Attack of the 50 Foot Blockchain

Bitcoin, Blockchain, Ethereum and Smart Contracts

David Gerard

First edition, July 2017

ISBN-13 (print): 978-1974000067

Book site: www.davidgerard.co.uk/blockchain

Contact the author: dgerard@gmail.com

Cover art and design: Alli Kirkham www.punkpuns.com/author

Chapter 2: The Bitcoin ideology

> At first, almost everyone who got involved did so for philosophical reasons. We saw bitcoin as a great idea, as a way to separate money from the state.
>
> – Roger Ver[4]

The Bitcoin ideology propagated through two propositions:

- if you want to get rich for free, take on this weird ideology;
- don't worry if you don't understand the ideology yet, just keep *doing the things* and you'll get rich for free!

The promise of getting rich for free is enough to get people to take on the ideas that they're told makes it all work. Bitcoin went heavily political very fast, and Bitcoin partisans promoted anarcho-capitalism (yes, those two words can in fact go together), with odd notions of how economics works or humans behave, from the start.

The roots of the Bitcoin ideology go back through libertarianism, anarcho-capitalism and Austrian economics to the "end the Fed" and "establishment elites" conspiracy theories of the John Birch Society and Eustace Mullins. The design of Bitcoin and the political tone of its early community make sense only in the context of the extremist ideas ancestral to the cyberlibertarian subculture it arose from.* Most of Bitcoin's problems as money are because it's built on crank assumptions.

Libertarianism and cyberlibertarianism

Libertarianism is a simple idea: freedom is good and government is bad. The word "libertarian" originally meant communist and anarchist activists in 19th-century France. The American right-wing variant starts at fairly normal people who want less bureaucracy and regulation and consider lower taxes more important than social spending. The seriously ideological ones go rather further – *e.g.*,

---

* This section draws from *The Politics of Bitcoin: Software as Right-Wing Extremism* by David Golumbia (University of Minnesota Press, 2016).

anarcho-capitalism, the belief in the supremacy of property rights and the complete elimination of the state.

American-style libertarians abound on the Internet. Computer programmers are highly susceptible to the just world fallacy (that their economic good fortune is the product of virtue rather than circumstance) and the fallacy of transferable expertise (that being competent in one field means they're competent in others). Silicon Valley has always been a cross of the hippie counterculture and Ayn Rand-based libertarianism (this cross being termed the "Californian ideology").

"Cyberlibertarianism" is the academic term for the early Internet strain of this ideology. Technological expertise is presumed to trump all other forms of expertise, *e.g.*, economics or finance, let alone softer sciences. "I don't understand it, but it must be simple" is the order of the day.

The implicit promise of cyberlibertarianism was the dot-com era promise that you could make it big from a startup company's Initial Public Offering: build something new and useful, suddenly get rich from it. The explicit promise of Bitcoin is that you can get in early and get rich – without even building an enterprise that's useful to someone.

Pre-Bitcoin anonymous payment channels

Peer-to-peer electronic payment services existed before Bitcoin. PayPal was explicitly intended to be an anonymous regulation-dodging money transmission channel, with an anti-state ideology; in a 1999 motivational speech to employees, Peter Thiel rants how "it will be nearly impossible for corrupt governments to steal wealth from their people through their old means"[5] – though they quickly realised that being part of the system made for a much more viable business.

e-Gold was a digital currency backed by gold, founded in 1996. It was perceived as anonymous but was actually pseudonymous, and the company made their records available to law enforcement. It was quite popular before being shut down in 2009 for not having obtained a money transmitter's license in the previous several years.

Liberty Reserve in Costa Rica operated from 2006 to 2013. It was all about the anonymous money transmission, and founder Arthur Budovsky (who had previously been convicted for running a similar

operation in the US) ended up jailed for 20 years for money laundering. Some Bitcoiners regarded Liberty Reserve as a predecessor to Bitcoin and worried at the possible precedent this might set.[6]

The prehistory of cryptocurrencies

Cryptographic money was first mooted by David Chaum in his 1982 paper "Blind Signatures for Untraceable Payments"[7] and his 1985 paper "Security without Identification: Transaction Systems to Make Big Brother Obsolete."[8] Chaum founded DigiCash in 1990 to put his ideas into practice. It failed in the market, however, and closed in 1998.

Most concepts later used in Bitcoin originated on the Cypherpunks mailing list in the early 1990s. The ideology was libertarian right-wing anarchism, often explicitly labeled anarcho-capitalism; they considered government interference the gravest possible threat, and hoped to fight it off using the new cryptographic techniques invented in the 1970s and 1980s. They also tied into the Silicon Valley and Bay Area Extropian/transhumanist subculture. Tim May's "Crypto Anarchist Manifesto," a popular document on the list, is all about the promise of money and commerce with no government oversight, and anticipates many of the future promises and aspirations of cryptocurrency.[9]

Chaum's DigiCash was not acceptable to the Cypherpunks, as a single company confirmed every participant's signature. They wanted something that didn't rely on a central authority in any way.

Adam Back proposed Hashcash to the list in 1997, money created by guessing the reversal of a cryptographic hash; Nick Szabo put forward Bitgold and Wei Dai b-money in 1998. These were all bare proposals, without working implementations.

"Cypherpunk" was a pun on "cyberpunk." Cyberpunk science fiction of the 1980s never got much into pure bank-free cryptographic currencies; it mostly treated the idea of transmitting money digitally at all as being interesting enough for story purposes. (If William Gibson had thought of Bitcoin for his cyber-heist short "Burning Chrome," it could have been set in the present day.) The Cypherpunks got very excited about Neal Stephenson's 1999 novel *Cryptonomicon*, one plot thread of which involves a fictional sultanate

promoting a cryptographic digital currency, even though the book example is issued by a government and backed by gold.

An anonymous person calling himself "Satoshi Nakamoto" started working on Bitcoin in 2007,[10] as a completely trustless implementation of the b-money and Bitgold proposals[11] (though Nakamoto wasn't aware of Szabo's work until quite late in the process).[12] In 2008, he emailed Adam Back with some of his ideas, and six weeks later announced the Bitcoin white paper on the Cryptography and Cryptography Policy mailing list, a successor to the Cypherpunks list. It was, at last, a proposal with a plausible decentralisation mechanism, soon followed by actual working code that people could try. Nakamoto and list contributor Hal Finney tested the software in November and December 2008, and Bitcoin 0.1 was released in January 2009.

The conspiracy theory economics of Bitcoin

The *gold standard* – an economy with a finite money supply – was accepted mainstream monetary policy up to the early 20th century, when the debts from World War I made it infeasible. Even the winners in World War I tried to back all the paper (that the economy had actually run on since the late 1600s) with gold until the 1930s. But they suffered manic booms and devastating busts, over and over, because there was too much economic activity for the gold on hand.

It took until the Great Depression for governments to accept that managing the money supply – injecting money every now and then, managing interest rates, requiring banks to be backed – was not optional, and that they just couldn't do that on gold. Countries recovered from the Great Depression pretty much as they left the rigid gold standard behind, because managing your money supply works much better and is much more stable. A version of the gold standard lingered in the form of the Bretton Woods system until 1971, but rigid backing of currency with gold had been delivered the fatal blow by World War I and then the Great Depression.

But a standard mode of pseudoscience is to adopt and fervently defend a discarded idea, and "gold bugs" were no exception, ardently pushing the version of the gold standard that had just been demonstrated utterly inadequate to a functioning economy.

(Gold bugs are frankly bizarre. There are lots of rarer metals than gold, but you never hear about "rhodium bugs" or "scandium bugs" or even "platinum bugs.")

The John Birch Society is an American far-right fringe group that has long claimed that inflation comes from central bank increase of the money supply – in fact, they try to redefine "inflation" to mean this – for the purpose of stealing "value" from the people, and that this is why the gold standard was abolished and the Federal Reserve founded.[13] Eustace Mullins furthered these ideas amongst conspiracy theorists with the 1993 reprint of his 1952 book *Secrets of the Federal Reserve*, in which he blames the Fed's creation on "the Rothschild-controlled Bank of England." (Mullins was also famous for his anti-Semitism; every time Mullins said "banker" he meant "Jew," but this mostly isn't *consciously* the case amongst Bitcoiners, who only *occasionally* rant about Zionists.)

These ideas had also been propagated in the mainstream by Ron Paul in the wake of the 2008 credit crunch and the quantitative easing (just printing money, to kick-start the economy) that followed. Though Paul isn't a fan of Bitcoin – he wants a return to actual gold after he abolishes the Fed.[14]

Old ideologies come back when they fill a present desire and there's an opening for them. So these claims, somewhere between incorrect and nonsensical, showed up full-blown in Bitcoin discussion, proponents straight-facedly repeating earlier conspiracy theories as if this was all actually proper economics. Because if it is, then maybe they'll get rich for free!

In this context, and particularly in Bitcoin discourse, you'll see many words that look like English but are actually specialised conspiracy theory jargon. "Liberty" means only freedom from government; "tyranny" means only government; "force" and "violence" mean only government force and violence; "open societies" is a code word for "free market without regulations"; "freedom" means "free market without regulations" and only that.

Pure commodities – gold and silver – haven't done the job of money well for a few hundred years, and Bitcoin wants to be money but was set up to work like a commodity. Nakamoto put a strict limit on the supply of bitcoins: there will only ever be 21 million BTC. So advocates claim Bitcoin is thus, somehow, sufficiently similar to gold to serve as a "store of value" in the desired manner, even "an Internet of *true* value" (whatever "true" means there). This is despite its

extreme volatility making it almost useless as a store of value, and despite it being way harder to use as money than any currency should be, even for its few use cases.

Bitcoin ideology bought into the entire Federal Reserve conspiracy package. The Fed is a plot to use inflation to steal value from the people and hand it to a shadowy cabal of elites who also control the government; the worldwide economy is in danger of collapse at any moment due to central banking and fractional reserve banking; gold – sorry, Bitcoin – has intrinsic value that will protect you from this collapse. Advocates repackage and propagate these ideas almost verbatim, even when they almost certainly don't know who or where they trace back to.

Conventional economics views inflation – a decline in money's purchasing power – as a phenomenon of consumer prices, consumer confidence, productivity, commodity and asset prices, etc., which a central bank then responds to with monetary policy. Printing more money *can* cause inflation, but it's not the usual cause. The conspiracy theorist view is that it's the central bank intervention *causing* the inflation. Bitcoin ideology assumes that inflation is a purely monetary phenomenon that can *only* be caused by printing more money, and that Bitcoin is immune due to its strictly limited supply. This was demonstrated trivially false when the price of a bitcoin dropped from $1000 in late 2013 to $200 in early 2015 – 400% inflation – while supply only went up 10%.

Nakamoto's 2008 white paper alluded to these ideas, but the 2009 release announcement for Bitcoin 0.1 states them outright:[15]

> The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible.

Bitcoin failed at every one of Nakamoto's aspirations here. The price is ridiculously volatile and has had multiple bubbles; the unregulated exchanges (with no central bank backing) front-run their customers, paint the tape to manipulate the price, and are hacked or just steal their users' funds; and transaction fees and the unreliability

of transactions make micropayments completely unfeasible. Because all of this is based in crank ideas that don't work.

A week after Bitcoin 0.1 was released, Jonathan Thornburg wrote on the Cryptography and Cryptography Policy mailing list: "To me, this means that no major government is likely to allow Bitcoin in its present form to operate on a large scale."[16] In practice, governments totally did, and treated it like any other financial innovation: give it room to run, make it very clear that regulation still applies, give it a bit more room to run, repeat. The advocates' ideas of how governments work were already at odds with completely predictable reality.

(I'm still baffled at the notion that the governments of first-world countries are somehow *fundamentally against* the idea of people doing well with innovations in finance.)

Austrian economics

The acceptable face of this conspiracy cluster is Austrian economics, first put together in its present form by Ludwig von Mises (hence "Austrian"). Its key technique is *praxeology*, in which economic predictions are made *entirely* by extrapolating from fundamental axioms. It explicitly repudiates any sort of empirical testing of predictions, and holds that you can't predict future behaviour from past behaviour even in principle, so testing your claims is meaningless:[17]

> The subject matter of all historical sciences is the past. They cannot teach us anything which would be valid for all human actions, that is, for the future too …
>
> No laboratory experiments can be performed with regard to human action. We are never in a position to observe the change in one element only, all other conditions of the event remaining unchanged. Historical experience as an experience of complex phenomena does not provide us with facts in the sense in which the natural sciences employ this term to signify isolated events tested in experiments. The information conveyed by historical experience cannot be used as building material for the construction of theories and the prediction of future events …

> [Praxeology's] statements and propositions are not derived from experience. They are, like those of logic and mathematics, a priori. They are not subject to verification or falsification on the ground of experience and facts.

Despite this, proponents keep *making* predictions and claims, and insisting they are, somehow, still worth listening to and applying to the world.

Austrian economics was heavily promoted by heterodox* economist Murray Rothbard, founder of the Ludwig von Mises Institute. Rothbard invented the term *anarcho-capitalism* for his ideology that a complete absence of government is essential, and that property rights, which are paramount, will somehow still function without it. An offence against one's property is equivalent to an offence against the self; so the "Non-Aggression Principle" holds that trespassing is aggression, but the owner shooting you for trespassing somehow isn't. Police will be replaced with private security services and courts with arbitration services. Really extreme Austrians like Hans-Herman Hoppe admit that all this would lead directly to functional feudalism. Which becomes neoreaction and the alt-right, but Elizabeth Sandifer already wrote that book.[18] †

Austrian economics has produced vast quantities of detailed theory to support the claim that a gold standard is the only sensible way to run an economy – rather than the more conventional view that a zero-sum economy quickly seizes up, both in theory and practice‡ – and that central banks and fractional reserve banking will inexorably lead to a collapse. *Disaster is imminent*, and you need to be hoarding *gold*.

Sadly for Bitcoin, most Austrian economists aren't fans – even as Bitcoiners remain huge fans of Austrian economics.[19] You will find Austrian jargon in common use in the cryptocurrency world.

Proponents of Austrian economics include the fringe economics blog *Zero Hedge*, which has confidently predicted two hundred of the last two recessions. *Zero Hedge* covers Bitcoin extensively, and Bitcoiners are fans in turn.

---

* *Heterodox*: a crank with a job. Austrian economics is funded by rich people who want theoretical backing for being selfish.

† I'd never encountered American-style ideological libertarianism and anarcho-capitalism before the Internet. When I first heard about it, I honestly thought it was a wacky Swiftian political satire that nobody could actually *believe*.

‡ Austrian economists *really hate* the example of (see Wikipedia) the Capitol Hill Babysitting Co-op.

Chapter 3: The incredible promises of Bitcoin!

Nobody buys a toothbrush on the basis that the toothbrush market will go *to the moon!* (There hasn't so far been a toothbrush asset bubble.) This is, however, the standard selling point for cryptocurrencies. As is claiming the selling point is anything other than hope that it will go to the moon.

Advocates claim all manner of practical use cases for Bitcoin. A lot of the claims contradict each other, and indeed the actual software; others merely run aground on reality. They mix up hypothetical ideas (most of it) and what is robust technology that actually exists (almost none), with bogus economics to boot. Just as long as they can get you to *buy Bitcoin*.

After the first Bitcoin bubble popped, many of these claims were carried forward unaltered into contemporary business "Blockchain" hype.

The Bitcoin Wiki answers many common objections on a "Myths" page.[20] The answers are of varying persuasiveness.

Decentralised! Secured by math!

Bitcoiners hold that immunity to central control is so overwhelmingly important that it's completely worth all that electricity wasted on mining. And the maths is unbreakable!

In practice, mining naturally recentralises due to economies of scale, so a few large mining pools now control transaction processing – and even though the cryptography is mathematically robust, the rest of the system is approximate, with attacks being a matter of how much economic power you can bring to bear. Pools with a large percentage of the mining power can attack the system in various ways, and have been caught doing so in the past. (*See* Chapter 5: How Bitcoin mining centralised.)

And that's before even considering bad user security, or exchanges written in dodgy PHP. Bitcoin's cryptography is solid, but it's a bit like putting a six inch thick steel vault door in a cardboard frame.

Anonymous!

Bitcoin was widely touted early on as anonymous – on the blockchain, nobody knows you're a dog. Of course, with every confirmed transaction logged in the blockchain forever, it's pseudonymous at best; as the case of Ross Ulbricht and the Silk Road showed (*see* Chapter 4), law enforcement will happily do the tedious legwork of tracing your transactions if you motivate them sufficiently.

There are ways to increase your anonymity, such as *mixers* – send coins to an address, they shuffle them with other people's coins, and you get them back later minus a percentage. (Assuming the mixer isn't a scam that just takes your coins.) There is also the trick of buying a chain of other cryptocurrencies in succession, to cloud your trail over multiple chains; though exchanges are increasingly wise to this one and tend to kick such traders off for obvious money laundering.

Instant! No fees!

Nakamoto's original 2008 white paper notes that Bitcoin will naturally progress to a transaction fee-based economy to pay the miners. "No fees!" was still a perennial claim for many years, until mid-2015 when it became glaringly obvious that this simply didn't hold any more.

Blocks in the blockchain were limited to 1 megabyte early on. But the blocks are now full – Bitcoin has reached capacity. This means a transaction may fail or be delayed for hours or days (if it isn't just dropped), unless the user correctly guesses a large enough fee to get their transaction into the block. The Bitcoin community is unable to agree on how to fix this.

The fees and delays mean that Nakamoto's 2009 dream of Bitcoin as a channel for micropayments becomes impossible (even as that dream contradicts the 2008 white paper).

No chargebacks!

Transactions are irreversible, and no human can intervene to fix mistakes. You might think this is obviously bad, but the white paper claims this as an *advantage* of the Bitcoin system. Bitcoin advocates

fervently believe that the one thing merchants fear most is credit card chargebacks, and that "no chargebacks" is the best hook Bitcoin could have.

Bitcoin Wiki's "Myths" page says: "Allowing chargebacks implies that it is possible for another entity to take your money from you. You can have either total ownership rights of your money, or fraud protection, but not both."

In practice, consumers, businesses and banks overwhelmingly expect errors or thefts to be reversible. There is negligible demand for a system where human intervention to reverse an error is impossible. Even merchants, as much as they dislike chargebacks, turn out to prefer consumer confidence and payment methods people will actually use.

When mining rig manufacturer Butterfly Labs failed to deliver rigs on time, credit card and PayPal purchasers could do (and did) chargebacks; those who bought using bitcoins were out of luck.

(Butterfly Labs also bought satirical site buttcoin.org to replace a detailed takedown of one of their terrible mining offerings with an advertising page;[21] the main product of this effort was the Federal Trade Commission saying "buttcoin."[22])

Be your own bank!

"Secured by math" means the cryptography is strong – but it says nothing about everything else you need to use bitcoins safely in practice. "Be your own bank" means you take on the job of providing *all* the security and technical knowledge that a regulated professional institution normally would.

The Bitcoin Wiki offers a page with step-by-step instructions on how to secure your personal Bitcoin wallet that would dismay even a typical IT professional, let alone a casual computer user.[23] You will need a security specialist's understanding of the possible modes of attack on a modern operating system, how to encrypt all data securely and yet accessibly, password strength, backup procedures, how to securely erase a disk, the quirks of whatever Bitcoin wallet software you're using …

This is why the vast majority of users store their bitcoins on an exchange like it's an unregulated and uninsured savings bank, even

though the exchanges' security and reliability record is dismal. (Keeping your money in a sock under someone else's bed.)

Better than Visa, PayPal or Western Union!

There is no way on earth that Bitcoin could possibly scale to being a general utility. At 1 megabyte per block, the blockchain can only do a maximum of 7 transactions per second, *worldwide total*. Typical throughput in early 2017 was 2 to 4 TPS.

Compare with the systems Bitcoin claims it can replace: PayPal, which ran about 115 TPS by late 2014;[24] Visa, whose 2015 capacity was 56,000 TPS;[25] even Western Union alone averaged 29 TPS in 2013.[26]

Various off-chain workarounds have been proposed (sidechains, Lightning Network); advocates talk about these as if they already exist, rather than being stuck in development hell.

Advocates sometimes excuse the electricity wasted on mining by claiming that it's nothing compared to the energy used by the conventional banking system; this is simply false, with Bitcoin mining taking thousands of times the energy per transaction.[27]

Remittances!

Bitcoin is put forward as the obvious replacement for Western Union for people working in rich countries to send money back to their families in poor ones – even for the present-day case where you need to convert to and from bitcoins at each end.

The bit where you transmit money between countries is not expensive at all – you pay Western Union to maintain services, cash on hand and so on for the "last mile" of the journey. With Bitcoin, the conversion fees at each end usually add up to more than the banking network would charge; the ten-minute transmission time (if it's that fast) turns out not to make up for the delays in purchasing the coins for the sender or selling them for the receiver; the price volatility is extreme enough to affect the amount transmitted. The remittance case could only work if Bitcoin were already a generally accepted international currency.

Rebit.ph is making a serious attempt at Bitcoin-based remittances to the Philippines, but has foundered on the volatility of Bitcoin prices and difficulties in exchanging the bitcoins for pesos at the far end. They eventually had to set up a Bitcoin exchange just to have sufficient conventional currency on hand.[28]

Bank the unbanked!

There are over two billion people in the world who have no bank account or access to even basic financial services; "banking the unbanked" is much discussed in international development circles. Around 2013, Bitcoin advocates started claiming that Bitcoin could help with this problem. Unfortunately:

- The actual problems that leave people unbanked are the bank being too far away, or bureaucratic barriers to setting up an account when you get there.
- Unless they use an exchange (which would functionally be a bank), they'd need an expensive computer and a reliable Internet connection to hold and update 120 gigabytes of blockchain.
- Bitcoin is way too volatile to be a reliable store of value.
- How do they convert it into local money they can spend?
- 7 transactions per second worldwide total means Bitcoin couldn't cope with just the banked, let alone the unbanked as well.
- A centralised service similar to M-Pesa (a very popular Kenyan money transfer and finance service for mobile phones) might work, but M-Pesa exists, works and is trusted by its users – and goes a long way toward solving the problems with access to banking that Bitcoin claims to.

Advocates will nevertheless say "but what about the unbanked?" as if Bitcoin is an obvious slam-dunk answer to the problem and nothing else needs to be said. But no viable mechanism to achieve this has ever been put forward.

Economic equality!

Bitcoin offered "equality" in that anyone could mine it. But in practice, Bitcoin was substantially mined early on – early adopters have *most* of the coins. The design was such that early users would get vastly better rewards than later users for the same effort.

Cashing in these early coins involves pumping up the price and then selling to later adopters, particularly during the bubbles. Thus, Bitcoin was not a Ponzi or pyramid scheme, but a pump-and-dump. Anyone who bought in after the earliest days is functionally the sucker in the relationship.

"Why should I spend money to make these guys rich?" is such a common objection that the Bitcoin Wiki answered it: "Early adopters are rewarded for taking the higher risk with their time and money." It is entirely unclear what the "risk" involved was, or how this would convince anyone who didn't already agree.

In economics, the *Gini coefficient* is the standard measure of how inequitable a society is. This is tricky to determine for Bitcoin, as it's not quite a "society" in the Gini sense, one person may have multiple addresses and many addresses have been used only once or a few times. (The commonly-cited figure of 0.88 is based on one small exchange in 2011.[29]) However, a Citigroup analysis from early 2014 notes: "47 individuals hold about 30 percent, another 900 hold a further 20 percent, the next 10,000 about 25% and another million about 20%"; and the distribution "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."[30]

Dorit Ron and Adi Shamir found in a 2012 study that only 22% of then-existing bitcoins were in circulation at all, there were a total of 75 active users or businesses with any kind of volume, one (unidentified) user owned a quarter of all bitcoins in existence, and one large owner was trying to hide their pile by moving it around in thousands of smaller transactions.[31]

(Shamir is one of the most renowned cryptographers in the world and the "S" in "RSA encryption"; of course, Bitcoiners attempted to disparage his credentials and abilities.)

The usual excuse is to say that it's still early days for Bitcoin. However, there are no forces that would correct the imbalance.

The supply is limited! The price can only go up!

Bitcoin is an imitation of the gold standard; the supply is strictly limited. Advocates tout this as an advantage as a currency. Hal Finney said in 2009:[32]

> As an amusing thought experiment, imagine that Bitcoin is successful and becomes the dominant payment system in use throughout the world. Then the total value of the currency should be equal to the total value of all the wealth in the world.

Bitcoin advocates then adopted this idle musing as something that would *obviously* happen.

The problem is that Bitcoin is deflationary. Let's assume for a moment that Bitcoin economic theories work. As economic value traded in Bitcoins increases, the limited supply means the economic value per bitcoin goes up, which means that the price of things in bitcoins goes down. This means the dollar value of one bitcoin indeed goes up! However, it also means there's absolutely no incentive to spend your bitcoins if they'll always be worth more tomorrow. This means economic activity goes down, and if there are alternatives – other cryptocurrencies, or just using existing payment systems – Bitcoin loses users and interest.

In practice, the price of Bitcoin goes up when there is demand for it as a speculative commodity, drops when demand drops and is hugely volatile because trading is so thin. But it's important to note that this idea wouldn't work even in hypothetical Bitcoin economics.

But Bitcoin saved Venezuela!

Periodically, there will be a rash of news stories claiming that Bitcoin has become popular in some country suffering economic problems, such as Venezuela, India or Argentina – because the word "Bitcoin" makes a headline catchy, even if there's nothing to the story. This transmutes into claims that Bitcoin will definitely take over the world, any day now. Or advocates will respond to scepticism "but Venezuela!"

These claims always fall apart on closer examination. Venezuela is a typical example: all the coverage traces back to a story in Libertarian magazine *Reason*, fiercely advocating Bitcoin as a way to avert the

spectres of socialism and regulation.[33] One of their interviewees had been arrested for stealing electricity to mine bitcoins, which the author describes as a "government crackdown" on "freedom" because "bitcoin mining is arguably the best possible use of electricity in Venezuela".

A story in *The Guardian* in the wake of the *Reason* story appears to be where the rest of the press picked it up. It speaks of some Venezuelans relying on Bitcoin for "basic necessities," and was based on interviews with a Bitcoin exchange owner, one of his employees and two of his customers.[34] The author had previously written of Argentina and bitcoin.[35]

These two questionably-founded stories were echoed and elaborated upon by the rest of the press, including – among *many* others – the *Washington Post* claiming that Bitcoin mining is "big business" in Venezuela,[36] the *New York Times* that Bitcoin has "gained prominence" *because* of Venezuela[37] or BBC News repeating claims from a Bitcoin boosterism blog[38] – all of this being factoids repeated in a media game of "telephone."

The Venezuelan volume on LocalBitcoins (a site for arranging person-to-person Bitcoin trades) at the time was on the order of 200-300 BTC per week,[39] which isn't nothing, but is negligible in the context of a whole country, and has tracked fairly closely with LocalBitcoins usage in other countries.

When the economy collapses, Bitcoin will save you!

No, really: there are Bitcoin advocates who seriously look forward to economic collapse as an opportunity for Bitcoin – continued availability of high powered computing machinery, mining chip foundries, fast Internet and electricity presumably being absolutely assured in the grim meathook Mad Max petrolpunk future. (And we can use colloidal Litecoin for antibiotics.*)

Even lesser crises get them all excited. Nick Szabo wrote up how to fix the Greek financial crisis of 2015 with Bitcoin.[40] Someone responded to the Cyprus financial crisis of 2013 (which did include the much-feared government haircut of bank account deposits over

* "The silver to Bitcoin's gold"… oh, never mind.

the insured €100,000) with a house music anthem about "the blockchain."[41]

You can use Bitcoin to buy drugs on the Internet!

This one is completely true and accurate, but Bitcoin advocates don't seem to like mentioning it for some reason.

Chapter 4: Early Bitcoin: the rise to the first bubble

The tulip bulb era

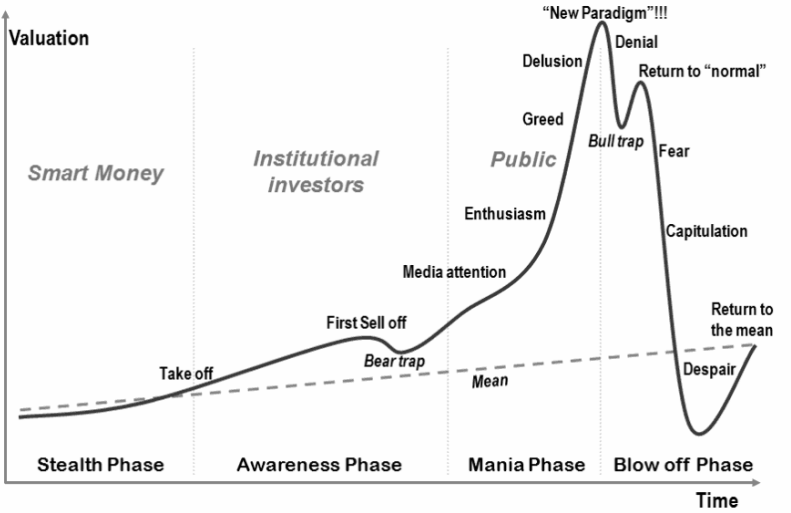
Asset bubbles follow a standard progression:

1. *Stealth phase:* The price of an asset is going up.
2. *Awareness phase:* Some investors become confident, enthused by the rise.
3. *Mania phase:* Popular buzz; media coverage. The public see these first investors and buy because others are buying, with the implicit assumption that there will always be Greater Fools to sell it on to. This is what makes a bubble: investing to sell to other investors. Someone will say that the old rules don't apply any more.
4. *Blowoff phase:* The old rules turn out to still apply. The bubble runs out of Greater Fools; prices collapse.

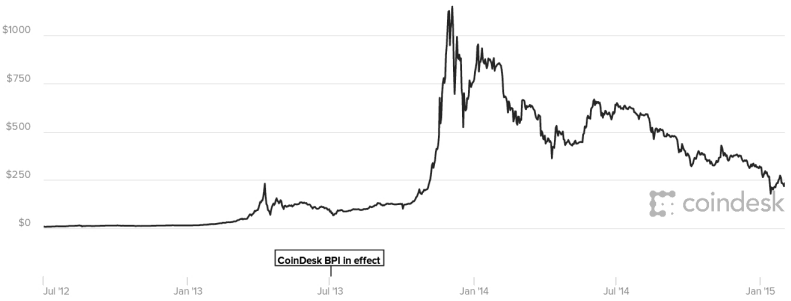
The asset need not be a commodity, *e.g.*, the Beanie Baby craze of the late 1990s, in which the asset was various instances of a manufactured product line controlled by a single company. (Though after that crash, at least you had a nice cuddly toy.) The key point is the "mania phase."

Charles Mackay's superlative *Memoirs of Extraordinary Popular Delusions and the Madness of Crowds*, first published in 1841, remains an excellent and accessible introduction to economic bubbles and the thinking behind them, starting with the Tulip Mania of 1637 and the South Sea Bubble of 1720.[42] Bitcoin is a completely standard example.

The first bitcoin was mined in January 2009, but for the first year the enthusiasts just exchanged them amongst themselves for fun. The first known conversion to conventional currency was by Martti Malmi, ardent anarcho-capitalist and Bitcoin core coder: "I sold 5,050 BTC for $5,02 on 2009-10-12."[43] The first exchange site was bitcoinmarket.com, which opened 6 February 2010. The famous first commercial transaction (two pizzas, cost $30 including tip, for 10,000 BTC[44]) was a few months later, on 22 May 2010.[45]



"Stages in a bubble" by Jean-Paul Rodrigue, 2008.[46]



Bitcoin prices, January 2012 to January 2015. Totally no resemblance to the above. Data: coindesk.com

From there the price rose steadily to 1c in July 2010. Bitcoin version 0.3 was mentioned on 11 July by tech news site Slashdot, gaining it some notice in the technology world, and inspiring the founding of the Mt. Gox exchange. In November 2010, WikiLeaks released the US diplomatic cables dump; the site was cut off from Visa, Mastercard and PayPal shortly after at the behest of the US government, but could still receive donations in Bitcoin. The price of a bitcoin hit $1 by February 2011.

In April 2011, anarcho-capitalist and businessman Roger Ver, who had made his fortune with computer parts business Memory Dealers, heard a segment about Bitcoin on the libertarian podcast Free Talk Live. Ver promptly went to Mt. Gox, the Bitcoin exchange mentioned on the show, and bought $25,000 worth of Bitcoins, single-handedly pushing the price up from $1.89 to $3.30 over the next few days. He would spend the next few years buying and advocating Bitcoin, branding himself "Bitcoin Jesus."

The earliest minor bubble grew and popped in June 2011, after an article on the Silk Road darknet market, mentioning Bitcoin, in *Gawker*. 1 BTC momentarily peaked at $30, before dropping to $15 after Mt. Gox was hacked in June, and slowly declining to $2 by December. By a year later, in December 2012, it had risen to $13. (With minor wobbles such as the August 2012 crash when the Pirateat40 Ponzi scheme collapsed.)

In this era, Bitcoin was largely evangelised by advocates for its hypothetical use cases and political possibilities. The actual use case was buying drugs on the Silk Road, the first notable darknet market, which started in January 2011. Mining at home could still be profitable at this time.

The bubble really got going in early 2013. By March, the price had hit $50 and *The Economist* warned that this was really obviously a bubble, noting how closely the price tracked Google searches for "bitcoin".[47] It hit $266 in April after a month of going up 5-10% *daily*, crashed to $130 in May and $100 in June, and rose steadily through the rest of the year – with occasional hiccups when Mt. Gox, by now the largest Bitcoin exchange, handling 70% of all Bitcoin transactions, had unexpected delays in allowing customers to cash out in US dollars.

The Silk Road was busted in early October and Bitcoin plummeted from $145 to $110. But it rose again with increased interest from China, with highly efficient mining operations starting up with custom-made ASIC mining chips, and local exchanges gaining great popularity.[48] The price started November at $350, and peaked at $1250 – or at least that was the spot price on Mt. Gox, and users were once again reporting problems withdrawing dollars. In December it started at $500, jumped to $1000 and fell back to $650 – the standard bubble peak had passed.

Mt. Gox stumbled along for a few months then finally collapsed, taking everyone's deposits with it; it later came out that they had been

insolvent since at least 2012. The price declined through the rest of 2014, bottoming out just below $200 in early 2015. As a currency, Bitcoin did somewhat worse in 2014 than the Russian rouble and the Ukrainian hryvnia.

It is important to note that Bitcoin advocates believed the late 2013 peak was not a bubble, but the natural upward progression of the price as Bitcoin increased its share of the economy; *e.g.*, Rick Falkvinge's March 2013 piece "The Target Value for Bitcoin Is Not Some $50 or $100: It is $100,000 to $1,000,000."[49] The collapse came as a complete shock to many; when Mt. Gox went down, Reddit /r/bitcoin posted and pinned suicide hotline numbers.

The art of the steal

As a financial instrument born without regulation, Bitcoin quickly turned into an iterative exploration of precisely why each financial regulation exists. A "trustless" system attracts the sort of people who just can't be trusted.

Many crypto scams are quite complex; some are simpler than you might expect. Many are everyday dodgy investment opportunities but with Bitcoin. It can be difficult to distinguish malice from incompetence. The general problem is that you don't know who or where these people are, and they routinely just disappear with everyone's money.

Scams common to the cryptocurrency world include:[50]

- *Ponzi schemes:* in which early investors are paid using money from later ones. These are so attractive to crypto fans that when Ethereum took blockchains and added "smart contracts" (programs that run on the blockchain), the first thing people did was write automatic "honest" Ponzis.
- *High-yield investment programmes:* a variety of Ponzi scheme. You might think it obvious that no investment scheme could pay 6% interest per week sustainably, particularly when it claims a "secret" investment strategy, but what worked on Bernie Madoff's victims works on Bitcoiners.
- *Coin doublers:* send it a small amount of bitcoins and you'll get double back! (No reason is given why anyone would just double your money.) Send a larger amount straight after and

… you won't. You'd think people would catch on, but years later these keep popping up and finding suckers.

(There's another layer of scam in there: the "doubler" *never* sends back coins. But it's publicised with a "warning" about the scam. Others think "hold on, if I only send coins once it'll never see me as a repeat user!" They send in a small amount of coins, which of course is not doubled. It's a scam which relies on the sucker thinking they're the scammer.[51] A similar scam ran in the game RuneScape.[52])

- *Mining software:* if you aren't designing your own mining chips and running them off super-cheap power, you won't have been able to break even mining Bitcoin since late 2013. But people keep claiming you can still mine on your PC. The software frequently includes malware.
- *Mining hardware:* there are real sellers of mining hardware (though you are unlikely to come out ahead of costs). The scam is to run it for months "testing" it: customers pay for hardware, you use their money to build it and you mine with it for the few months it's viable before you send it to them. Butterfly Labs was the most notorious culprit,[53] but far from the only one. (Butterfly's co-founder turned out to have a conviction for mail fraud;[54] Bitcoin scammers are often serial scammers.)
- *Cloud mining:* you invest in remote mining hardware. Many such schemes appear indistinguishable from Ponzis; there is generally no evidence the money-printing machine you're renting even exists.
- *Scam wallets:* sites offering greater transaction anonymity, but which just take everyone's bitcoins after a while.
- *Biased "provably fair" gambling:* "Provably fair" gambling sites generate their random numbers in advance then send you a cryptographic hash of the sequence of numbers, so you don't know the numbers ahead of time but you can verify the hash afterwards.[55] Some sites, if you *don't* grab the hash, then use a biased sequence of numbers instead.[56]
- *Scam versions of normal services:* exchanges, bitcoin mixers, shopping deal sites and so on. You have no idea who these people are, and every now and then they'll just take your bitcoins or link you to phishing or other scam sites, possibly including the gift of malware.

Fortunately, Bitcointalk.org deals harshly with scammers: it may add a "scammer" tag to someone's forum name, or list their site in the "List of Bitcoin Scam Sites" thread.

Many Bitcoin advocates consider the scammers worth it to be free of government regulation. Anarcho-capitalist Jeffrey Tucker wrote an amazing apologia, "A Theory Of The Scam,"[57] in which he admits Bitcoin is suffused with fraud, but posits that "scam artists are the evil cousins of genuine entrepreneurs" and are actually a sign of *health* for an area – so, since good things had scams, this scam-riddled thing must therefore be good! (With all this horse poop there's *gotta* be a pony in here.) No doubt subprime-mortgage-backed collateral debt obligations, Business Consulting International and Bernard L. Madoff Investment Securities LLC were just severely underpriced investment opportunities.

Pirateat40: Bitcoin Savings & Trust

> Now that Pirateat40 closed down his operatations thanks to all the fud that was going on and growing on the forum, I expect everyone that spreads this fud, accused and insulted Pirate and the people that supported him to apologize. Not only did Pirate brought us a great opportunity for investors (once in a lifetime actually), he did help stabilise and grow steadily bitcoin price, volume exchange, and thus contributed to the success of bitcoin. For that, Pirate, I want to thank you. You've done a wonderful work, and I hope you're stay around here.
>
> – Raphael Nicolle, founder of the Bitfinex exchange, just after Bitcoin Savings & Trust collapsed[58]

By 2012, as the Bitcoin subculture was heating up, high-yield investment programmes – *i.e.*, Ponzi schemes – had begun manifesting in the bitcointalk.org "Lending" section. One user even literally called high-yield investment programmes a "Bitcoin Killer App".[59]

The most famous of these was Bitcoin Savings & Trust, opened in late 2011 by Trendon Shavers, *a.k.a.* Bitcointalk forum user Pirateat40 (named after the song "A Pirate Looks at Forty" by Jimmy Buffett). It offered interest of 7% weekly – or about 3300% annually – on

investments over 25,000 BTC. Hands up anyone who can see a problem here …

Investment was strictly limited and accounts were much-coveted. Pirateat40 was a VIP Donor (50 BTC) to Bitcointalk; he built up a strong forum reputation and got other highly-rated people to resell his investment programme, offering "Pirate Pass-Through" bonds. Those who pointed out that this had all the really obvious signs of being a Ponzi scheme had much lower forum reputations, especially after saying this.

Pirateat40 claimed to be making his money from Bitcoin market arbitrage, including selling bitcoins in person or in large quantities. Others were not reassured; he had so many bitcoins in his scheme that others worried at the effect on Bitcoin itself when the scheme collapsed.[60]

On 17 August 2012, basic arithmetic reasserted itself. Pirateat40 announced the closure of Bitcoin Savings & Trust. He said he had 500,000 BTC (about $5.6 million) in the fund as of its closure and that he would be returning it to investors.[61] Apart from some refunds to friends and long-time investors, this of course didn't happen.

On 17 September, Pirateat40 announced on IRC that "the earliest estimated time that coins can begin moving is Friday, Oct 12th" (not that any coins actually moved on 12 October). He also declared that "Those looking to file a suit against me or BTCST will not be eligible for repayment" and "Threats are taken seriously by myself and my attorney. A few of you will find out how serious I mean."[62]

Burnt investors tracked him down. They found his name, they found where he lived, they even found his business that had closed at the same time. They initially had some trouble convincing the authorities not only that this was really money, but that they had given it to some guy on an Internet forum called "Pirate" on the strength of him saying "sure, I'll double your bitcoins, no worries."

The SEC started investigations and depositions in late 2012. It turned out Shavers didn't have a lawyer after all, and spilled the beans on his entire operation in deposition, including admitting to destroying evidence (server logs) that had specifically been subpoenaed.[63] He did finally find a lawyer, who set up a Bitcoin donation address to fund the case since Shavers' assets had been frozen.[64]

The SEC filed a civil enforcement action against Shavers in July 2013.[65] As well as running the scheme as a Ponzi, he had taken about

150,000 BTC to day trade on Bitcoinica and Mt. Gox, from which he took about $150,000 to spend personally. His lawyer's entire defense was that bitcoins were not "money" under US law because they were not legal tender; the judge didn't buy it, and Shavers was required in September 2014 to pay back $40.7 million.[66] He was also prosecuted for criminal securities fraud for the Ponzi in November 2014,[67] pled guilty in September 2015 and was sentenced to one and a half years in jail.[68] The lawyer later maintained that the SEC only went after Shavers because they were upset they hadn't caught Bernie Madoff in time, and not at all because Shavers stole millions of dollars from people.[69]

The astounding thing is how successful such an obvious Ponzi had been. Pirateat40 held about 7% of all bitcoins in circulation at the time. Some Bitcoiners offered insurance against Bitcoin Savings & Trust failing, then put the insurance premiums into the scheme; or just didn't pay up when it went down. Others offered investment schemes that were pass-throughs to Pirateat40's scheme, while swearing up and down they weren't.

Bitcoin exchanges: keep your money in a sock under someone else's bed

"Be your own bank" is actually very hard – particularly with "no chargebacks", meaning that in the event of a theft or even a mistake you're completely out of luck – so almost everyone who uses cryptocurrencies keeps their coins on an exchange. Exchanges also let you trade between different cryptocurrencies, crypto assets and conventional currencies, and some even offer short-selling and other margin trading, which are enormously popular.

Bitcoin exchanges were started by amateur enthusiasts. Most were computer programmers whose approach to anything outside their field was "I know PHP, how hard could running an exchange be?" As Dunning and Kruger pointed out in 1999,* this approach tends not to work out so well.

In real securities trading, you can presume the exchanges themselves are not going to mess you around, and indeed that they're basically competent. You can't assume either with crypto exchanges.

---

* Wikipedia: Dunning-Kruger effect. From which another name for bitcoins, "Dunning-Krugerrands."

The gateways to the world of real money are stringently regulated – you'll need to give amazing quantities of government ID to these people you know nothing about – but inside the exchanges it's the Wild West.

Hacks, supposed hacks and exchanges just disappearing with all their customers' money remain dismally regular occurrences. As of March 2015, a full third of all Bitcoin exchanges up to then had been hacked, and nearly half had closed.[70] Since the exchanges are largely uninsured, unregulated and not required to keep reserves, depositors' money goes up in smoke.

It's not just scamminess on the part of the proprietors, but sheer jawdropping incompetence:

- Bitomat, then the third-largest exchange, were keeping the whole site's wallet file on an Amazon Web Services EC2 server in the cloud that didn't have separate backups and was set to "ephemeral," *i.e.,* it would disappear if you restarted it. Guess what happened in July 2011? Whoops.[71]
- Bitcoinica was its sixteen-year-old creator's first serious PHP project. He read up on PHP, Ruby on Rails, personal finance and startups, and wrote an exchange.[72] It collapsed in May 2012: "No database backups … Everyone had root."* The exchange's remaining funds were lost in further hacks, after the administrators turned out to be using their (leaked) Mt. Gox password as their LastPass password.[73]
- BitPay claimed to be fully insured. It suffered a "phishing" attack in December 2014, when an attacker broke into an outside partner's computer and sent an email posing as the CFO to the CEO and chairman telling them to send 5,000 BTC to the attacker. The insurer refused to compensate the company, pointing out they had taken out a policy that only covered BitPay computers and physical cash on BitPay's premises, and bitcoins didn't count as physical cash.[74]
- AllCrypt ran their exchange off a MySQL database … and were running WordPress on the same database, and their WordPress got hacked such as to allow access to the

* genjix. Comment on "[Emergency ANN] Bitcoinica site is taken offline for security investigation". Bitcointalk.org Bitcoin Forum > Bitcoin > Bitcoin Discussion, 25 May 2012. "root" is the administrator account for a Unix or Linux server.

exchange data.[75] The same thing happened to Bitcoin lending startup Loanbase.[76]

- Cryptsy appeared to collapse from a "hack" in January 2016 with much apology from the proprietor; the court-appointed receiver's report details how the proprietor ran off with all the bitcoins and moved to China to start a new exchange.[77]
- Kraken publicly blamed web content distribution network Cloudflare for its website problems.[78] Cloudflare's CEO went so far as to publicly tweet that Kraken hadn't paid its bill in months. "Let's get the facts straight. Credit card provided for payment expired. After 3 warnings you were downgraded to a free account."[79]

To be fair, conventional banks say "Yes, Mr. Smith, I'm sorry, but it seems we misplaced all your money irretrievably. Yes, yours in particular. It's gone. Forever. No, I'm sorry, but we aren't liable. Have a nice day!" all the time. *No wait, they don't do anything of the sort*. Not since regulation, insurance and central bank backing were put into place.

The rise and fall of Mt. Gox

> I'm Roger Ver, long time Bitcoin advocate and investor. Today I'm at the Mt. Gox world headquarters in Tokyo, Japan. I had a nice chat with Mt. Gox CEO, Mark Karpelès, about their current situation. He showed me multiple bank statements, as well as letters from banks and lawyers. I'm sure that all the current withdrawal problems at Mt. Gox are being caused by the traditional banking system, not because of a lack of liquidity at Mt. Gox. The traditional banking partners that Mt. Gox needs to work with are not able to keep up with the demands of the growing Bitcoin economy. The dozens of people that make up the Mt. Gox team are hard at work establishing additional banking partners, that eventually will make dealing with Mt. Gox easier for all their customers around the world. For now, I hope that everyone will continue working on Bitcoin projects that will help make the world a better place.
>
> – Roger Ver, July 2013, during the first rumblings at Mt. Gox.[80] (He later apologised.[81])

Bitcoin got its first big publicity push with the announcement of version 0.3 on technology news site Slashdot on 11 July 2010.[82] * †

At this time, Jed McCaleb was a programmer at a loose end. He had previously developed eDonkey, an early file sharing network, which was shut down in late 2005 after being sued by the Recording Industry Association of America. He then went on to develop a game, The Far Wilds, leaving that to its community in 2009.

McCaleb saw the Slashdot post, tried and failed to buy some bitcoins, and thought an exchange would be a good idea. (Early Bitcoin core developer Martti Malmi had an exchange site, but it wasn't very usable.[83]) He had run the "Magic: The Gathering Online Exchange," a trading site for an online card game, for a few months in 2007, using the domain name mtgox.com; he quickly wrote some exchange software in PHP and reused the name because his girlfriend liked it.

McCaleb announced the site on 17 July and it was an immediate hit, because people could buy and sell bitcoins via PayPal – using his personal account. Furthermore, users could keep both dollars and bitcoins there on the exchange to trade more quickly.

By late 2010, McCaleb was doing well from Mt. Gox, even though it was a completely amateur operation – he didn't even talk to a lawyer about the regulatory implications of his business until December 2010, though it was taking and holding people's actual money, uninsured, unregistered and unregulated. But he was finding it enough work to be annoying, he was tiring of attempted hacker attacks, PayPal kept cutting him off, and he worried about the amounts of money he was personally moving around.

He befriended Mark Karpelès, a French web developer. Karpelès was a massive fan of Japanese animation – his online handle MagicalTux was a reference to the anime *Sailor Moon* – so had moved to Japan in 2009. (He also left France before a 2010 fraud trial, in which he was sentenced in absentia to a year's jail.[84]) McCaleb first offered to sell Mt. Gox to Karpelès in January 2011 and finalised the sale in February, announcing it to the world in March.

---

* This section draws from *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money* by Nathaniel Popper (Harper, 2014). Mark Karpelès has disputed parts of the book's account of events: "Restoring the truth". Blog post, 29 May 2015.

† Disclosure: Mark Karpelès bought me a month of Reddit Gold (value $5) after I posted an early draft of the Bitfinex section of this book to /r/buttcoin, with the note "reddit gold for comedy gold, fair trade I'd say".

The deal used a contract they worked out between them, without either of them using a lawyer. It included terms such as:[85]

> the Seller is uncertain if mtgox.com is compliant or not with any applicable U.S. code or statute, or law of any country.
>
> The buyer agrees to indemnify Seller against any legal action that is taken against Buyer or Seller with regards to mtgox.com or anything acquired under this agreement.

It was only in April, after the handover, that Karpelès realised that 80,000 bitcoins (then worth $62,400) had already been missing when he bought Mt. Gox. McCaleb told him "maybe you don't really need to worry about it" and suggested he buy up more BTC to cover the shortfall, shuffle his internal accounts around, get an investor or just mine more himself – but didn't offer any explanation of where the coins might have got to or how.

Karpelès tried to fill the hole himself, but the price of bitcoins kept going up. By June, the missing coins were worth $800,000. Unfortunately, a nondisclosure agreement with McCaleb meant he felt he couldn't tell anyone about the massive hole in the accounts. (He didn't even reveal it to Mt. Gox's own accountant until shortly before the company went bankrupt in February 2014.)

On 18 and 19 June 2011, someone hacked into Mt. Gox. The attacker shuffled hundreds of thousands of bitcoins around – only inside the exchange, not on the public blockchain, though Mt. Gox was the main trading venue to such a degree that this momentarily drove the price of one BTC from $17 down to 1 cent. (The usual surmise is that the hacker wanted to get as many coins as possible out past Mt. Gox's $1000/day withdrawal limit.) The price oscillated between $1 and $20 for the rest of the day; this severe volatility affected other exchanges.

Around 19:15 UTC on 17 June, someone posted a complete list of 61,016 Mt. Gox usernames, email addresses and password hashes to the Bitcoin forums. Many of the passwords were "unsalted"* and so could be more easily cracked. The attacker appeared to have come in through McCaleb's administrative account, which was still active.

Karpelès went into a panic, taking much of the exchange's Bitcoin store and putting it into offline cold wallets – keys printed on paper and stored in safety deposit boxes around Tokyo – where it couldn't be hacked. Since the hacker's trading was internal to Mt. Gox,

---

* In cryptography, "salting" is used to make it even harder to work out a password from its hash. Wikipedia: Salt (cryptography).

Karpelès was able to roll back most of the transactions; eventual losses were a few thousand BTC, which the company could cover.

Roger Ver, who was also living in Japan by then, came over to help Mt. Gox (still a one-man operation at this stage) in dealing with the hack, and got to know Karpelès – Ver realised that Mt. Gox was critical at this time to Bitcoin's continued growth.

In the aftermath of the hack, Karpelès' paranoia overcame accounting considerations. He kept putting off reconciling the cold wallets with customer accounts, even as his accountant begged him to, as taking them out of cold storage would risk them being hackable. Thus, Mt. Gox was increasingly running on virtual paper money that it wasn't keeping track of.

Mt. Gox continued in this manner through 2012 and 2013. Karpelès took on staff, but remained chronically unable to manage or delegate to them. Ver sometimes had to visit the Mt. Gox offices to make sure his own important transactions went through. The company was still by far the largest Bitcoin exchange, running on the increasing popularity of the Silk Road, as it struggled to keep up with demand – 75,000 new users joined in the first ten days of April 2013.

On 14 May 2013, the US government seized $2.9 million from Mt. Gox, shutting down the main account it used to pay US customers, on the basis that Mt. Gox was transmitting money while having claimed not to be in the money transmission business. In June, the US seized another $2.1 million; Mt. Gox temporarily suspended US dollar transfers. In July, Roger Ver recorded his video assurance that all Mt. Gox's problems were with the "traditional banking system." The exchange partnered with CoinLab to serve its US customers, but this arrangement broke down soon after, Mt. Gox and CoinLab suing each other. By late 2013, customers were complaining of long delays in withdrawing US dollars, just as the Bitcoin bubble was reaching its peak.

On 7 February 2014, Mt. Gox shut down all withdrawals, of bitcoins as well as dollars. According to a leaked "Crisis Strategy Document", Mt. Gox was insolvent after losing track of 744,408 bitcoins – about $350 million at the time.[86] Karpelès had also been topping up the active online hot wallet with coins moved from the paper cold wallets and had not properly kept track.

The bitcoin leak was attributed by Karpelès to what became known as the transaction malleability bug. Bitcoin transaction IDs are not fixed – you can sometimes intercept an unprocessed transaction,

modify the transaction ID (though not the amounts or the sender or receiver addresses) and send it on, meaning it's added to the blockchain with a different transaction ID to the one it was sent with. This can lead to someone thinking a transaction they knew they sent didn't go through when it did, and sending the amount again.[87] Once this came out, other exchanges were also attacked in this manner. This news alone crashed the bitcoin price from $700 to $600.[88] (Researchers later ascertained from examining the blockchain that there was no way all of Mt. Gox's claimed 750,000 BTC loss could have been due to transaction malleability attacks.[89])

Mt. Gox had leaked bitcoins before this. In October 2011, 2,609 BTC had been lost to a programming error that sent bitcoins to a nonexistent address.[90] The exchange had been technically insolvent since about 2012, knowingly or unknowingly.[91] It remains entirely unclear how much in total was hacked and how much was just lost.

On 24 February, Mt. Gox finally closed down. $400 million in customer dollars and bitcoins had gone up in smoke.

Karpelès is still dealing with the Japanese authorities, including being arrested for embezzlement in August 2015 and held in custody for several months, with his trial starting in July 2017 (though he maintains his innocence). McCaleb went on to develop the cryptocurrencies Ripple and Stellar; his LinkedIn page details his career back to eDonkey, but chooses to omit Mt. Gox.

Drugs and the Darknet: The Silk Road

> Both Anne Frank, and Ross Ulbricht created dark markets to help people hide from violent oppressors who were trying to hurt peaceful people.
>
> – Roger Ver[92]

Anonymous or pseudonymous cryptocurrency has one obvious application: paying for things you'd rather not be caught buying or selling. Drug users take to new communication channels as soon as they're invented; the first known e-commerce was the sale of marijuana between Stanford and MIT students over email in 1971 or 1972.[93] Nakamoto noted in September 2010:[94]

> Bitcoin would be convenient for people who don't have a credit card or don't want to use the cards they have, either

> don't want the spouse to see it on the bill or don't trust giving their number to "porn guys", or afraid of recurring billing.

Ross Ulbricht grew up in Austin, Texas, born to a well-off family. He was an Eagle Scout; friends and acquaintances were widely impressed by what a polite, helpful young man he was. He studied physics and materials science at college. At Penn State, he took up with the College Libertarians group, and was an activist in support of Ron Paul's 2008 presidential bid.

He left Penn State in 2010 and posted on his LinkedIn page that he was moving from physics to "use economic theory as a means to abolish the use of coercion and aggression amongst mankind … I am creating an economic simulation to give people a first-hand experience of what it would be like to live in a world without the systemic use of force."

Tor is a protocol and network created in 2002 to let you browse the web in privacy, heavily sponsored by the US government, both for their own use and to aid dissidents in oppressive countries.[95] [96] (And, of course, it's popular with annoying Internet trolls.) You can also set up servers, only available through the Tor network, whose real location can't be traced.[97] Ulbricht realised in 2010 that Tor plus Bitcoin meant you could build a secret marketplace to deal in *anything*, licit or illicit. He adopted the name "Dread Pirate Roberts" (from the book and movie *The Princess Bride*) and launched the Silk Road in January 2011.

The Silk Road was avowedly ideological. Ulbricht was a huge fan of von Mises, Rothbard, Austrian economics and anarcho-capitalism, even hosting a libertarian book club on the Silk Road forums. He consistently put forward the Silk Road as being not just a market, but an experiment to reshape the world.

The site was a sort of eBay for illicit goods. The first sale was psychedelic mushrooms Ulbricht had grown himself, though he quickly moved to just taking a percentage on others' transactions. As well as almost any drug, you could buy steroids, forged government identification (but not *private company* identification), medical and lab supplies (build your drug lab without being flagged), hacking tutorials or drug synthesis tutorials. Sellers were pseudonymous, but relied on building up good ratings from customers. Even investigating FBI and DHS agents found it was surprisingly reliable in both delivery and quality.[98]

One thing you *couldn't* buy was child pornography – even crooks have standards, and Ulbricht forbade child pornography as not being victimless. No weapons of mass destruction, no stolen credit card numbers.

The Silk Road was publicised in March 2011 on libertarian podcast Free Talk Live (the episode that got Roger Ver into Bitcoin). By May, the site, as the one place you could actually use Bitcoin, had driven the price of 1 BTC to $10; when the site went down in mid-May for upgrading, the price of a bitcoin dropped.

The site got a massive boost in June from an article in *Gawker* describing it as an anonymous and convenient drug marketplace, providing a link to the site and directing people to Mt. Gox if they wanted to buy bitcoins to spend there.[99] Jeff Garzik, a Bitcoin core developer, explained to *Gawker* that Bitcoin wasn't "anonymous" but pseudonymous at best, given the blockchain had every transaction ever conducted. "Attempting major illicit transactions with bitcoin, given existing statistical analysis techniques deployed in the field by law enforcement, is pretty damned dumb."

Ulbricht emphasised the site's ideological mission to *Gawker:* "The state is the primary source of violence, oppression, theft and all forms of coercion. Stop funding the state with your tax dollars and direct your productive energies into the black market."

By November 2011, Ulbricht was making $30,000 a month in transaction fees. By early 2012, it was still the only functioning marketplace using bitcoins, and for some time it remained the primary driver of the Bitcoin economy.

Ulbricht had big plans for the Silk Road, as a "brand people can come to trust and rely on … Silk Road chat, Silk Road exchange, Silk Road credit union, Silk Road market, Silk Road everything!"

Around the end of 2012, Ulbricht contracted the murder of a Silk Road administrator who had been arrested, and who he believed had stolen bitcoins from him, fearing he would talk to the police and endanger the Silk Road project. When he received photos of the murdered man, he wired payment for the hit. He would order five more hits over the next few months, the last of which included killing the target's three roommates as well.

(In reality, most were faked by law enforcement agents who were out to catch "Roberts," and one by a scammer who successfully bilked Ulbricht of $500,000. His negotiations and payments to

procure murder came up in his eventual trial, and are the subject of a separate Grand Jury indictment in Maryland.)

Ulbricht had been doing all his Silk Road work from his main daily laptop. One afternoon in September 2013, he was sitting in a library, using their wi-fi to administer the site, and talking to a friend in the site's online chat. Two apparently-homeless people started arguing loudly behind him; he turned to look, and the slight young woman using the desk opposite snatched his laptop. She was a government agent. So were the homeless people. So was the friend he was chatting to.

The laptop contained the near-complete collection of smoking gun evidence on the Silk Road, gift-wrapped with a little bow on top. It included the list of Silk Road servers and the names Ulbricht had used to rent them, the Silk Road accounting spreadsheets (including the purchase of the laptop), on-site chat logs, the PHP code for the site itself, photo ID for other Silk Road administrators, all the encryption keys for the site, 144,000 bitcoins … and log.txt, Ulbricht's daily diary of his Silk Road activities: building the site, dealing with business issues, ordering hits on people.*

"I imagine that someday I may have a story written about my life, and it would be good to have a detailed account of it," he wrote in January 2012.

The DEA had started investigating the Silk Road in late 2011. They had first started looking into Ulbricht himself in July 2013, when they intercepted a package of fake passports and driver's licenses he had ordered on his own site. He had asked questions on a programming forum about using Tor via PHP as user "Altoid," a handle he had used to promote the Silk Road when he had just launched it, and had included his GMail address, which the FBI obtained a search warrant on. The Silk Road server had been traced when its real address leaked; they had found the name "Frosty" for the apparent system administrator, an alias Ulbricht had used with forum accounts linked to his GMail account and in many other places. Multiple FBI agents had befriended him on the site and even become administrators.

Everyone had assumed that "Dread Pirate Roberts" had the most painstaking operational security imaginable. It turned out Ulbricht

---

* *United States v. Ross William Ulbricht*, S1 14 Cr. 68 (KBF), Government Exhibit 241. This file is commonly referred to as "mycrimes.txt," but its actual name was "log.txt". There were also other personal journal files on the laptop.

was protected by nothing more than an impenetrable shield of narcissism, and an apparent belief that he was too smart and virtuous to be caught.

At trial, on charges of money laundering, computer hacking, conspiracy to traffic fraudulent identity documents and conspiracy to traffic narcotics, Ulbricht's defense amounted to digital identity being ambiguous, with unsubstantiated claims that someone else had set him up.

Unfortunately for Ulbricht, the prosecution had a powerful weapon on its side: overwhelming evidence. Not just from the laptop, but also from the Silk Road server, seized from its hosting company in Iceland. They also had evidence from the Bitcoin blockchain – which, of course, contained a tamper-proofed record of every transaction ever conducted on it and which addresses were involved.[100] Which is why Bitcoin is otherwise known as "prosecution futures".[101]

The defence threw various Hail Mary passes – when your client's been live-logging his criminal activities in real time, there's a limit to what sweet reason and even the most silver tongue can achieve. They admitted Ulbricht had started the Silk Road – then they claimed he then sold it to someone else, who duped him into buying it back just as the FBI was closing in; they claimed that Mark Karpelès was the real "Dread Pirate Roberts" (the DEA had looked into Karpelès in 2012, but decided it wasn't him); they attempted to call surprise last-second expert witnesses (this being slapped down in no uncertain terms by the judge, who told them to stop playing silly buggers[102]); they claimed that all the chat logs, spreadsheets and the daily diary could have somehow been planted on the laptop via BitTorrent; they claimed there was *no way* the real "Dread Pirate Roberts" would be so *stupid* as to have kept a *diary of crimes* on the laptop he *daily ran the site* from.

The charges of procuring murder were lined up to be dealt with in Maryland. However, the negotiations and payments for the hits were brought into the New York trial as evidence for the conspiracy charges, and mentioned in sentencing concerning Ulbricht's character: his freedom-loving anarcho-capitalist ideals and adherence to the non-aggression principle apparently being completely compatible with murdering all the roommates of someone who'd trespassed upon his bitcoins.

In fairness, some of the case against Ulbricht was not flawlessly kosher. The FBI may not have touched all legal bases when tracing the Silk Road server[103] (though the defence failed to challenge the evidence, despite the judge suggesting it to them repeatedly); and two of the agents on the case, Carl Mark Force IV and Shaun Bridges, turned out to have been stealing bitcoins from Ulbricht and the Silk Road and were later jailed. (They too were substantially busted by evidence straight from the blockchain.) Despite this, the evidence was sufficiently convincing that the jury took four hours, including lunch, to find Ulbricht guilty on all seven counts. He was sentenced to life imprisonment without parole.

Ulbricht's fans and family remain unshakably convinced of his innocence and virtuous character: he didn't do it, you can't prove he did it, what he did was harm reduction in the war on drugs, he was jailed just for *running a website* like anyone could, the murders didn't *actually* happen so paying to murder people and all their roommates isn't a crime and shouldn't have been mentioned in the other trial, he hasn't been *convicted* of procuring murder so it probably never happened and he's really a good guy, he was *entrapped* into paying hundreds of thousands of dollars to murder someone and all their roommates, the government ignores the Constitution, also freedom. Darknet posters had threatened the judge, Katherine B. Forrest, and posted private personal information about her in October 2014,[104] and 8chan /baphomet/ posted private information about her again between the verdict and the sentencing.[105] His mother, Lyn Ulbricht, maintains FreeRoss.org:[106]

> They used mostly digital evidence in this trial. Whether or not you believe their evidence … it significantly lowers the standard of evidence at trials. Digital material can be created out of nothing. It doesn't take much imagination to see how this is a threat to us all.

If only the prosecutors had had to hand some sort of cryptographically robust ledger of all transactions, widely distributed, with thousands of verifiable copies available.

Ulbricht's January 2016 appeal was primarily on the basis that the investigation included corrupt law enforcement agents, therefore all the evidence should be thrown out as tainted. This is not an inherently unreasonable basis for an appeal, but, well, log.txt.[107] The appeal was rejected in May 2017, the appeal judges upholding in particular the life sentence without parole on the basis that "Ulbricht was prepared, like other drug kingpins, to protect his profits by

paying large sums of money to have individuals who threatened his enterprise murdered".[108]

Silk Road imitators sprang up soon after it started, and many more after it went down. Atlantis ran from March to September 2013. Project Black Flag closed when the Silk Road was busted, stealing all its users' bitcoins. Sheep Marketplace ran from March to December 2013, closing when a vendor apparently stole $100 million in users' bitcoins, though it may have been an exit scam.[109] Silk Road 2.0 started in November 2013, lost bitcoins to the transaction malleability bug, was crippled by arrests, and the operator was finally arrested in November 2014. One undercover federal agent from The Silk Road had been invited to the administrator group of Silk Road 2.0 on its very first day of operation.[110]

Chapter 5: How Bitcoin mining centralised

The firetrap era

Bitcoin promised that anyone could mine bitcoins themselves – you could make magical Internet money out of *nothing* (but electricity and hardware). The mining difficulty is adjusted automatically every 14 days to keep the block rate at about one every ten minutes, and in the early days the difficulty was very low indeed.

Mining works by calculating one specific function over and over, as absolutely fast as possible. As far back as 2009, people had realised that graphics cards would be much more efficient[111] – a graphics processing unit (GPU) is designed to run simple calculations very fast to compute video game pixels, and the same sort of processing was able to compute Bitcoin hashes eight hundred times as fast as a general CPU. By 2010, this had become the normal mining method. These were consumer graphics cards, so mining was still accessible to anyone with a few hundred dollars, and it was quite feasible to come out ahead while the price was on the upward slope of the first bubble. (Particularly if you stole the electricity, a popular strategy.)

There are many hilarious and horrifying stories from these days. The now defunct Bitcoin Mining Accidents blog featured home miners' proud photos of their hideously bodged firetrap mining rigs.[112] This famous tale was posted in June 2011:

> I'm done with Bitcoin. It was easy money, but it wasn't worth the (literal) heat.
>
> >had 4 machines with multiple overclocked 5850s in my bedroom
>
> >fan speeds at 100%
>
> >room was warm, but tolerable
>
> >weather suddenly gets hotter one day
>
> >get severe heat stroke while I'm sleeping
>
> >get taken to the ER, get covered in bags of ice and drink tons of gatorade and water

>finally cool down after what seemed like forever

>find out I have minor permanent brain damage now because my brain was hot and swelled a lot

I wish I was joking.[113]

The sort of thing home Bitcoin miners proudly photographed to show everyone back in the day. Source: Killhamster, Buttcoin Foundation; original source unknown.

Further efficiency was possible. In late 2012, Butterfly Labs released mining hardware using a field-programmable gate array (FPGA), a silicon chip that you can program the circuit of. This was five times as efficient (in hashes per kilowatt-hour) as the graphics cards of the time. This was the start of industrial Bitcoin mining, and the decline of end-user mining.

Bitcoin mining was fully industrialised in 2013 with application-specific integrated circuits (ASICs). These were pretty much the FPGAs but manufactured as custom silicon chips, and were much more efficient again. The largest bitcoin miners now sponsor the

development of new ASICs for their own use – since 2013, you can't compete without designing your own mining chips.

You can buy ASIC mining rigs – in May 2017, the Bitmain AntMiner S9 was $1161 for 13.5 terahash/sec at 1323 watts – but they will rapidly become obsolete, and you are unlikely to be able to turn a profit unless you have very cheap or free electricity.

(I know one person who mined at home through to 2014, keeping a close eye on electricity and hardware costs, and stopped when home mining was no longer viable even with ASICs. He came out a few hundred dollars ahead and had fun with it while there was fun to be had. This is not the usual story, however.)

From 2014 onward, the mining network was based almost entirely in China, running ASICs on very cheap subsidised local electricity. (There has long been speculation that much of this is to evade currency controls – buy electricity in yuan, sell bitcoins for dollars.[114]) On 30 June 2017, the total Bitcoin network hash rate was 5.5 exahashes per second – that's 5.5×10^{18}, or three million times the hash rate in the GPU era as of early 2011.

Everything about mining is more efficient in bulk. By the end of 2016, 75% of the Bitcoin hashrate was being generated in *one building*, using 140 megawatts[115] – or over half the estimated power used by *all* of Google's data centres worldwide at the time.[116]

There have been occasional calls to re-democratise mining by changing the hash function; some other cryptocurrencies deliberately chose hash functions that wouldn't be efficient on a graphics card or an ASIC. But it is always the case that *any* function, particularly a simple one like a hash, will be more efficient on hardware specialised to just that function than on more general-purpose hardware. And we know how to program a hash function into an FPGA for mining and then base an ASIC on it. If the Bitcoin hash were to change, new ASICs would follow with only manufacturing lead time.

Abusing your hashpower for fun and profit

Bitcoin relies on distributed consensus: the blockchain is what a majority of mining capacity says it is. The consensus model relies on the fact that you can't outdo all the other miners casually – so it's not "secured by math," but secured by *economics*, balanced between multiple players.

Unfortunately, every force in the Bitcoin ecosystem tends to centralisation. Mining benefits from economies of scale, so it's progressed from mining on your PC, to graphics cards, to programmable chips (FPGAs), to ASICs.

Nakamoto's original Bitcoin white paper assumes a peer-to-peer network that anyone can join. In practice, the miners operate their own centralised communication pool, previously the Bitcoin Relay Network and now called the Fast Internet Bitcoin Relay Engine (FIBRE), as it's more efficient.

(This came close to being a single point of failure in January 2016, as the BRN was about to shut down from lack of funding, and the decentralised peer-to-peer network would not have been able to handle the traffic.)

As of March 2017, three pools controlled over 50% and six pools over 75% of the hash rate, with the largest individual pool at 21.3%.[117] There is no reason that multiple pools could not have a single owner. The largest mining pool owners already meet and operate as a cartel.[118]

If you control more than 50% of mining power, you can perform a "51% attack," which allows you to write the longest blockchain, which will then be taken by the rest of the network as canonical. You can double-spend confirmed transactions, or reject any new transaction you don't approve of. You can reject other miners' blocks. You can't spend someone else's bitcoins, but you can stop the owner from spending them.

Even if you have a bit less than 50%, you can still mount similar attacks with a better-than-average chance of success. From 25% of the hash rate upward, a selfish miner can mount 51%-style attacks and expect to turn a greater profit than they would otherwise.[119]

This isn't hypothetical – mining pool GHash.io went over 50% of the hash rate several times in June and July 2014.[120] GHash doing this was particularly problematic, as the pool had double-spent against a gambling site earlier that year. They blamed a rogue employee.[121]

Bitcoin decentralises things that should not be decentralised, then centralises them anyway but wastefully.