. Demurrage is the cost associated with owning or holding currency over a given period. One current cryptocurrency that has attempted to experiment with this concept is [Freicoin](#). See also, [Prohibited changes](#)

782 I would like to thank Andrew Lapp for articulating this scenario and line of reasoning to me.

783 [Bitcoin Cooperative Proof-of-Stake – CPoS](#) by Stephen Reed

784 [DogeChain Statistics](#)

785 [Feathercoin](#) (case study by MaxMiner), [Worldcoin](#), [Powercoin](#), [CoiledCoin](#), [Terracoin](#) and [Auroracoin](#)

786 [Re: \[ANN\] MemoryCoin | R.I.P.](#) from Bitcoin Talk

787 See [MemoryCoin Exclusive Interview – The Random Coin of the Day](#) from *Cryptocoins News* and [Memorycoin](#)
wiki

788 [On The Longest Chain Rule and Programmed Self-Destruction of Crypto Currencies](#) by Nicolas Courtois

789 [Unobtanium Hashrate comparison chart](#)

790 [Re: Crapcoins vs Promising Coins. Short Guide: How to tell the difference?](#) by Ray Dillinger

791 [Unobtanium](#) from Coinmarketcap

792 One reviewer explained that another reason this might not occur in an open market is due to the [Wheat and chessboard problem](#).

793 [Jamaican Bobsledders Ride Dogecoin Into Olympics](#) from *Bloomberg* and [Reddit, Dogecoin support NASCAR racer at Talladega](#) from *CNN*

794 According to calculations from John Normand.

795 [Merged Mining AMA/FAQ](#) by Charlie Lee

796 [4 New Bitcoin Features Revealed by Core Developer Mike Hearn](#) from *Cryptocoins News*

797 [Gavin Andresen: Rising Transaction Fees Could Price Poor Out of Bitcoin](#) from *CoinDesk*

798 [Transparent mining, or What makes Nxt a 2nd generation currency](#) from Bitcoin Talk

799 [It Will Cost You Nothing to 'Kill' a Proof-of-Stake Crypto-Currency](#) by Nicolas Houy

800 [Cooperative Proof-of-Stake – CPoS](#) by Stephen Reed

801 [Merged Mining AMA/FAQ](#) by Charlie Lee

802 [Fluttercoin](#) was the first to implement Proof of transaction, however in its current implementation it does not work in a decentralized manner.

803 [The Marginal Cost of Cryptocurrency](#) by Robert Sams and [Hayek Money: the Cryptocurrency Price Stability Solution](#) by Ferdinando Ametrano

804 [What is dev team going to do about Dogecoin's dangerously low hashrate?](#) by Charlie Lee

805 [Charlie Lee's \(aka coblee\) final thoughts on Merged Mining](#) by Charlie Lee

806 [Dogecoin Core Development Interview](#) by Tristan Winters

807 [Dogecoin to enable AuxPoW soon - All infos inside](#) by langer_hans and [Merged mining specification](#) from Bitcoin wiki

808 [Peter Todd explains why side-chains are insecure and bad for decentralization](#) on reddit

809 One Dogecoin developer, lleti, [posted a rebuttal](#) to Charlie Lee's claims, yet did not fully address the fact that this is purely a matter of economics and time is not on Dogecoin's side. See also [Understanding Economies of Scale](#) by Digiconomist

810 [Dogeparty](#) from Humint

811 [Litecoin hashrate](#)

812 [Bitcoin hashrate](#)

813 See [Bitcoin Price Index](#) from CoinDesk

814 [Engineering the Bitcoin Gold Rush: An Interview with Yifu Guo, Creator of the First Purpose-Built Miner](#) from Motherboard and [AVALON ASIC has delivered first RIG \(68GH/s Confirmed\) 2nd out proof](#) at Bitcoin Talk

815 [The Rewards For A Bitcoin Miner](#) by Dave Hudson

816 [Bitcoin: the Stripe perspective](#) by Greg Brockman

817 [Changing Landscape of Remittances](#) from Around the Coin

818 Ripple can provide settlement infrastructure too. SWIFT does not provide settlement infrastructure. The messages contain information about the payment itself (amount, destination, etc.) but settlement is actually done through crediting and debiting of nostro/vostro accounts as the money hops from bank to bank.

819 [Ripple](#) by David Schwartz

820 [Ripple is officially open-source!](#) by Stefan Thomas

821 Nicolas Courtois has a working paper entitled, "On Four Original Sins of Open Source Crypto Currencies and Some Possibly Catastrophic Events" that discusses the vulnerabilities in this curve.

822 A lengthy debate between Greg Maxwell and David Schwartz took place last year in a Bitcoin Talk thread: [WTF happened to ripple?](#)

823 ["Decentralized", you keep using that word but I don't think it means what you think it means...](#) by L.M. Goodman

824 On March 18, 2013, the Financial Crimes Enforcement Network (FinCEN) which is part of the US Department of Treasury issued guidance ([pdf](#)) related to Anti-Money Laundering Laws (AML) which specifically discussed virtual currencies such as Bitcoin. See [History of Anti-Money Laundering Laws](#). For KYC and Money Service Business (MSB) see also, [Understanding global KYC differences](#) from PriceWaterhouseCoopers and [Am I an MSB?](#) from FinCEN

825 [Stellar](#) by Greg Brockman

826 [Mt. Gox, Ripple Founder Unveils Stellar, a New Digital Currency Project](#) from *The Wall Street Journal*

827 From [Chapter 3, Great Chain of Numbers](#). Note that Counterparty intends to 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.

828 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](#)).

829 Blockchain address: <http://blockchain.info/address/1EXoDusjGwvnjZUyKkxZ4UHEf77z6A5S4P>

830 [Backed by \\$5 Million in Funding \(4,700 BTC\), Mastercoin Is Building a Flexible, New Layer of Money on Bitcoin](#) from MarketWired

831 [Ethereum](#)

832 While some claim that all other holders of bitcoin saw a net gain in value by roughly 0.01%, the demand could have shifted simultaneously. In fact, burning their bitcoins in this way demonstrated preference for the new currency over bitcoin, a decrease in demand to hold bitcoin. Meanwhile the supply of the new units increased. Did the new coins capture all of the value created, or was some sent back to the holders of bitcoin? See [I burned BTC through blockchain.info, how do I access my XCP?](#) from Counterparty.co and the exact address was

[1CounterpartyXXXXXXXXXXXXUWLpVr](#). 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.

⁸³³ Image and data via: [Re: \[ANN\]\[XCP\] Counterparty Protocol, Client and Coin \(built on Bitcoin\) - Official](#)

⁸³⁴ Personal correspondence with dexX7 on July 29, 2014

⁸³⁵ Original announcement thread: [\[ANN\]\[CHA\] Chancecoin, a coin for betting in a decentralized casino](#) from Bitcoin Talk and [Chancecoin](#)

⁸³⁶ [Bitcoin Series 24: The Mega-Master BlockchainList](#) by Antonis Polemitis from Ledra Capital

⁸³⁷ LTBCoin's utility bridges the user-created asset category as well as crowdequity. It could potentially be used as an "app-coin" as well.

⁸³⁸ [On Mining](#) by Vitalik Buterin

⁸³⁹ Personal correspondence, July 28, 2014

⁸⁴⁰ See [Necronomicon thread: Altcoins which are dead](#). And [Blockchain 2.0 – Let a Thousand Chains Blossom](#) from *Let's Talk Bitcoin*

⁸⁴¹ See [Episode #99 – Sidechain Innovation](#) from *Let's Talk Bitcoin* and [Blockchain 2.0 – Let a Thousand Chains Blossom](#) by Tim Swanson

⁸⁴² [25-second irreversible confirmations for instant payments](#) by Sergio Lerner

⁸⁴³ 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](#))

⁸⁴⁴ [Gartner Says Supply Chain Management Software Revenue Is on Course to Reach \\$10 Billion in 2014](#) from *Gartner*

⁸⁴⁵ [SkuChain](#)

⁸⁴⁶ For a discussion on logistics and how they are "invisible" to consumers, see [I Drank a Cup of Hot Coffee That Was Overnighted Across the Country](#) from *The Atlantic*

⁸⁴⁷ [Float management](#) will likely continue to play a role either way.

⁸⁴⁸ [CoinBlaster](#)

⁸⁴⁹ At 3:50m ([video](#)) Jackson Palmer explains CoinBlaster at Hackadodge.

⁸⁵⁰ [Walmart Stores, Inc. Getting Started with EDI Implementation Guideline](#)

⁸⁵¹ [Towards Risk Scoring of Bitcoin Transactions](#) by Malte Möser, Rainer Böhme, and Dominic Breuke

⁸⁵² [Kimberley Process Certification Scheme](#)

⁸⁵³ [Saldo.mx](#); Saldo has a development team of 6 people in Mexico, India and the US and is backed by Crosscoin Ventures.

⁸⁵⁴ [Remittances to Latin America Recover—but Not to Mexico](#) from *PewResearch*

⁸⁵⁵ [Digital currency usage in the developing world](#) by Tim Swanson

⁸⁵⁶ [Remittances up 5.2% in April](#) from *PhilStar*

⁸⁵⁷ [Remittance Prices Worldwide](#) from the World Bank

⁸⁵⁸ [Pay Another Way: Bitcoin](#) from WordPress

⁸⁵⁹ [Bitcoin's Vast Overvaluation Appears Partially Caused By \(Usually\) Illegal Price-Fixing](#) by Rick Falkvinge

⁸⁶⁰ The last chart ([image](#)) they published was after Bitcoin Black Friday in November 2013 at the height of transactional volume. It is likely significantly lower today.

⁸⁶¹ See also: the report at [Scribd](#) and [coverage](#) from *CoinDesk*. Special thanks to Tuur Demeester for highlighting this chart in a [tweet](#).

⁸⁶² 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*

⁸⁶³ 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.

⁸⁶⁴ [Beenz](#), [DigiCash](#) and [FlooZ](#)

⁸⁶⁵ [Competition in the Crypto-Currency Market](#) by Neil Gandal and Hanna Halaburda ([Slides](#))

⁸⁶⁶ [The Bitcoin Question](#) by Adrian Blundell-Wignall at the OECD

⁸⁶⁷ [Lastwall](#)

⁸⁶⁸ Mike Hearn uses a new term called “marriage wallets” to differentiate his proposed solution with a multi-sig wallet for organizations. See [Design notes for supporting married wallets](#). One challenge for companies like BitPay and BitGo is that they can potentially be disintermediated by their customer base through BIP 70 (payments protocol) as well as multisig and married wallets.

⁸⁶⁹ [Satoshi Legal](#) and [SEiiAN Rewards](#)

⁸⁷⁰ [Think you own property in Greece?](#) from HNA

⁸⁷¹ [Proof-of-existence](#) and [Bistamped](#); see also [Mike Hearn: Underfunding is Leaving Bitcoin Development in Crisis](#) from *CoinDesk* and [Bitcoin contracts](#) from *Curiosity Driven*

⁸⁷² [NodeShares](#) and [Adopt-a-node](#)

⁸⁷³ [Empowered Law](#)

⁸⁷⁴ Personal correspondence, March 23, 2014

⁸⁷⁵ Personal correspondence, March 25, 2014

⁸⁷⁶ [Subledger](#)

⁸⁷⁷ [JOBS Act](#)

⁸⁷⁸ [Howey test](#)

⁸⁷⁹ [Accredited investor](#)

⁸⁸⁰ [SEC Charges Bitcoin Entrepreneur With Offering Unregistered Securities](#) from U.S. Securities and Exchange Commission

⁸⁸¹ [Move Over Kickstarter, Crypto-Equity Is the Next Frontier](#) from *PanamPost* and [The Death of Dogecoin](#) by Kevin Collier

⁸⁸² [Unauthorized practice of law](#)

⁸⁸³ [LegalZoom Gets Nod From South Carolina Supreme Court](#) from *3 Geeks and a Law Blog*

⁸⁸⁴ [Secure Asset Exchange](#)

⁸⁸⁵ [The Future of Payments: 2014](#) from *Business Insider*

⁸⁸⁶ [Common Accord](#), [Codius](#) and [Bithalo](#)

⁸⁸⁷ Legal Framework For Crypto-Ledger Transactions by Primavera De Filippi (forthcoming)

⁸⁸⁸ [Email use-cases for ‘colored coins’ and DACs](#) by Tim Swanson

⁸⁸⁹ [Overstock’s Radical Plan to Reinvent the Stock Market With Bitcoin](#) from *Wired*

⁸⁹⁰ Personal correspondence, July 31, 2014

⁸⁹¹ [Interacting with fiat institution, a guide](#) by Mircea Popescu, [SEC Charges Bitcoin Entrepreneur With Offering Unregistered Securities](#), [SEC charges bitcoin entrepreneur for share offering](#) from *MarketWatch* and [SEC Alleges Texas Man Ran \\$4.5 Million Bitcoin Ponzi Scheme](#) from LexisNexis

⁸⁹² [Investor Alert: Bitcoin and other Virtual Currency-Related Investments](#) from SEC

⁸⁹³ [“Most Bitcoiners Are Unaware or In A State of Deep Denial”](#) by Juan Llanos and [Bitreserve](#)

⁸⁹⁴ [Bitcoin’s Evolution toward Self-Destruction](#) by Dan Kervick

⁸⁹⁵ GPG and obfuscated contracts will probably not change that.

⁸⁹⁶ [New York Department of Financial Services drafts nation’s first comprehensive Bitcoin regulation](#) from *Venture Beat*

⁸⁹⁷ [The Wealthy & Influential Hijack Bitcoin In One Move](#) by James Duchenne

⁸⁹⁸ [Pebblecoin](#), [Coinaaa](#), [Hyperledger](#)

⁸⁹⁹ [Tweet](#) from Antonis Polemitis; see [Red flag traffic laws](#) and [Road Traffic History - Before the Streets Got Swamped](#) from *autoevolution*

⁹⁰⁰ [How the decline of BitTorrent helped take the edge off broadband growth](#) from *The Washington Post*

⁹⁰¹ While Mint, Ubuntu and Fedora are more popular on desktops, in terms of overall usage and penetration, Android is far and away the leader in Linux-based adoption. See [The most popular end-user Linux distributions are...](#) from *ZDNet*

⁹⁰² 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 and in most cases just 1 second) 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.

⁹⁰³ One estimate is that over the years 75% of the original code has been replaced within bitcoind by other contributors.

⁹⁰⁴ [Charlie Munger on the Psychology of Human Misjudgment](#), [The Psychology of Human Misjudgement](#), [The Best of Charlie Munger: 1994-2011](#)

⁹⁰⁵ [Xerox Memo of the Month](#)

⁹⁰⁶ [Coins.ph CEO Talks Opportunity for Bitcoin in the Philippines](#) from *CoinDesk*

⁹⁰⁷ [Concurrent but non-integrable currency circuits: complementary relationships among monies in modern China and other regions](#) by Akinobu Kuroda

⁹⁰⁸ Despite all the shortcoming discussed in this book, Bitcoin (the protocol) will still likely grow relative to other platforms in the near term due to BitLicenses (which confer barriers to entry), developer mind-share and venture funded edge-based ecosystem.