CRYPTO WORDS

The Gigi Anthology

A collection of Bitcoin commentary from Gigi.

Contents

Goals and Scope

Crypto Words is a journal of Bitcoin commentary, established February 13, 2019. Its purpose is to document and advance commentary and research in disciplines of particular interest to the Bitcoin community. The journal is broad in scope, publishing content from original research, essays, blog posts, and tweetstorms from a wide variety of fields, especially governance, technology, philosophy, politics, and economics, but also legal theory, history, criticism, and social or cultural analysis. Its broader mission is to capture the conversations and think pieces in the Bitcoin space for current and future researchers. *Crypto Words hopes to* continue and expand the tradition established by publications such as the *Journal of Libertarian Studies* and *Libertarian Papers*.

History

There exists a gap in Bitcoin publishing. For authors with commentary and scholarly papers on topic, the choice of publication outlets is relatively limited. The number of journals that serve as outlets for crypto research is in any event too small, as the number of crypto thinkers continues to grow with every market cycle.

This generation of Bitcoin thinkers have limited places to submit thought pieces for publication. Content is scattered across the web, and in some cases behind paywalls which prevent the free flow of information. With the advent of the Twitter and blogging, authors also now have the option of self-publishing: they post the content to their own site or some private site, link it in a blog post, or post a working paper. But this is obviously not the best way to document and publish. What is needed is a journal that takes full advantage of the possibilities of the digital age as a go to resource for think pieces in the crypto space.

Enter *Crypto Words*. Published independently, *Crypto Words* is a journal that welcomes submissions on a range of topics of interest to the crypto community. In addition to conventional research articles, we welcome review essays blog posts, tweets as well as papers in other formats, such as distinguished lectures. Finally, wherever possible, content on this site is licensed under a Creative Commons Attribution 4.0 License. Authors retain ownership without restriction of all rights under copyright in their articles. *Crypto Words* is open access, and we encourage readers to "read, download, copy, distribute, print, search, or link to the full texts of these articles…or use them for any other lawful purpose." We want our ideas read, spread, and copied.

Support Crypto Words

The posts and journals published here have been carefully curated and crafted as a true labor of love. If you've found any of this content useful here's how to show your thanks and keep the project going.

Send Bitcoin | tippin.me | Send CashApp | Send PayPal

Spread the word

Have a website or use social networking sites like Twitter, Facebook, or LinkedIn? Please consider sharing the content found on Crypto Words or linking to https://cryptowords.github.io.

Follow us on social media

We post regularly on Twitter and use it as our main form of communication. — We don't rapid fire posts but add commentary where we see fit. Posts are typically links to our content here, trolling nocoiners, sarcastic remarks, and other things regarding development of this site.

If these sorts of things interest you, follow along on:

Twitter

Subscribe to our newsletter

We publish our journal monthly and share it via Twitter and via newsletter. Consider subscribing to the newsletter. If you're not on Twitter all day, it might make sense to subscribe so you never miss a publication.

Our pledge

- We will never sell you out.
- We will never shill you shitcoins.
- We will only deliver what is promised.

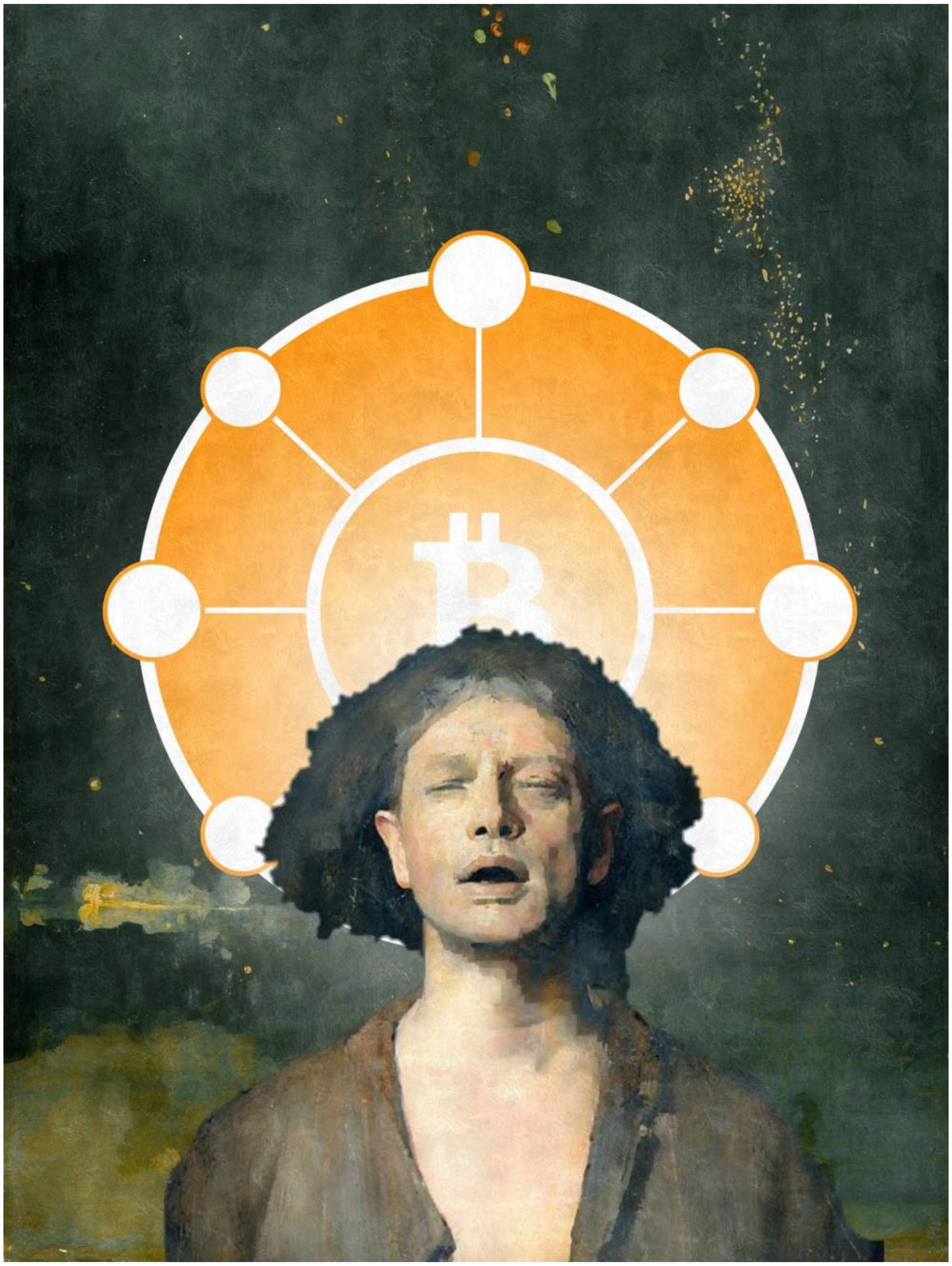
Subscribe

Tweetstorm: Circularity

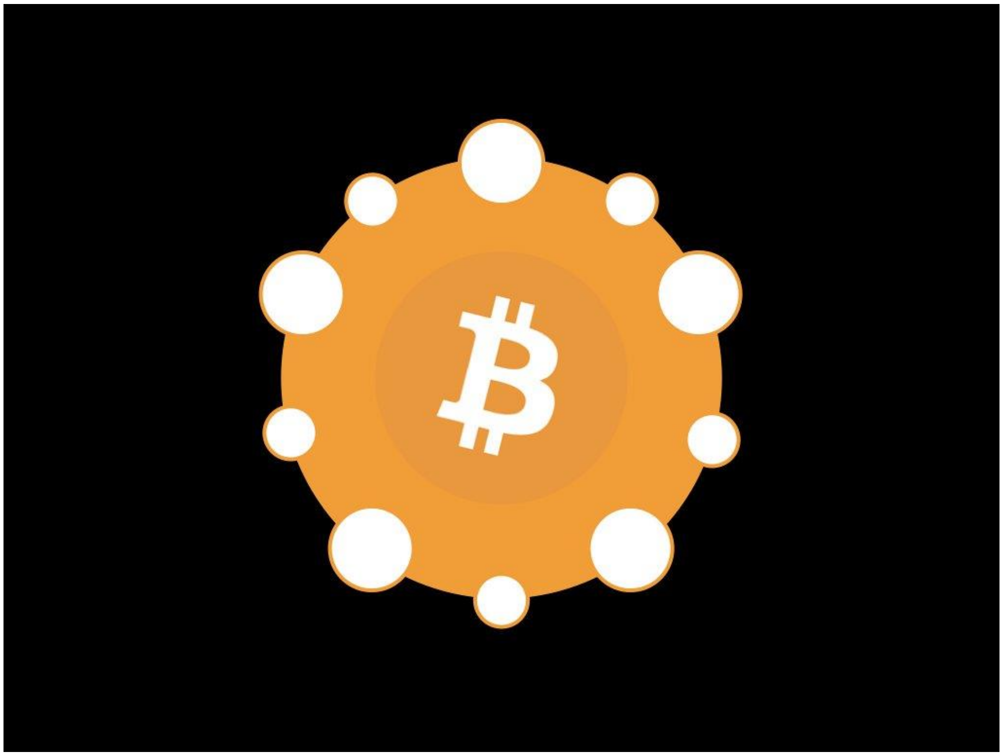
By Gigi

Posted October 30, 2019

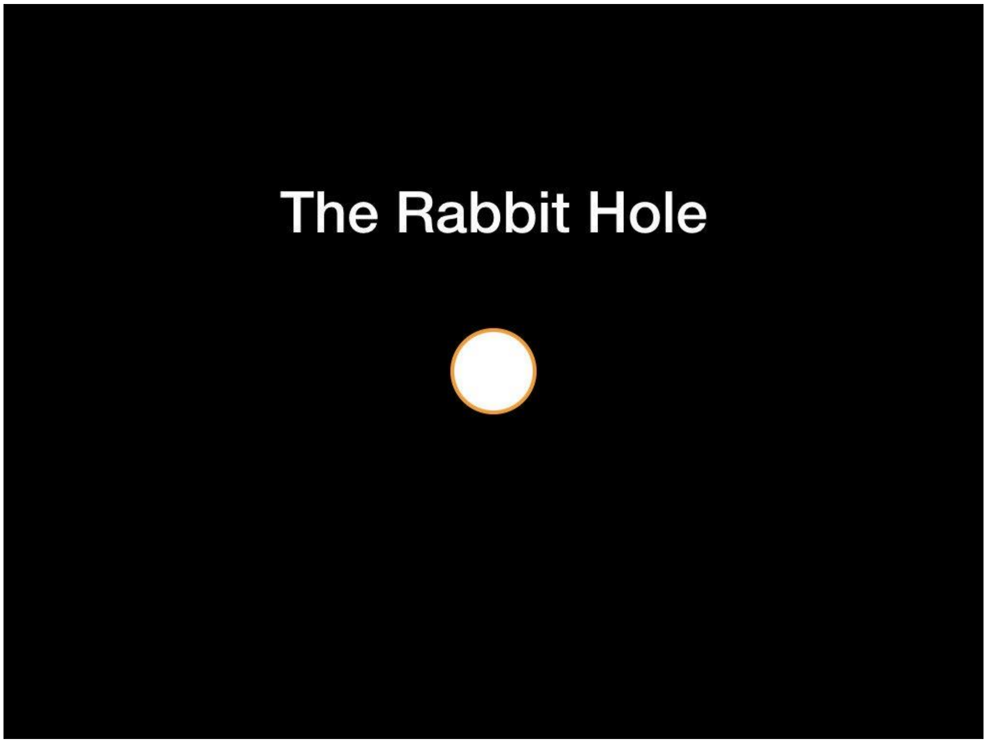
“Circularity” - A thread about Bitcoin, religion, mirrors, my rabbit hole journey, and where Bitcoin (and bitcoiners) might go in the next couple of years.



2/ I drew it in various forms, so the details (e.g. how many outside circles there are) aren't that important. The main idea is important - at least to me.

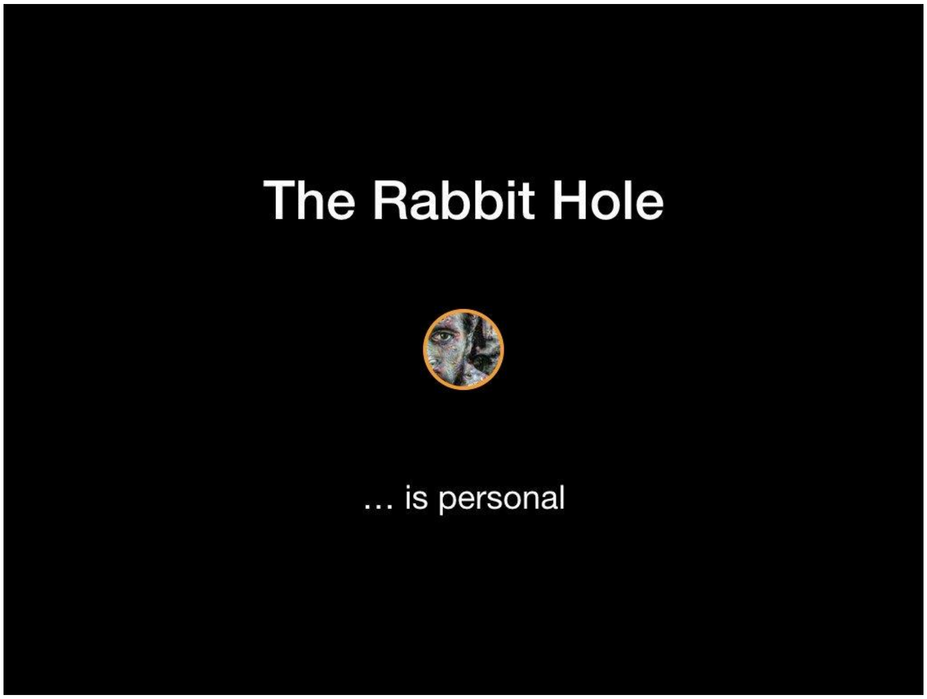


3/ The Bitcoin "rabbit hole" might look innocuous at first. After all, you're just trying to answer a very simple question: "What is Bitcoin?"



The Rabbit Hole

4/ First of all, I believe that falling down the Bitcoin rabbit hole is a deeply personal experience.

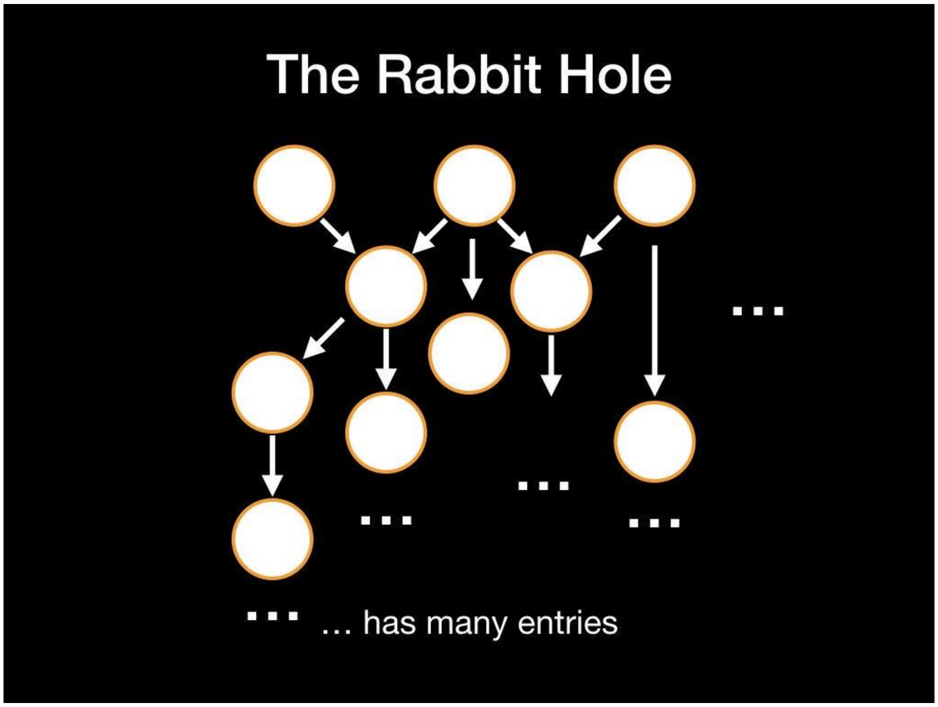


The Rabbit Hole

… is personal

5/ The rabbit hole has many entries. Your particular entry point depends on circumstance, your background, and your previous experience.

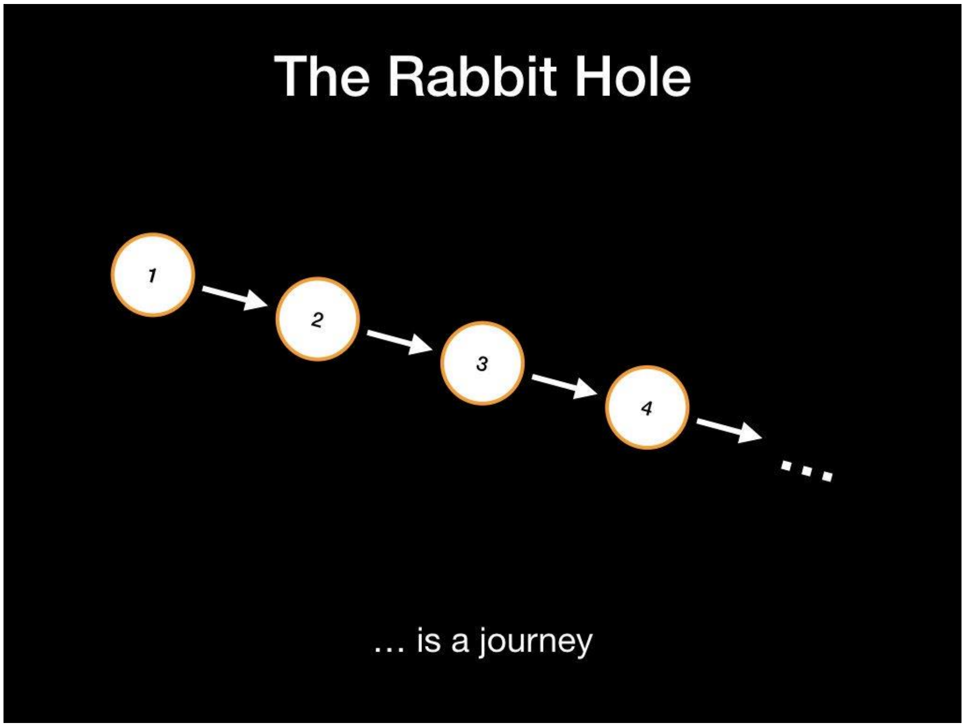
Once you are inside, however, you will stumble upon things that are far removed from your particular point of entry.



The Rabbit Hole

… has many entries

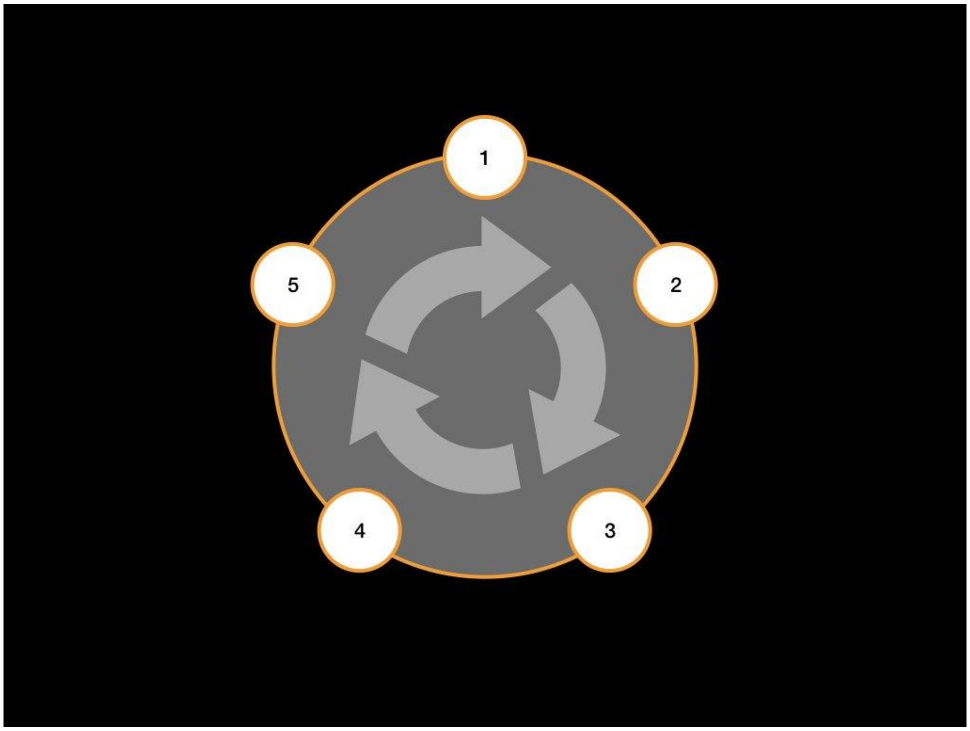
6/ Many say that the rabbit hole is bottomless, and I tend to agree. It certainly feels like a journey without end.


The Rabbit Hole

... is a journey

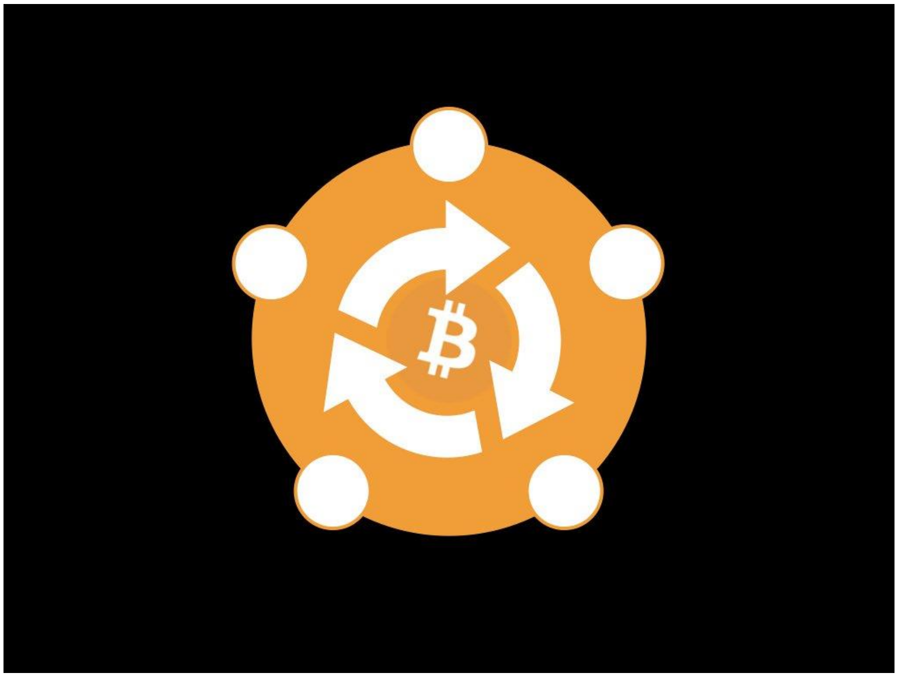
7/ However, I believe that Bitcoin - and the rabbit hole journey - is circular.

For whatever reason, this insight was of such profundity that it changed me, my view of the world, and my outlook in regards to the future.



8/ Bitcoin is profoundly circular. It is circular because it is anchored in nature, via the energy expended in proof-of-work. Some even go further and conclude the following:

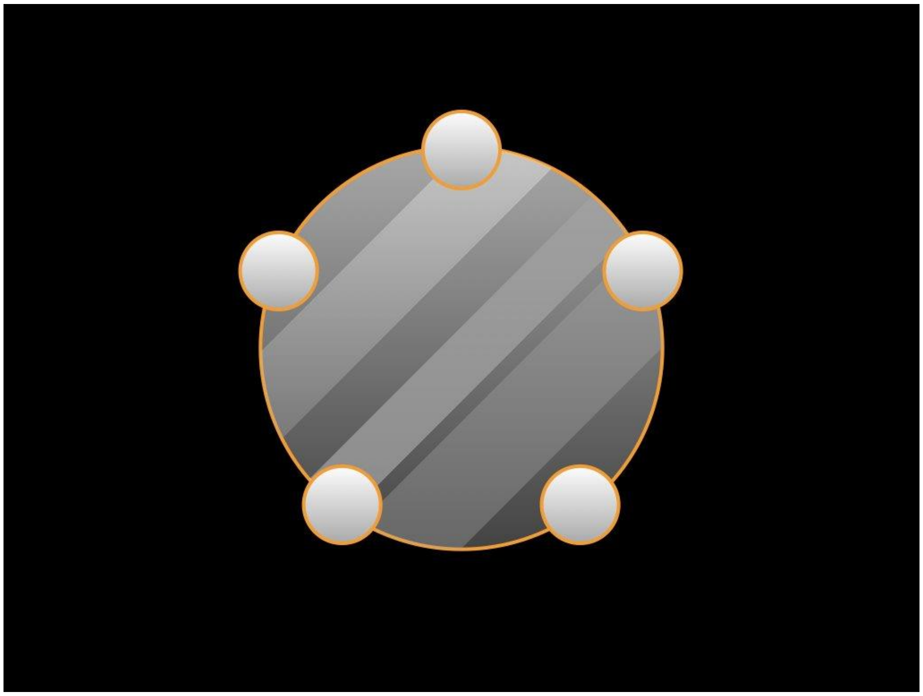
“Bitcoin is Nature” – @FriarHass



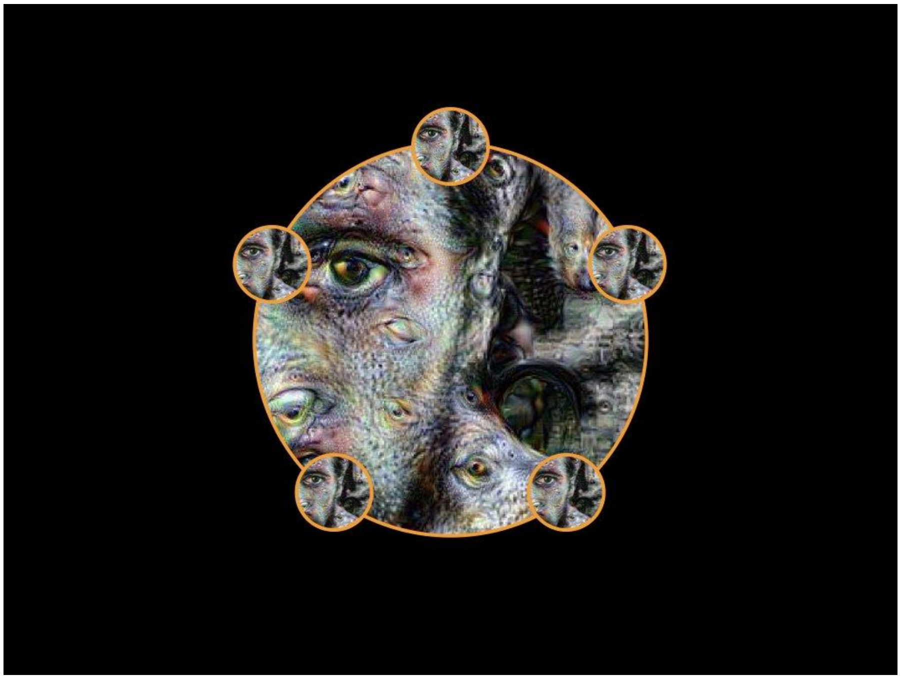
9/ You can get stuck in the smaller circles, which is partly why Bitcoin is so hard to understand. If you are a trader, you might get stuck trading. Others might get stuck on the whitepaper, or get stuck on implementation details.

10/ I sometimes drew this image as a mirror, because, well, I believe that Bitcoin is a mirror - it reflects who you are; it reflects your beliefs.

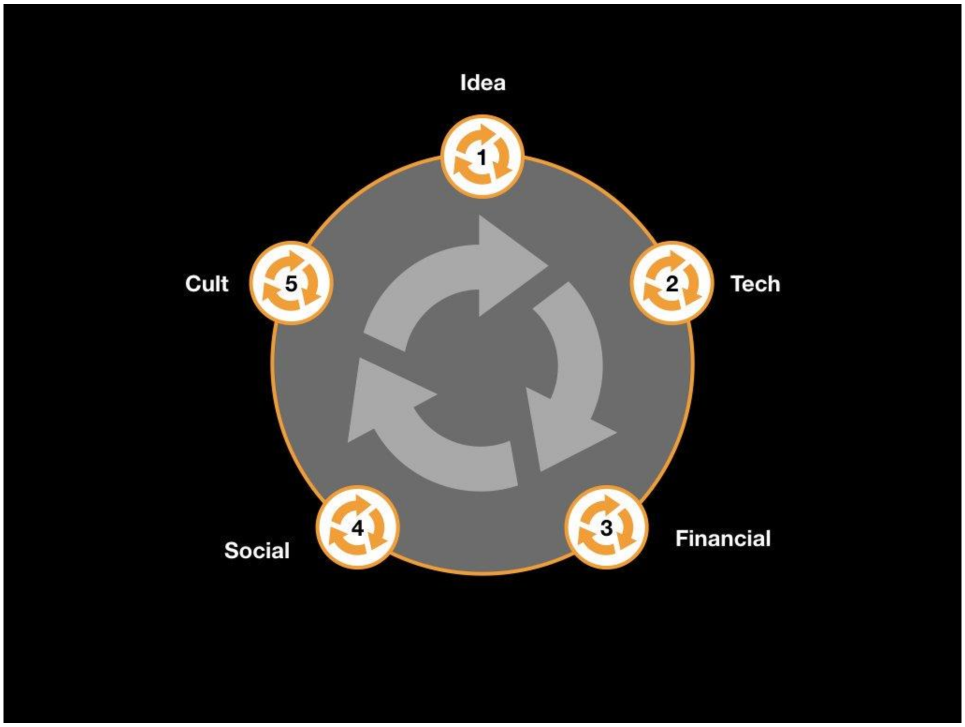
“Bitcoin is different things to different people.” “Bitcoin is whatever it needs to be…”



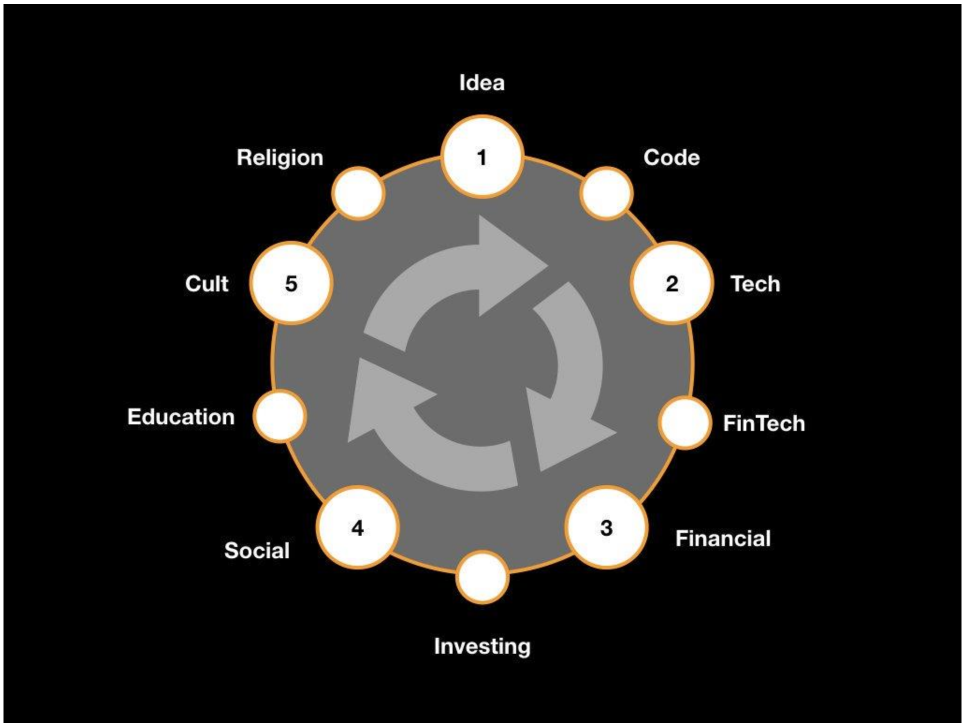
11/ “Knowledge is a mirror and for the first time in my life I was allowed to see who I was and who I might become.”



12/ The main journey, as I see it now, is roughly as follows: Idea -> Tech -> Finance -> Social -> Cult -> Idea



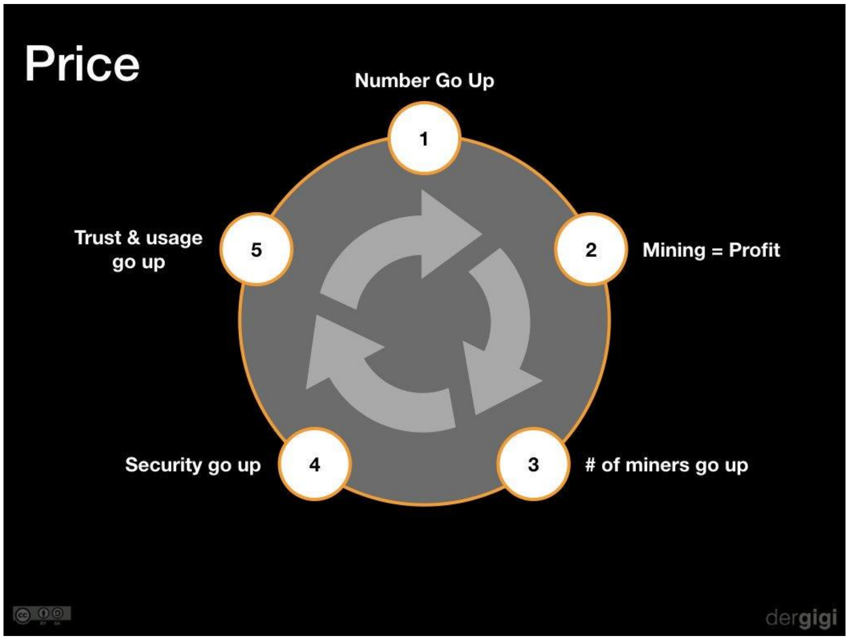
13/ There might be multiple stops in-between; that's not particularly important. What is important, is that a cult exists, and some people will take it to the next level. What is the next level? I think it's Religion.



14/ Up to now, the most powerful ideas have been religious ideas.

Bitcoin fixes this. It combines financial incentives, economic realism, mathematics, and physics with fundamentalism and religious devotion. More powerful.

“Bitcoin religion” is real. It has already started.



Price

1 Number Go Up

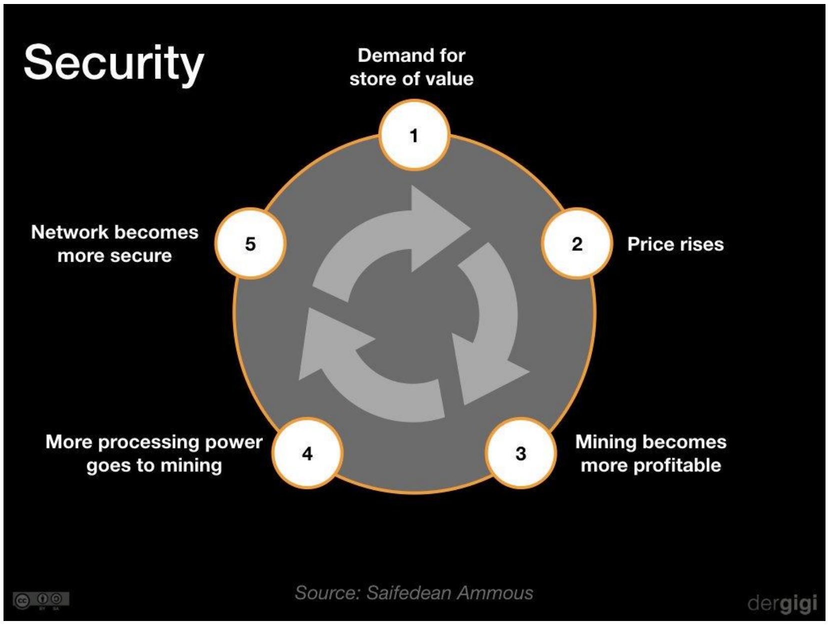
2 Mining = Profit

3 # of miners go up

4 Security go up

5 Trust & usage go up

15/ I believe that Bitcoin is the most powerful idea of our time. It is about to become one of the most powerful memes of our time. I believe that more and more people will be religious about Bitcoin, about the idea of separating money and state through absolute scarcity.



Security

1 Demand for store of value

2 Price rises

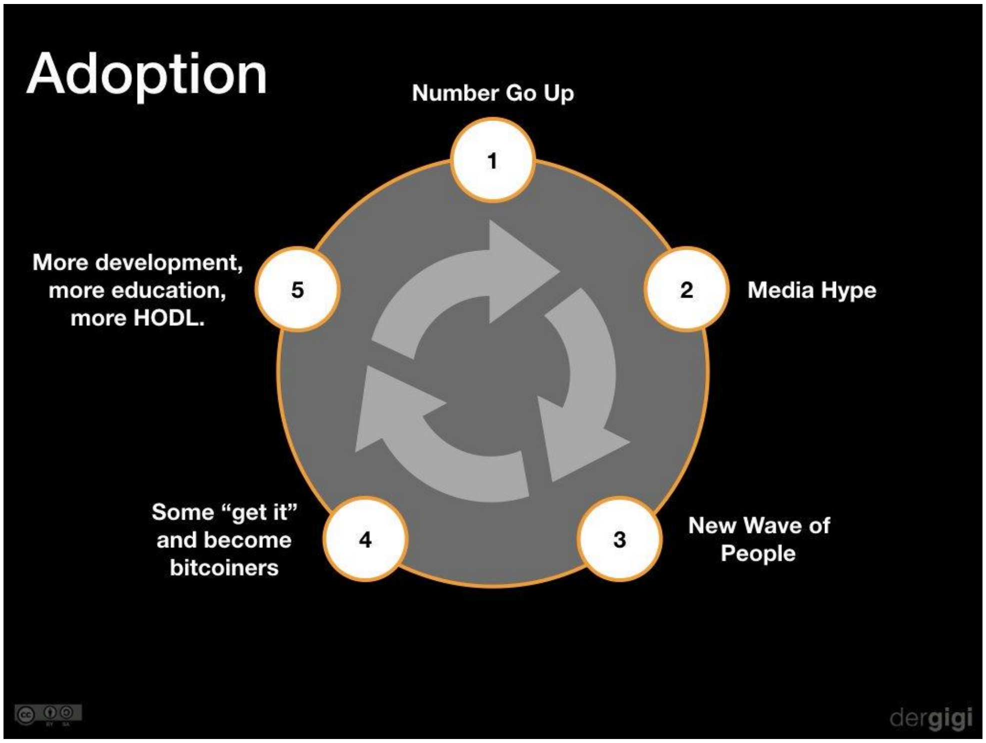
3 Mining becomes more profitable

4 More processing power goes to mining

5 Network becomes more secure

Source: Saifedean Ammous

16/ Every cycle new bitcoiners are born. Some of these bitcoiners become maximalists, and some of these maximalists will have religious devotion.


Adoption
Number Go Up
1
2
Media Hype
3
New Wave of People
4
Some “get it” and become bitcoiners
5
More development, more education, more HODL.
dergigi

17/ I’m prepared to be wrong about this.

But I ask you, dear skeptics: are you prepared to deal with tens of thousands of zealots, in case I’m right?

The Rise of the Sovereign Individual

How power is re-aligning itself in an internet-native world

By Gigi

Posted August 22, 2019

Photo cc-by Studio Incendo

Not too long ago, the internet was a fringe phenomenon. Very few people saw the benefits of a global communications network. Even fewer people had the vision and the foresight to see what it might enable. Today, most people take the internet for granted. It is simply expected to be there, like running water in your home.

Even before the internet became ubiquitous, technologists and visionaries realized the potential of this transformative technology. They realized that an undiscriminating network combined with the magical power of public-key cryptography tips the power-balance in the individual’s favor.

Eavesdropping-resistant communication which can’t be stopped is poison to authoritarian regimes, which, after all, are in the business of suppressing and controlling the flow of information. If people are still able to communicate and assemble, they can rise up and speak truth to power. We saw the liberating potential of communications technology during the Arab Spring, and we continue to see individuals rise up and fight authoritarian rule today.

What the cypherpunks understood 30 years ago is starting to play out right before our eyes: the tools of our information age have the potential to empower individuals like never before.

The Freedom to Transact

As I am writing these lines, hundreds of thousands of people are marching in the streets of Hong Kong, protesting against an extradition bill proposed by the government. As always, protests like these shine a light on the current power balance between individuals and the powers that be.

Unfortunately, the current system of surveillance, automated facial recognition, and cashless transfers enables not only a single point of failure, but also a single point of control in times of unrest. If the government doesn't like your opinion or the fact that you were part of a (peaceful) protest, a simple truth becomes apparent: your freedom of assembly was an illusion, as was your freedom to transact freely.

In a free society, these freedoms should be guaranteed. How? Well, as we have seen in the past, information technology and strong cryptography — if used carefully — *guarantee* the right to speak freely. After all, no amount of violence will ever solve a math problem. In the same vein, an information technology exists today which *guarantees* the right to transact freely: Bitcoin.

It is easy to forget that "permissionless" and "censorship-resistant" are more than mere buzzwords. Under difficult circumstances, these words become a matter of life and death. The Hong Kong protests make evident once again what privacy advocates have been preaching for years, even decades: if censorship and surveillance are built into the system, it will be used and abused by those who are in charge. And if you don't have the option to detach from your identity, free speech, free thought, and free action are impossible.

What is true for WeChat, Facebook, and Google, is also true for our current payment rails and the financial institutions of this world. No matter how noble the motivation of building central controls into communication or financial systems — power corrupts, and absolute power corrupts absolutely, as the saying goes.

"Decentralized and private payments are a necessary innovation for a digital future where we retain our civil liberties and personal freedoms." —Alex Gladstein

Strong cryptography allows us to reclaim our right to private conversations in the digital age, thanks to end-to-end encryption. The same cryptography allows us to reclaim our right to transact freely in a digital world, thanks to digital signatures, cryptographic hashes, and the global machine of truth and freedom which is Bitcoin.

The Freedom to Remain Private

In today's digital world — as Hong Kong protesters know — finding out who went to which protest is as easy as retrieving data from a database. Whether it is from people's bank accounts, WeChat, Alipay, or other virtual profiles, the convenience of the status quo inevitably leads to a system of total surveillance, and thus total control.

The solution to this conundrum is enabling privacy by default, which has been the default setting for thousands of years. Neither the internet nor Bitcoin is perfect in this regards, which is why constant vigilance and the development of privacy-enhancing technology are a necessity.

In the last couple of years, efforts to encrypt all internet traffic by default have been made. In the next couple of years, we hope to see continued efforts being made to make every bitcoin transaction even more private than they are now (which is one of the reasons why Bull Bitcoin uses Wasabi's CoinJoin by default).

As is evidenced by the long lines at Hong Kong's train ticketing machines, surveillance renders all other freedoms useless.

Source: Mary Hui

The current situation in Hong Kong paints a vivid picture of the disastrous side-effects of a cashless society. Without a way to transact privately and anonymously, people are enslaved to the masters of finance. And no amount of going digitally dark will allow you to avoid this slavery.

Arguably, things are bound to go from bad to worse. The financial elite which controls the most important good of our society — money itself — is playing god with our shared macroeconomic reality. In the last couple of decades, a concerted effort was made to attack another financial freedom: the freedom to save.

The Freedom to Save

Even without people marching in the streets, it is apparent to most that these are chaotic times. Currencies are not holding their value. A recession is looming. The most powerful men in the world are openly fighting currency wars and are bragging about it on twitter. All while the endless printing of money continues and politicians/bankers are spewing propaganda to normalize negative interest rates.

People talk about Quantitative Easing (QE) and Negative Interest Rate Policies (NIRPs) as if they were anything other than pure insanity. The first is simply printing massive amounts of money, the second is paying borrowers and stealing from savers.

Gone are the days where you would get interest from your money in the bank. In the world of NIRPs, *you have to pay the bank to hold your money*. In the same vein, gone are the days where you have to pay back your loan plus a little extra to reimburse your lender for taking on the risk. In the world of NIRPs, *you are getting paid to take out a loan*. Need some money? No worries! We are giving you the money and are paying you a little extra, for enjoying the privilege of giving you a loan!

As should be apparent for every child which is offered the choice between two marshmallows today, or one marshmallow tomorrow: the current financial world is defying common sense. I repeat: pure insanity.

More and more people realize that this insanity has to stop and decide to exit a system in which a global negative-yielding debt of $15 trillion is the new normal. The broken financial system, with its negative interest rates and "modern" monetary policies, are, in part, responsible for the rise of sovereign individuals all over the world.

Source: Rachel Cheung

People begin to realize the stupidity of this game. Putting pressure on this broken system by making a run on banks is one form of peaceful protest. Storing your value in an asset which can not be inflated, can not be confiscated, and can not be subject to the whim of politicians and bankers is another one.

“Sats are my safe haven.” —Matt Odell

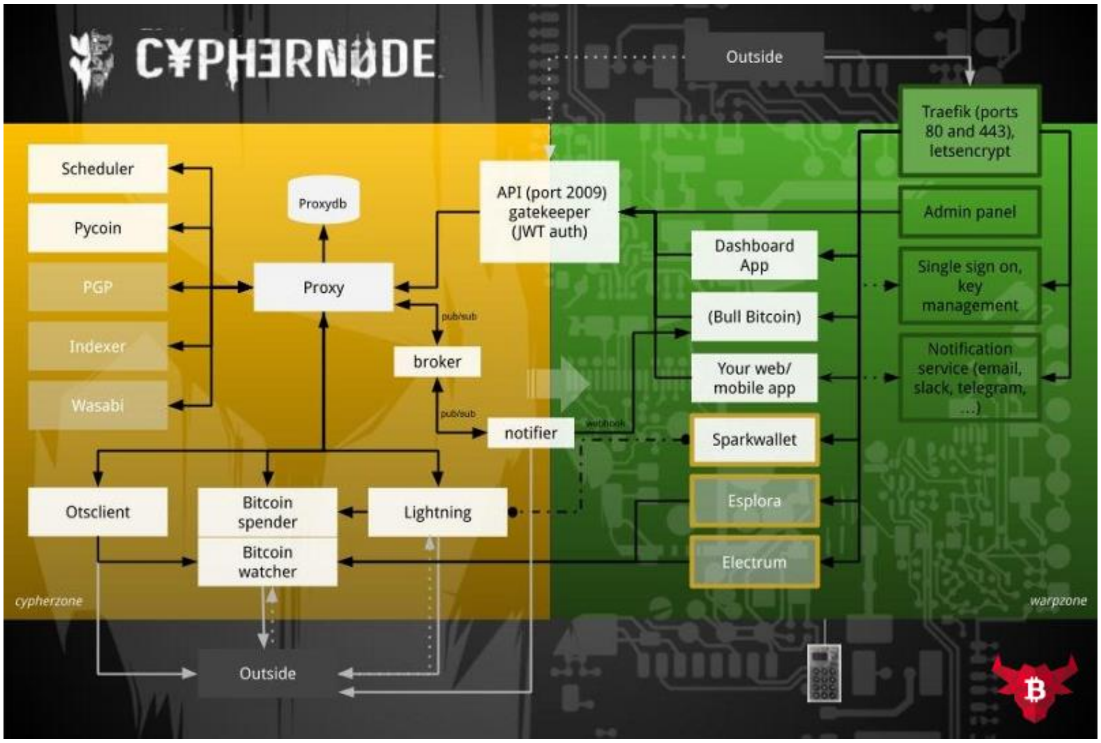
Bitcoin is quickly becoming a safe haven asset, especially for people who don’t have easy access to more “stable” currencies than their own. On a long enough time scale, bitcoin offers stability in a world of global instability. It _guarantees_the right to save: nobody will be able to take away your sats — you must give them away willingly.

Building towards a Sovereign Future

People are fed up with the tyranny of the banks, the tyranny of the state, the tyranny of Facebook, WeChat, Sina Weibo, and everything else which is “too big to fail.”

It is our collective responsibility to build a better future. A future where the freedom to transact, the freedom to remain private, and the freedom to save your wealth over time are guaranteed. In the words of the United Nations: the same rights and freedoms people have offline must also be protected online.

We want to help build a world which enables sovereign individuals to strive. A world where every individual — and every company, for that matter — can use freedom-enabling technologies, as they see fit, without asking anyone for permission. This is one of the reasons why we have released cyphernode, a suite of software and utilities to operate enterprise-grade Bitcoin services, as free software.



Cyphernode— free as in freedom.

While it is debatable whether Bitcoin can literally solve every problem of the world, it is undoubtedly a big piece of the puzzle. Technologies which empower the individual are more important than ever before. Technologies which enable you to remain private, speak and transact freely, or tip the balance of power towards the individual in another way will be invaluable for the world we are heading towards.

China is giving us a taste of what living in a dystopian surveillance state is like: you cross the street at the wrong place or the wrong time, and thanks to facial recognition, a fine is automatically deducted from your bank account while an algorithm adjusts your social credit score downwards. You pay for a bus ticket to take part in a peaceful protest, and you are at risk of being erased from the central registry, effectively erasing your ability to live a normal life as a citizen. It might happen today, it might happen tomorrow, or at any point in the future. The surveillance state does not forget.

The tools to guarantee freedom for all exist today, they are just not evenly distributed, not well understood, and not widely deployed. However, with every passing day, more and more people are realizing what kind of power is in their hands.

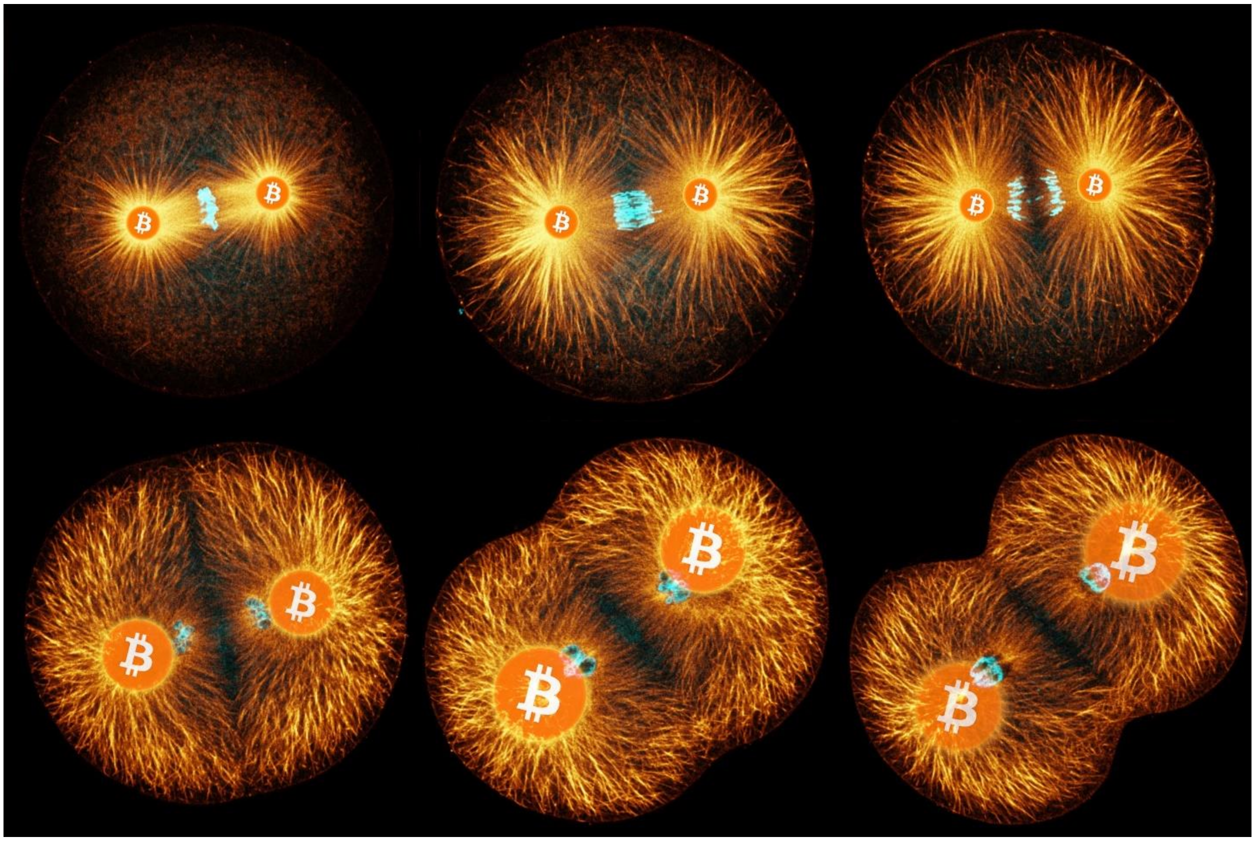
We encourage you to stay strong. We encourage you to keep on building. We encourage you to not give in to tyranny. We, and many people like us, will do our best to build towards a better future. Stay safe out there, and don’t forget to buy bitcoin.

Proof of Life

Why Bitcoin is a Living Organism

By Gigi

Posted August 7, 2019



The definition of life has been a challenge for scientists and philosophers alike. While many definitions have been put forward, what precisely differentiates the living from the non-living remains elusive. Are viruses alive? DNA molecules? Computer viruses? Biologically produced minerals?

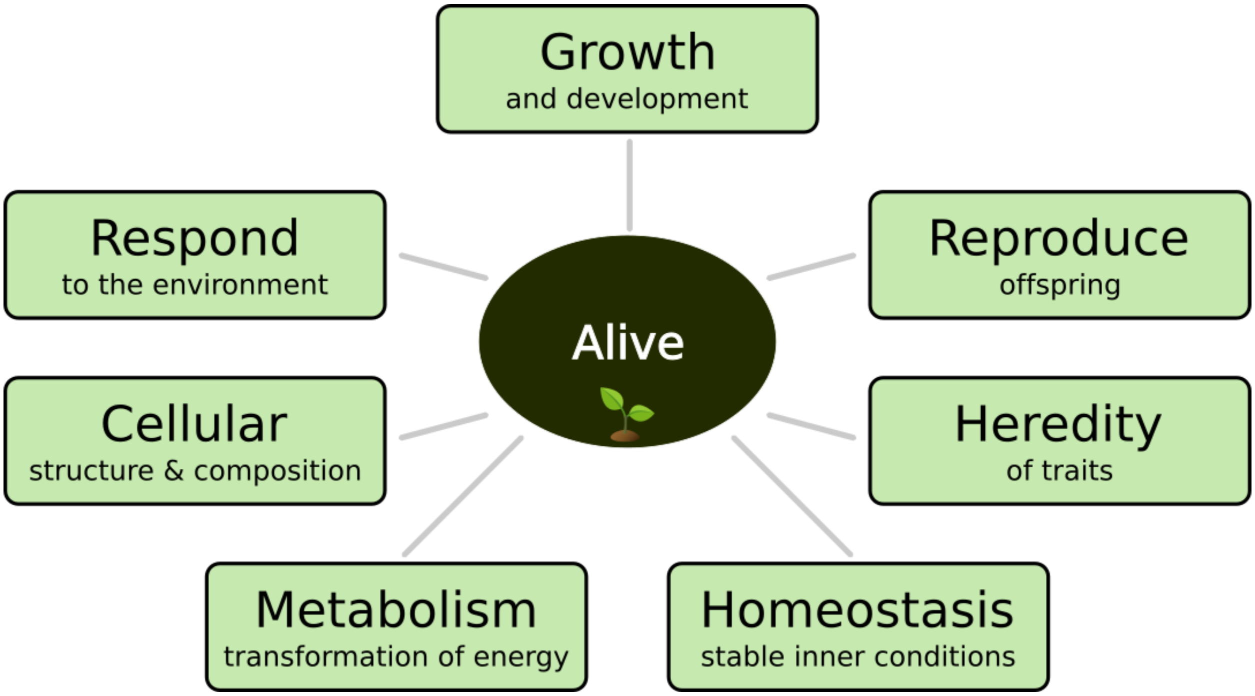
Ralph Merkle, inventor of cryptographic hashing and namesake of the Merkle tree, made the argument that Bitcoin is the first example of a new form of life. In this article series, I intend to take this claim seriously, explore it further, and see what can be gleaned from viewing Bitcoin as a living organism.

The first part will establish that Bitcoin is indeed a living organism. The second part will take a closer look at Bitcoin's various habitats, and how changes in these habitats might affect the organism. In the third part we will dissect the Bitcoin organism, trying to understand some of its parts in more detail. Finally, we will perform the thought experiment of trying to kill Bitcoin, to illustrate the remarkable resilience of this strange, decentralized organism.

What is Life?

The question of whether something is alive or not obviously hinges on one's definition of life. Life is endlessly complex, so it is no surprise that answering the question "What is Life?" leads to a multitude of answers. New-age speculations aside, it seems that life is a process, not a substance.

We can try to describe this process by looking at things which are alive, and looking at what they do: they tend to grow, reproduce, and respond. They inherit traits, are made up of smaller units (cells), and use energy to maintain their internal structure in the face of entropy.



Based on Chris Packard's Characteristics of Life, cc-by-sa 4.0

From a physics perspective, living things are thermodynamic systems: they utilize the energy-differences in their surroundings to maintain a specific molecular organization and create copies of themselves. Thermodynamically speaking, living systems are able to decrease their internal entropy at the expense of "free" energy taken in from the environment. In short, living things create order out of chaos.

Bitcoin is doing exactly that: it takes energy from the environment and puts things in order, i.e. it decreases its internal entropy. It does so by appending blocks to a well-ordered structure. Some call this structure the blockchain, others call it a distributed ledger. I will refrain from using either name, since the name of this particular structure isn't important, and doesn't help to convey a deeper truth: that this structure is just one part of a large and complex system, just like the backbone in vertebrates. It is important, no doubt. But distributed or not, a ledger on its own is as useful and as alive as a bag of bones.

To understand why Bitcoin behaves animatedly we will have to look beyond the buzzwords and ask ourselves what Bitcoin actually is, what it is made of, and what its boundaries are.

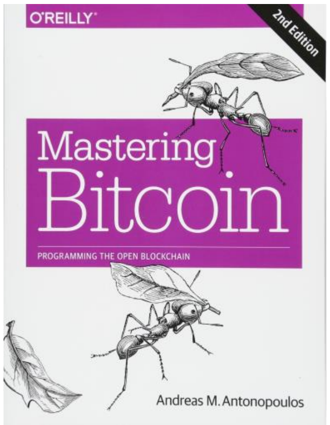
What is Bitcoin?

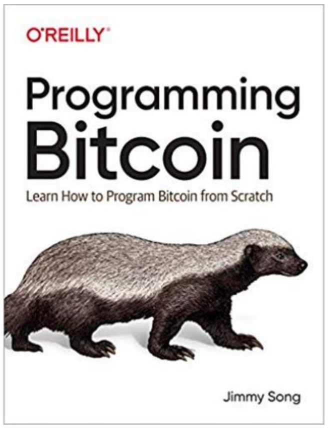
Compared to biological life, Bitcoin is quite simple. Nevertheless, finding a succinct answer to "What is Bitcoin?" is not.

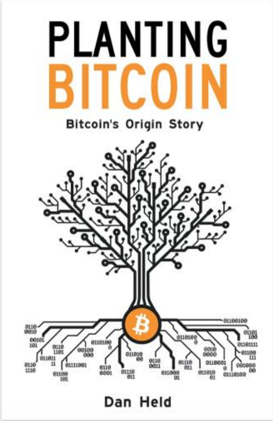
Depending on your background it might be a computer network, a financial revolution, a way to protect your wealth, a payment system, a global settlement layer, an alternative to central banking, sound money, a parallel economy, an exercise in free speech, a bubble, a pyramid scheme, a messaging system, a communications protocol, an inefficient database, internet money, or all of the above. In short, Bitcoin is different things to different people.

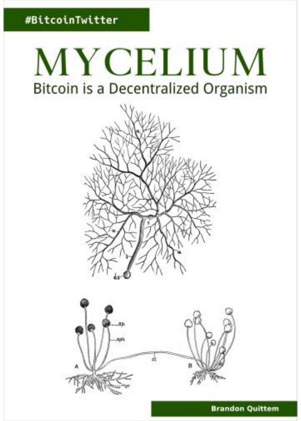
Whatever Bitcoin might be, it undoubtedly is a force to be reckoned with. It has a life of its own, and thus arguably, it is best described as a living thing.

Many people seem to have come to this conclusion independently. Bitcoin is described as an army of leaf-cutter ants in Andreas M. Antonopoulos' Mastering Bitcoin — a biological system which is working in concert without a central coordinator. The honey badger, an animal which is commonly used to refer to Bitcoin (since it doesn't care and isn't afraid of anything) is on the cover of Jimmy Song's Programming Bitcoin. Dan Held compared the invention of Bitcoin to planting a tree, examining the species (code), season (timing), soil (distribution), and gardening (community) that were essential to its success. Brandon Quittem postulates that Bitcoin is most similar to mycelium, the underground network which powers the fungi kingdom, and can thus be best understood as a decentralized organism.









The snake of regulation and central banking is biting you while you are eating it alive? *Honey badger don't care!* And just like an army of ants doesn't care if half of the workers are washed away by a flood, the Bitcoin network doesn't care if half of the nodes are offline tomorrow.

"Honey badger don't care, honey badger don't give a fuck." — Randall

Memes like these, especially if they survive and continue to be popular over a long period of time, tend to be right, conceptually. What people seem to be saying when they refer to Bitcoin as the honey badger is that, in essence, Bitcoin behaves like an animal which can't be controlled, can't be tamed, and doesn't care too much about externalities.

Which particular organism Bitcoin resembles most closely will be left as an exercise for the reader. The above examples should merely illustrate that multiple authors made the intellectual leap of classifying Bitcoin as a living organism - a leap which I believe to be fascinating, useful, and ultimately, correct.

Bitcoin is a living organism, and we should try to understand it as such if we want to live in harmony with it.

The Bitcoin Organism

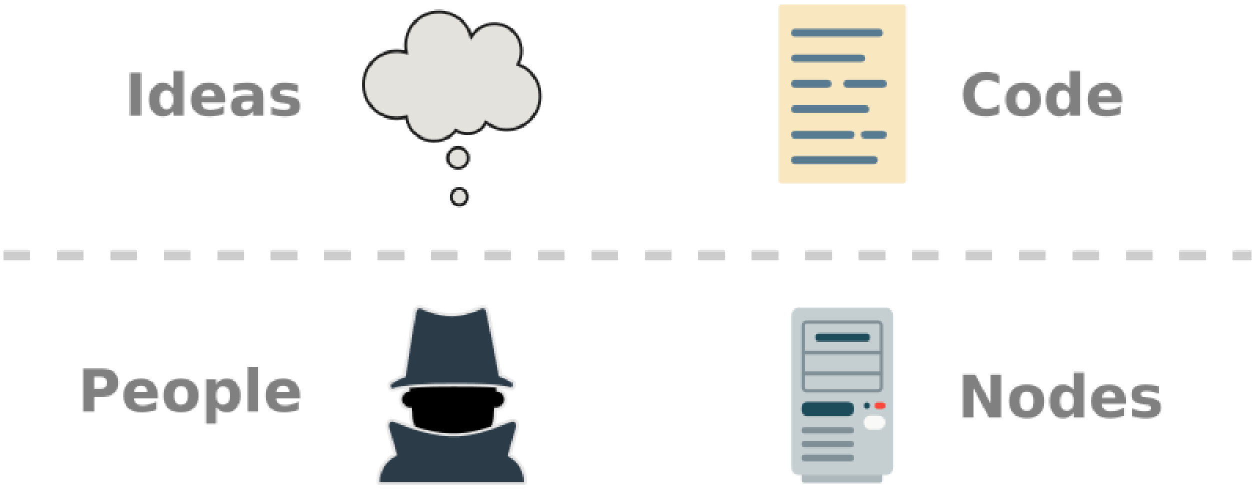
As mentioned above, Ralph Merkle was the first to point out that Bitcoin can be seen as a living entity. He remarked that Bitcoin has spawned an incredible amount of excitement in the technical community, and tried to translate this excitement into something which can be understood by everybody: a new form of life.

"Briefly, and non-technically, Bitcoin is the first example of a new form of life. It lives and breathes on the internet. It lives because it can pay people to keep it alive. It lives because it performs a useful service that people will pay it to perform. It lives because anyone, anywhere, can run a copy of its code. It lives because all the running copies are constantly talking to each other. It lives because if any one copy is corrupted it is discarded, quickly and without any fuss or muss. It lives because it is radically transparent: anyone can see its code and see exactly what it does." — Ralph Merkle

While Bitcoin is indeed radically transparent, it is not perfectly obvious where Bitcoin begins and where it ends. Like all living things, Bitcoin isn't just a uniform blob of matter. It is a dynamic, *living* thing, consisting of many different parts, all of which communicate with and influence each other, as well as other living things and the environment as a whole.

The Bitcoin organism is made up of many interlocking parts which work together to ensure the survival of the whole. As with biological organisms, as soon as one crucial part is missing, the whole organism is bound to die.

Bitcoin, however, is a strange beast. It lives across domains, with one foot in the purely informational realm (ideas and code) and one foot in the physical realm (people and nodes).



The Bitcoin organism manifests itself through the interplay of ideas, code, people, and nodes. All four of these conceptual pieces react to and influence each other in a value-generating feedback loop which keeps Bitcoin alive.

Whether people are part of the Bitcoin organism, or merely living in symbiosis with it, depends on your point of view. For now, let's take an all-encompassing view of the Bitcoin organism, including people as one part of the whole. After all, just like we can't live without a multitude of bacteria, fungi, viruses and other creepy-crawlies which make up the human microbiome, Bitcoin can't live without us: the tiny beings in meatspace which keep it alive.

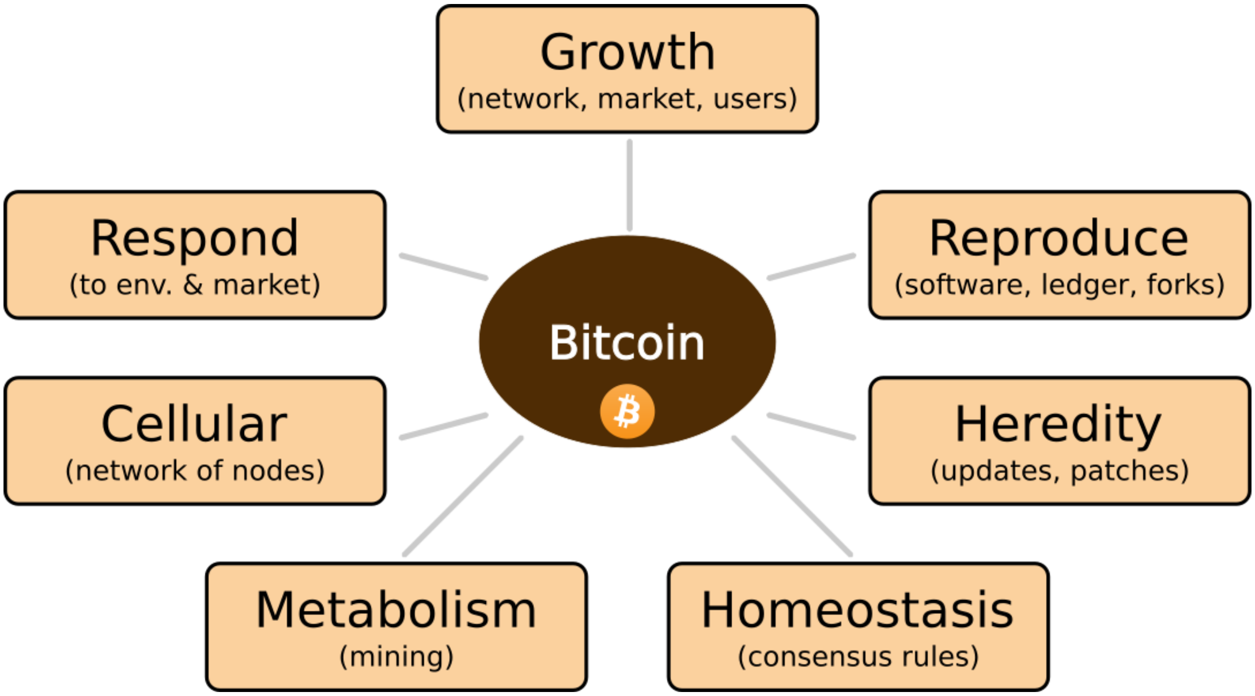
In any case, nodes and their operators are tangible things which are manifest in the physical world. Like the cells in your body, all physical components of the Bitcoin organism can and will be replaced over time. Node operators come and go, node and mining hardware is replaced periodically, and even whole mining farms go offline and are replaced by more cost-efficient facilities.

Ideas and code are more ethereal. They can’t be grasped or pointed to in the same fashion. However, Bitcoin has an *essence*, the *soul* of the organism, if you like. Note that this essence could, in theory, breathe life into a new host if the current incarnation of the organism dies. The ghost of Bitcoin is independent of its physical body, to borrow a metaphor from Shirow’s *Ghost in the Shell.*

As long as something is compatible with this essence, it will be treated as part of the whole. If something is incompatible, however, it will be rejected — just like biological organisms reject foreign objects inside their bodies.

Part of this essence is made explicit by Bitcoin’s consensus rules, other parts are repeated as mantras: “ *not your keys, not your bitcoin*” and “ *run your own node*” are gentle reminders of lessons learned, as well as shortcuts to a deeper understanding of what Bitcoin is and should be.

With a basic idea of the constituents and the extent of the Bitcoin organism in mind, let’s return to the descriptive definition of life above and see how Bitcoin maps onto each trait.



- **Growth:** Bitcoin grows in multiple ways. The network grows, the value of each bitcoin grows, the market grows, its user base grows, and the ecosystem as a whole grows as well.
- **Reproduction:** Paradoxically, Bitcoin uses replication to create absolute scarcity. It reproduces itself in multiple ways, and on multiple levels: the source code is replicated across repositories, the software is copying itself upon installation, the ledger reproduces itself on every node, blocks propagate across the network by replication, and even UTXOs can be

understood as reproductive entities, dividing and merging during the transaction process. Mutations exist on every level as well: invalid transactions, invalid blocks, hundreds of forks, and thousands of imperfect copies have been spawned by Bitcoin in the last couple of years.

- **Heredity:** Bitcoin inherits several traits from its predecessors: public-key cryptography, digital signatures, peer-to-peer networking, digital timestamping, and unforgeable costliness — just to name a few. Further, Bitcoin's open nature enables both vertical and horizontal gene transfer: some traits develop by gradual mutations of previous versions, others find their way into the codebase by incorporating ideas from other projects.
- **Homeostasis:** Above all else, Bitcoin's consensus rules are responsible for its stable inner conditions. If blocks do not adhere to the current consensus rules, they will be rejected mercilessly and quickly. The Bitcoin network will rid itself of these blocks just like we shed the dead cells of our skin.
- **Metabolism:** Mining rigs around the world keep the organism alive, erecting virtually impenetrable walls in the process. Energy is transformed into digital amber, ensuring that the shield around past transactions is growing and Bitcoin's heart keeps beating.
- **Cellular:** Multiple parts of Bitcoin are cellular: the Bitcoin network consists of nodes, each of which a self-sustaining, functional entity. The ledger itself is cellular since blocks (and transactions) are basically cells in a large, append-only spreadsheet.
- **Responsive:** Bitcoin is a highly responsive organism. It responds to changes in price, political changes, economic changes, environmental changes (e.g. if parts of the internet are cut off), technological changes (e.g. breakthroughs in chip manufacturing), and changes in our scientific understanding (e.g. breakthroughs in computer science, mathematics, or cryptography). It reacts on its own, without any person, company, or nation-state in charge.

As mentioned above, life is a process, not a substance. A delicate dance of innumerable parts, all signaling and communicating in an intricate way to self-sustain each organism, and the phenomenon which we call life as a whole.

"Life is like fire, not water; it is a process, not a pure substance. […] The simplest, but not the only, proof of life is to find something that is alive." — Christopher McKay

In the words of astrobiologist Chris McKay, the simplest proof of life is to find something that is alive. I have found Bitcoin, and as far as I can tell, it is alive — for all the reasons outlined above.

Conclusion

Bitcoin checks all the boxes when it comes to the characteristics of living things: it grows, reproduces, inherits and passes on traits, uses energy to maintain a stable inner structure, is cellular in nature, and responds to the various environments it lives in.

In the next part of this series we will take a closer look at these environments, and how Bitcoin responds to changes in them. Bitcoin lives and breathes on the internet, as Ralph Merkle beautifully said. But arguably, the internet isn't the only environment it is living in.

For now, I hope to have convinced you that Bitcoin can be seen as a living organism — alien as it may be.

Further Reading

- Bitcoin is a Decentralized Organism by Brandon Quittem
- Planting Bitcoin by Dan Held
- DAOs, Democracy and Governance by Ralph C. Merkle
- Bitcoin's Gravity by Gigi

Acknowledgements

Thanks to Dan Held,Brandon Quittem, and Raph for their feedback on earlier drafts of this article.

I hope you have enjoyed this excursion into the world of the Bitcoin organism. If you like to accelerate the growth of both Bitcoin and this article series feel free to drop me a line, some applause on medium, or even some sats via the beast which is Bitcoin. Thanks for all the encouragement, and thank you for reading.

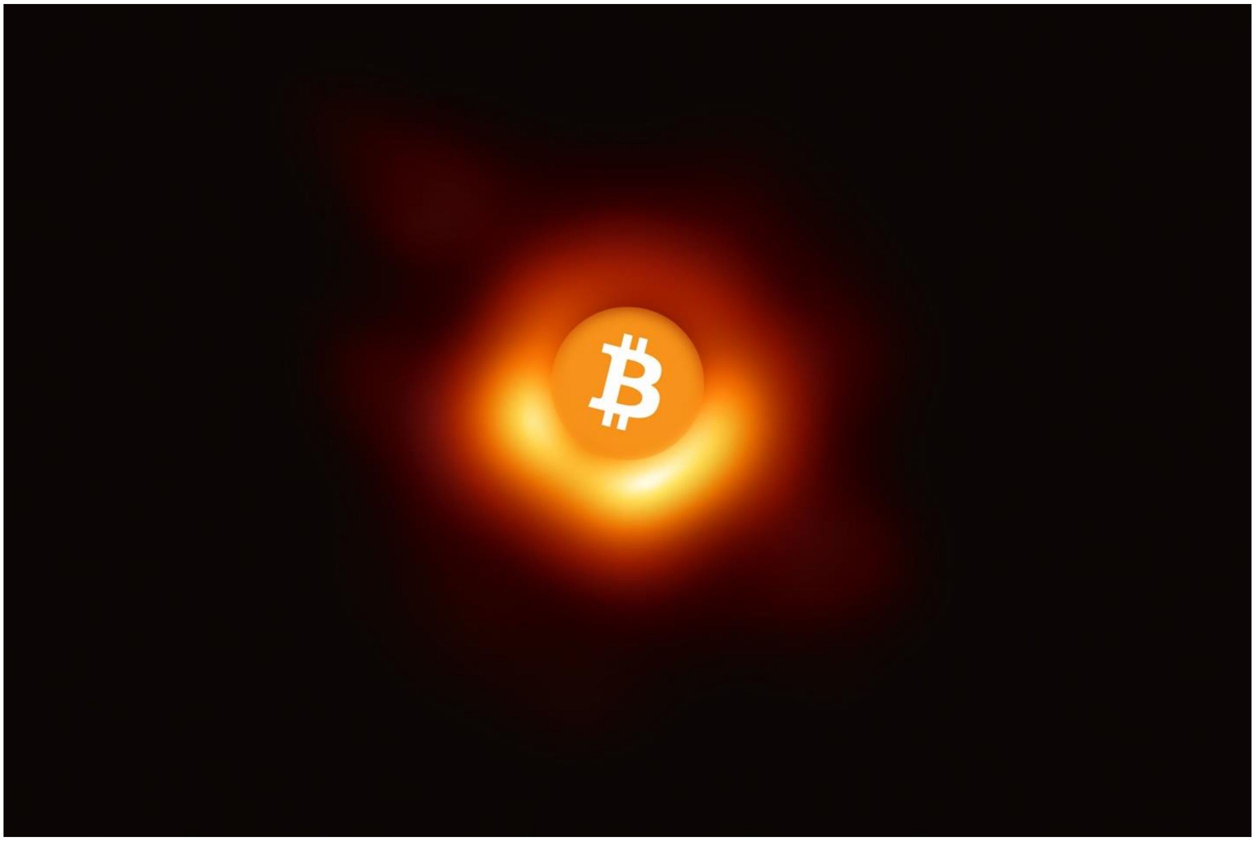
Thanks to Brandon Quittem and Dan Held.

Bitcoin's Gravity

How idea-value feedback loops are pulling people in

By Gigi

Posted May 1, 2019



Bitcoin is different things to different people. Whatever it might be to you, it is undoubtedly an opinionated and polarizing phenomenon. There are certain ideas embedded in the essence of Bitcoin, and you might be intrigued by some or all of them.

The invention of Bitcoin, and its underlying blockchain, which is so widely misunderstood, spawned many projects, networks, and communities. Some of these networks are in direct competition, which has resulted in endless conflicts and lots of debate. The root of these conflicts is ideological in nature: disagreement about how the world is and how it should be—a disagreement about ideas.

The following is an attempt to explain some of the reasons behind this polarization, explore the underlying dynamics in more detail, and illustrate why an increasing number of people seem to be gravitating towards Bitcoin.

"There are some oddities in the perspective with which we see the world. The fact that we live at the bottom of a deep gravity well, on the surface of a gas covered planet going around a nuclear fireball 90 million miles away and think this to be normal is obviously some indication of how skewed our perspective tends to be, but we have done various things over intellectual history to slowly correct some of our misapprehensions."*Douglas Adams*

Agreeing on a Set of Ideas

The goal of the Bitcoin network is to reach *consensus*, a general agreement on the state of the system. Bitcoin's breakthrough innovation was utilizing unforgeable costliness to reach global consensus without relying on a central authority.

Bitcoin can be understood as a game that anyone can join. Like all games, it can only be played if it has rules, certain ideas which are internally consistent. Otherwise, it wouldn't be a game; it would be chaos.

"Before any game can be played, the rules have to be established; before the game can be altered, the rules have to be made manifest. […] All those who know the rules, and accept them, can play the game—without fighting over the rules of the game. This makes for peace, stability, and potential prosperity—a good game. The good, however, is the enemy of the better; a more compelling game might always exist."*Maps of Meaning* Bitcoin's consensus rules are just that: a set of ideas, codified into validation rules, acted out by nodes on the network. Changing this core set of ideas is akin to changing what Bitcoin is, and the decentralized nature of the network makes changing them extremely difficult. There is no central authority to dictate changes, making unanimous adoption of a new set of ideas virtually impossible. Anyone who changes the rules, even if he thinks such a change is for the better, will start to play a different game, with only those who join him.

As Bitcoin's creator famously said: the nature of Bitcoin is such that once the first version was released, the core design was set in stone for the rest of its lifetime.

Undoubtedly, Satoshi had certain ideas in mind when he created Bitcoin. Many of these ideas are articulated in his writing, and even in the genesis block. Most importantly, however, his core ideas are codified in Bitcoin's consensus rules:

- fixed supply
- no central point of failure
- no possibility of confiscation or censorship

- everything can be validated by everyone at all times

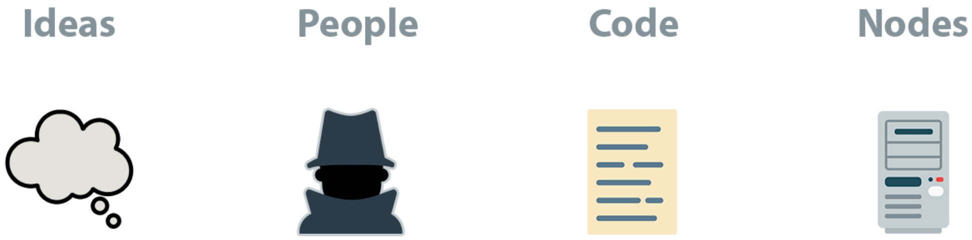
This set of ideas is embedded in the rules of the network, and you have to adopt them to participate. In essence, a network like Bitcoin encodes a social contract in its software: ideas which are shared by everyone on the network.

Spreading ideas

All great things start small, and Bitcoin was no exception. In the beginning, it was one node, one piece of software, one person, one set of ideas. On 31 October 2008, the Bitcoin whitepaper was published. Two months later, on 3 January 2009, the genesis block was mined.

"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."*Bitcoin's Genesis Block* It took only two days until a second person was intrigued enough to join the network. Hal Finney ran the software, connected to Satoshi's node, and the Bitcoin network was born. Soon, other people picked up on the idea, ran the software, and set up their nodes to join the network. The rest, as they say, is history.

The Bitcoin network is a complex piece of machinery. The constituents of the network—part technology, part biology—make it inherently difficult to describe and understand. While the following doesn't claim to be a complete description of the system by any means, I think it's helpful to focus on some constituents in more detail. In particular, I want to focus on the following four: **ideas**, **people**, **code**, and **nodes**.



Bitcoin's ingredients: two parts software, two parts hardware.

On the physical layer, the network is made up of interconnecting *nodes*. Bitcoin's consensus rules are embodied in its software, i.e. the *code* which is running on its nodes. Ultimately, *people* are choosing which software to run, a decision which is shaped by the set of *ideas* they hold.

The possibility of running self-sovereign nodes is part of the reason why Bitcoin's consensus rules are so hard to change. As mentioned above, there is no central authority, no entity to trust. Changes have to be adopted voluntarily by everyone. People are free to run any version of the software, be it out of conviction, laziness, or contempt.

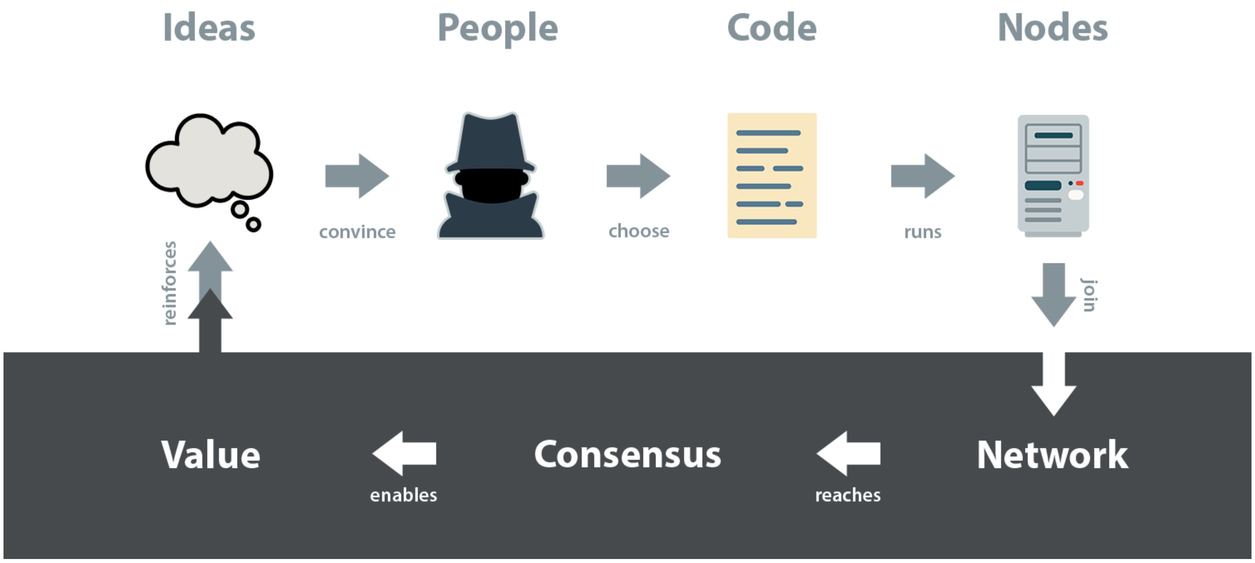
Bitcoin is a system "based on cryptographic proof instead of trust," to quote the whitepaper. The implication is that *you* are the authority and *you* have to verify everything for yourself from scratch. Out of this, consensus emerges.

"Freedom brings men rudely and directly face to face with their own personal responsibility for their own free actions."*Frank Meyer, In Defense of Freedom*
As soon as consensus is reached on the network, *value* comes into play. That bitcoins—or any monies, for that matter—have value, is in itself an idea that people need to be convinced of.

For Bitcoin, this process took almost 500 days. When the network was in its infancy, bitcoins weren't worth anything. They were mined and sent back and forth between curious cypherpunks. However, the moment Laszlo exchanged 10,000 BTC for two pizzas, Bitcoin went from zero to one. In an instant, the network became valuable in a tangible way.

Ever since this moment, the following *idea-value feedback loop* is at play:

- Bitcoin's set of **ideas**—its value proposition—is attracting people.
- Those **people** freely choose which code to run.
- The selected code runs on individual **nodes**, dictating their behavior.
- Nodes join the **network**, connecting to peers who share their ideas.
- The network reaches **consensus**, enabling agreement on who owns what.
- The **value**, in turn, is based on the set of ideas enforced by consensus rules: the embodiment of its value proposition.



Idea-value feedback loop.

This idea-value feedback loop, the re-enforcement of ideas through value creation, is the mechanism behind Bitcoin's gravity. Everything in this cycle influences everything else—whether it is software, hardware, or wetware. This loop is what ultimately captures people, and since Bitcoin's core set of ideas is virtually fixed, it has some surprising effects on the sets of ideas held by people.

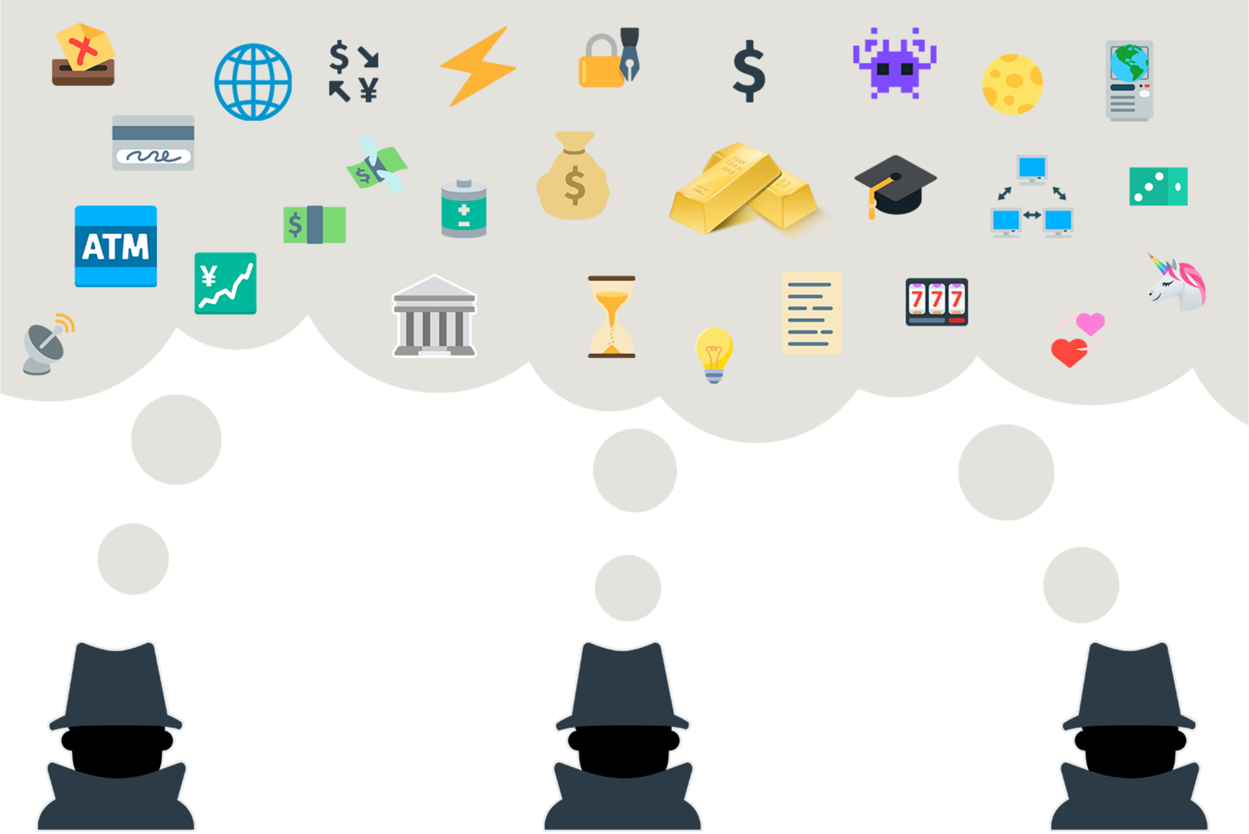
Bitcoin's Gravity Well

As we have seen above, Bitcoin is an opinionated piece of software, creating an opinionated network. The result of an opinionated network is that it attracts opinionated people.

Arguably, most early adopters of Bitcoin shared its core set of ideas. As Dan Held points out in *Planting Bitcoin*, Satoshi carefully chose the initial group of people: cryptographers and cypherpunks, who understood the technical components Bitcoin is made of.

There are many paths which might bring you close to Bitcoin's gravitational pull: you might have an interest in cryptography, information security, or financial technologies. You may hold certain political or economic beliefs. You might be a gold bug, free speech advocate, or a speculator. You may need to use Bitcoin out of necessity. Whatever the reasons for your initial contact with Bitcoin, there is a certain probability that you are pulled in. Satoshi alluded to this multi-dimensional attractiveness in one of his emails to the cryptography mailing list.

"It's very attractive to the libertarian viewpoint if we can explain it properly. I'm better with code than with words though."*Satoshi Nakamoto* One way to illustrate this is by visualizing a landscape of ideas. Since the number of all possible ideas is basically infinite, we will have to focus on a small subset. And since we are talking about Bitcoin, we will focus on the small universe of ideas spawned by asking the question of what Bitcoin is.



What is Bitcoin?

Ask three strangers what Bitcoin is, and you will probably get three very different answers. Any answer is necessarily shaped by past experience, political and economic beliefs, and an individual understanding of the world. Your personal set of ideas, your world view, defines where you are on the landscape of ideas.

The landscape has sets of ideas which clump together: *narratives*, which help to explain what Bitcoin is. One person might think of Bitcoin primarily as digital gold, focusing on the store of value aspect of Bitcoin. Another person might think of Bitcoin as a payment system, focusing on the medium of exchange aspect of Bitcoin. Yet another person might think of Bitcoin as a way to automate more complex social constructs, focusing on automation of contracts and similar ideas.

“Nobody can know everything. The complexity of society is irreducible. We cling to mental models that satisfy our thirst for understanding a given phenomenon, and stick to groups who identify with similar narratives.” *Dan*

Held These narratives, these sets of ideas, describe both what Bitcoin *actually* is—at least in part—and what people *think* it is. These narratives will necessarily evolve over time as our understanding of the system and the system itself evolves. Neither ideas, nor people, nor Bitcoin, nor the world at large are static things. Our visions of Bitcoin have changed, and will continue to do so in the future.

Whatever Bitcoin is, it acts as a *gravity well* in this universe of ideas. If your set of ideas overlaps with those embodied by Bitcoin, you are close to its gravity well and captured easily. If your set of ideas is opposed to Bitcoin's, you are far away from its gravitational pull and remain unattracted.

What is Bitcoin?

Consequently, Bitcoin is attracting opinionated people who share certain ideas and ideals. "Birds of a feather flock together," as the saying goes. In this case, many nerd-birds and cypherpunks flocked around Bitcoin early. Not particularly surprising.

What is surprising, however, is the side-effect of an opinionated network: it influences people. Since the set of ideas embodied by Bitcoin is fixed, it is the set of ideas held by *people* which has to align—not vice-versa. The last ten years have shown that Bitcoin is very effective in changing minds. So far, no single mind was particularly effective in changing it.

"So the universe is not quite as you thought it was. You'd better rearrange your beliefs, then. Because you certainly can't rearrange the universe." —Isaac Asimov To repeat an old TFTC trope: Bitcoin will change us more than we will change it, as I have learned myself.

Attraction and Repulsion

But what if your set of ideas does not overlap with Bitcoin's? What if you wish to change Bitcoin's set of ideas, not convinced of the futility of this endeavor? What if you are downright repulsed by some of its ideas?

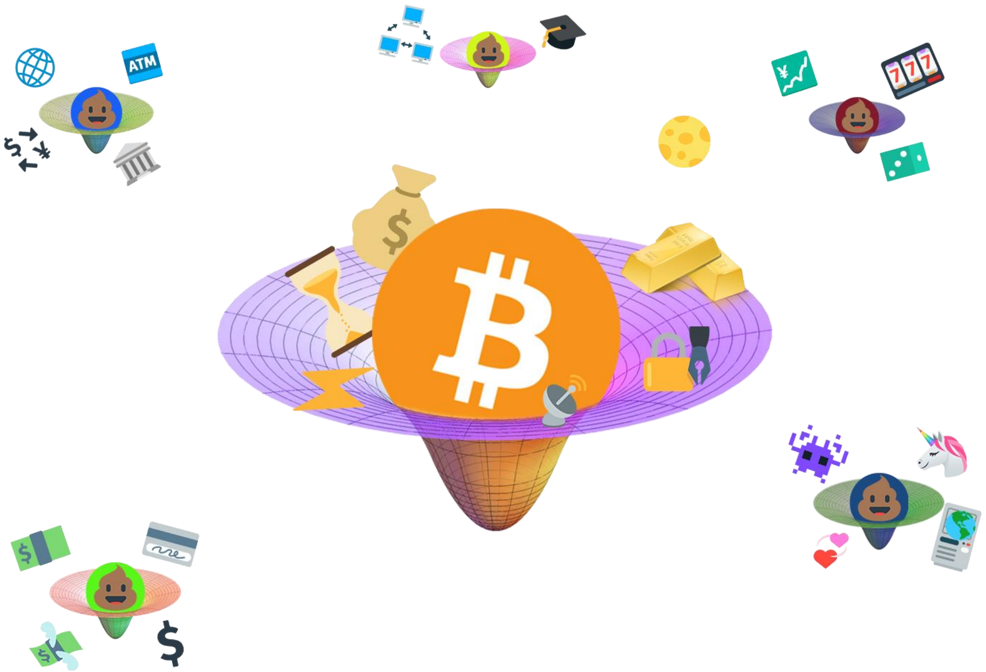
"The miracle of physics that I'm talking about here is something that was actually known since the time of Einstein's general relativity; that gravity is not always attractive. Gravity can act repulsively."*Alan Guth* If you are truly repulsed by Bitcoin's ideas, you might end up drifting away into space, joining the interstellar void where nocoiners float around.

If you want to change Bitcoin's ideas in a fundamental way, you might end up creating another gravity well. This is easily possible because of Bitcoin's openness. Its open source code, permissionless network structure, and lack of formal organization of any kind allows anyone to copy, modify, and run the code without asking for permission.

As outlined above, changing the core rules of Bitcoin results in a new game—different from the game everyone else is playing. To not play alone, you would have to convince other people to play with you. If you want to have the same number of people to play with, you will have to convince *everyone* on the network that your set of ideas is better than the one held by everyone else. And since this is mostly a financial game, strong network effects are very beneficial; it is in your best interest to convince everyone.

Failing to do so will create a competing system; either by creating a new network or by splitting off from the existing Bitcoin network. Since all new projects are inspired by Bitcoin, the set of ideas necessarily overlaps; sometimes almost exactly.

"Tracking narratives is a good way to help people understand that there are, in fact, a menu of beliefs competing for their affiliation; [...] Trying to identify where one narrative ends and another begins is a challenging task, as ideas tend to have permeable borders."*Nathaniel Whittemore* Since creating new gravity wells is (a) possible and (b) relatively easy to do (copy Bitcoin's code, change a few parameters, launch the new network with a couple of friends) there was an explosion of alternative coins in the last few years. While most of these altcoins are outright scams, some try to find a niche, attracting people who share its new or modified set of ideas.



Different ideas are captured by different gravity wells.

Being sucked into one of these gravity wells—and thus into an idea-value feedback loop—is the reason for much of the toxicity we see in Bitcoin and elsewhere. The direct link between holding beliefs (ideas) and holding assets (value) is a multiplying factor which can result in ever deeper entrenchment.

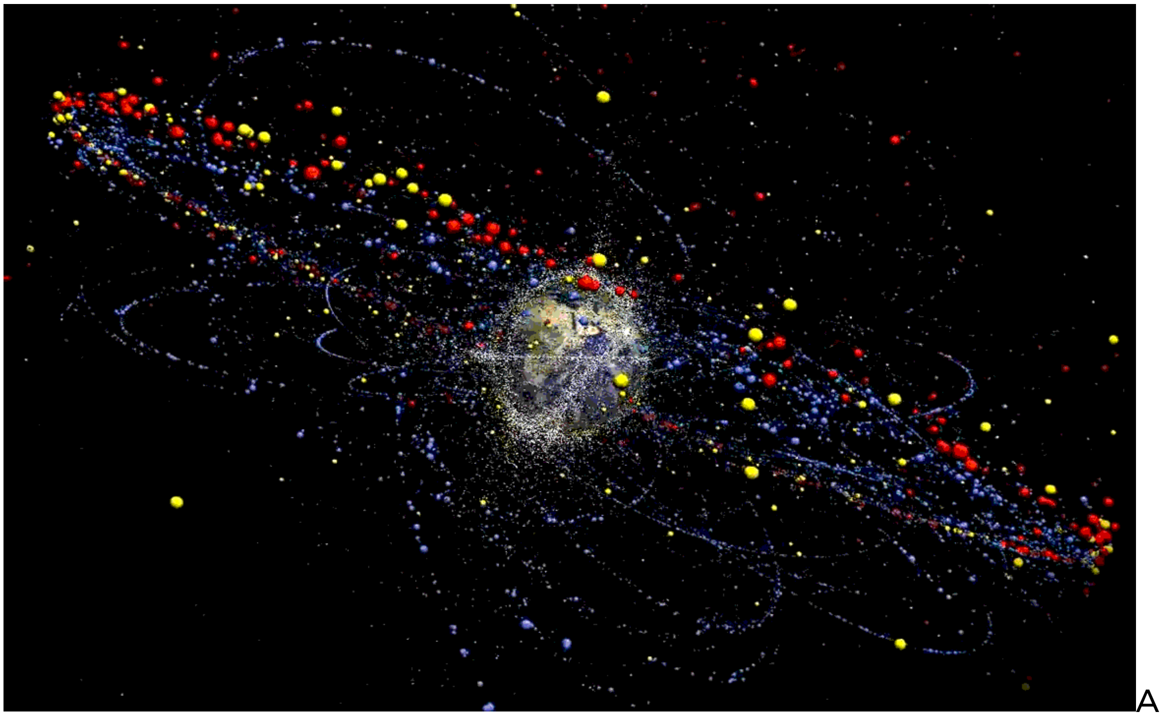
“Everyone knows nowadays that people “have complexes.” What is not so well known, though far more important theoretically, is that complexes can have us.”*Carl Jung* One could argue, as Carl Jung did in relationship to complexes, that *blockchains have people*. At the root of every gravity well is a set of ideas and a group of people which are had by them.

Once captured, a difference in technicalities can easily become a difference in ideologies—and vice versa. Giving up on ideas is difficult in any case, but if your net worth is intractably linked these ideas it becomes ever more difficult.

Orbits and Collisions

The formation of any gravity well isn't exactly a smooth ride. Just like stellar and planetary formation is violent at times—suns swallowing planets, planets bumping into each other, and moons being smashed to pieces—the formation of Bitcoin's gravity well had some violent events too.

I plan to explore some of these events in the future, but for now, let's just acknowledge that there are other projects orbiting Bitcoin and that there have been collisions in the past.



An artist's impression of Bitcoin and its satellites. Source: KQED Science

Whether all other projects will be swallowed by Bitcoin or die on their own, or whether some will find stable orbits, is yet to be seen. What can be observed today, however, is that most networks are competitive. To quote Eric Hoffer: "the gain of one in adherents is the loss of all the others."

What can also be observed, since it has happened multiple times over the last couple of years, is that projects which fail to deliver on their value proposition are quickly losing most of their adherents and also their value—the former due to disillusion, the latter due to market forces. Value, and speculation on future value, is an integral part of the idea-value feedback loop. If ideas don't materialize or fail, real (and speculative) value is lost, which is effectively killing those ideas and the networks which embody them.

However, as long as people hold different sets of ideas, and as long as a project in Bitcoin's orbit embodies this set of ideas, people will flock to it. Whether those ideas have merit will be decided by time, the open market, and ultimately, reality. Horrible ideas don't work at all, bad ideas not for long, and solutions which aren't substantially better than the status quo won't thrive in a free market.

The best ideas, however, might be discovered by the biggest networks and will be assimilated, if assimilation is possible. If Bitcoin can eat it, it will eat it.

Feeding on Ideas

As mentioned above, Bitcoin's core set of ideas is fixed from day one. However, this doesn't imply that Bitcoin can't be improved. It can and *should* be improved, but it has to be improved in ways that don't destroy the essence of Bitcoin. Such improvements are happening all the time, which is why we can send payments to script hashes, have segregated witness, and can pay small amounts quickly and cheaply on the lightning network.

The technicalities of improving Bitcoin—and the important difference between a soft and a hard fork—are well worth exploring, but are beyond the scope of this article. Without going into more details in regards to the nature of these improvements, Bitcoin undoubtedly *is* improving, and thus its feature set is changing and expanding.

In terms of gravitational pull, this means that Bitcoin is gaining mass. The set of ideas which describes Bitcoin is expanding along with its feature set, potentially capturing more people and swallowing competing projects and ideas in the process.

The idea of cheap payments, for example, has re-emerged thanks to payment channels on the lightning network. While still in its early stages, other projects built on this idea will lose their merit if the lightning network is successful on a large scale.

Privacy is another idea which is at the root of several competing projects. If future privacy enhancements in Bitcoin prove to be successful (Schnorr signatures, lightning, whirlpool, wallets supporting CoinJoins), these projects might be swallowed by Bitcoin as well.

"And the earth opened her mouth, and swallowed them up, and their houses, and all the men that appertained unto Korah, and all their goods. They, and all that appertained to them, went down alive into the pit, and the earth closed upon them: and they perished from among the congregation."*Book of Numbers* I'm not saying that *all* other projects will perish, necessarily. But networks thrive because of network effects: the winner takes most, if not all.

The Value of Conviction

Whenever people are debating ideas, tribalism is the norm, not the exception. Whether it is politics, sports, iPhone vs Android, or pineapple on pizza, people identify with the camp that is closest to their ideas and ideals.

While the validity of ideas are sometimes hard to measure, either because their consequences are very indirect (politics) or subjective and not truly consequential in the grand scheme of things (pineapple on pizza), networks like Bitcoin come with a direct measurement: value.

While this value can be distorted by both manipulation and speculation, it is a reliable and (almost) direct indicator of both conviction and validity of ideas. If more people are convinced by a network's set of ideas, more people will hold its native token as an asset. And the more those ideas align with reality, the more real-world value is generated by the network, convincing more people and deepening the convictions of those already convinced.

Bitcoin has the largest gravity for a reason: it works since day one, solves real problems for real people, generating real value. It works because its set of ideas aligns most closely with reality. It is valuable because people believe in its value proposition, and with good reason: Bitcoin is the largest, most secure, most robust network for permissionless and digital value transfer to date. And it is growing.

Whether you are already convinced by Bitcoin's ideas or are diametrically opposed to them, Bitcoin will continue to not care. Its gravitational pull will continue to increase, swallowing ideas, people, code, and nodes in the process.

Conclusion

We have seen that Bitcoin embodies a certain set of ideas in its consensus rules and overall architecture. Changing Bitcoin's core set of ideas is virtually impossible, which is why its core design is "set in stone" since day one.

The idea-value feedback loop is what creates Bitcoin's gravity. People coming close to this feedback loop have a certain probability of being captured, which forces them to align their own set of ideas with Bitcoin's or "fork off."

Understanding that any unchanging system will change its participants is helpful in understanding both attraction to and repulsion by Bitcoin. Since changing the core set of ideas is not an option, new projects embodying new sets of ideas are launched, creating new gravity wells in the process.

A different idea-value feedback loop is the basis for each gravity well. Tribalism and loss-aversion help to explain some of the toxicity between competing projects and communities, since falling into any feedback loop will taint the world view of anyone captured by it.

"For one can fall victim to possession if one does not understand betimes why one is possessed. One should ask oneself for once: Why has this idea taken possession of me? What does that mean in regard to myself?"*Carl Jung* Both the world and Bitcoin are dynamic things, making any set of ideas we currently hold insufficient for a permanent, complete view of either. Bitcoin can and does change, even if its essence is virtually unchangeable. No matter our individual beliefs, we must not get too attached to any narrative, or to any set of ideas.

Bitcoin's dominance is no accident. Its set of ideas managed to convince the largest group of people, generating the most value in turn. However, exploring other ideas can be a good and healthy thing, if pursued genuinely. Time and the free market will decide which ideas align with reality. Bad ideas will vanish, and good ideas will be absorbed.

In a world where people hold a combination of ideas and valuable assets, a feedback loop which links and reinforces both is a powerful force of attraction. Whether you just started to feel Bitcoin's gentle pull or you've been a hodlonaut in close orbit, Bitcoin's gravity will continue to increase. I am convinced of that idea, and I hope to have planted a seed of conviction in you as well.

Further Reading

- Unpacking Bitcoin's Social Contract by Hasu
- We can't all be friends: crypto and the psychology of mass movements by Tony Sheng
- Visions of Bitcoin - How major Bitcoin narratives changed over time by Hasu and Nic Carter
- The Many Faces of Bitcoin by Murad Mahmudov and Adam Taché
- Bitcoin: Past and Future by Murad Mahmudov and Adam Taché
- Crypto-incrementalism vs Crypto-anarchy by Tony Sheng
- Bitcoin Culture Wars by Brandon Quittem
- Schrödinger's Securities by Nathaniel Whittemore
- Market Narratives Are Marketing by Nathaniel Whittemore
- Quantum Narratives by Dan Held

Acknowledgments

- Thanks to Hasu, whose incredible feedback helped to shape large parts of this article. His writing on Unpacking Bitcoin's Social Contract was my inspiration for writing about Bitcoin's gravity.
- Thanks to Nathaniel Whittemore for his writings on narratives and feedback on earlier drafts of this article.
- Thanks to Ben Prentice for proofreading the final draft.
- Graphics based on the fxemoji set cc-by Sabrina Smelko
- Dedicated to the bravest space cat of them all (* April 2017, † April 2019).

Translations

- Turkish translation by @deniz_zgur

Philosophical Teachings of Bitcoin

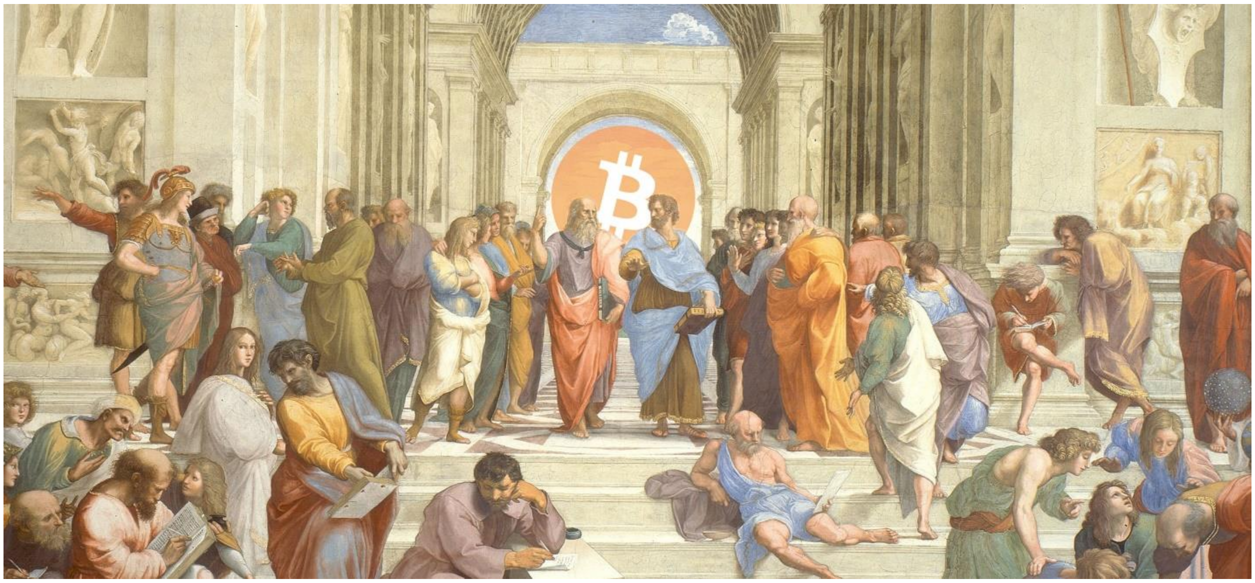
What I've Learned From Bitcoin: Part I

By Gigi

Posted December 21, 2018

This is part 1 of a 3 part series

- Part 1 Philosophical Teachings of Bitcoin
- Part 2 Economic Teachings of Bitcoin
- Part 3 Technological Teachings of Bitcoin



Some questions have easy answers. "What have you learned from Bitcoin?" isn't one of them. After trying to answer this question in a short tweet, and failing miserably, I realized that the amount of things I've learned is far too numerous to answer quickly, if at all. I also realized that any set of answers to this question will be different for everyone—a reflection of the very personal journey through the wonderful world of crypto. Hence, the subtitle of this series is *What I've Learned From Bitcoin*, with which I want to acknowledge the inherent personal bias of answering a question like this.

I tried to group the teachings of Bitcoin by topics, resulting in three parts:

- **I: Philosophical Teachings of Bitcoin**
- II:Economic Teachings of Bitcoin

- III:Technological Teachings of Bitcoin

As hinted above, attempting to answer this question fully is a fool's errand, thus my answers will always be incomplete. I would like to lessen this shortcoming by inviting you, dear reader, to share your own answers to this question:

Bitcoin is indeed a game disguised. It is akin to a trapdoor, a gateway to a different world. A world much stranger than I would have ever imagined it to be. A world which takes your assumptions and shatters them into a thousand tiny pieces, again and again. Stick around for long enough, and Bitcoin will completely change your worldview.

"After this, there is no turning back. You take the blue pill—the story ends, you wake up in your bed and believe whatever you want to believe. You take the red pill—you stay in Wonderland, and I show you how deep the rabbit hole goes."

— Morpheus

***

Lesson 1: Immutability and change

Bitcoin is inherently hard to describe. It is a *new thing*, and any attempt to draw a comparison to previous concepts—be it by calling it digital gold or the internet of money—is bound to fall short of the whole. Whatever your favorite analogy might be, two aspects of Bitcoin are absolutely essential: decentralization and immutability.

One way to think about Bitcoin is as an automated social contract. The software is just one piece of the puzzle, and hoping to change Bitcoin by changing the software is an exercise in futility. One would have to convince the rest of the network to adopt the changes, which is more a psychological effort than a software engineering one.

The following might sound absurd at first, like so many other things in this space, but I believe that it is profoundly true nonetheless: You won't change Bitcoin, but Bitcoin will change you.

"Bitcoin will change us more than we will change it." —Marty Bent

It took me a long time to realize the profundity of this. Since Bitcoin is just software and all of it is open-source, you can simply change things at will, right? Wrong. *Very* wrong. Unsurprisingly, Bitcoin's creator knew this all too well.

The nature of Bitcoin is such that once version 0.1 was released, the core design was set in stone for the rest of its lifetime. — Satoshi Nakamoto

Many people have attempted to change Bitcoin's nature. So far all of them have failed. While there is an endless sea of forks and altcoins, the Bitcoin network still does its thing, just as it did when the first node went online. The altcoins won't matter in the long run. The forks will eventually starve to death. Bitcoin is what matters. As long as our fundamental understanding of mathematics and/or physics doesn't change, the Bitcoin honeybadger will continue to not care.

"Bitcoin is the first example of a new form of life. It lives and breathes on the internet. It lives because it can pay people to keep it alive. […] It can't be changed. It can't be argued with. It can't be tampered with. It can't be corrupted. It can't be stopped. […] If nuclear war destroyed half of our planet, it would continue to live, uncorrupted. " —Ralph Merkle

The heartbeat of the Bitcoin network will outlast all of ours.

Realizing the above changed me way more than the past blocks of the Bitcoin blockchain ever will. It changed my time preference, my understanding of economics, my political views, and so much more. Hell, it is even changing people's diets. If all of this sounds crazy to you, you're in good company. All of this is crazy, and yet it is happening.

Bitcoin taught me that it won't change. I will.

Lesson 2: The scarcity of scarcity

In general, the advance of technology seems to make things more abundant. More and more people are able to enjoy what previously have been luxurious goods. Soon, we will all live like kings. Most of us already do. As Peter Diamandis wrote in Abundance: “Technology is a resource-liberating mechanism. It can make the once scarce the now abundant.”

Bitcoin, an advanced technology in itself, breaks this trend and creates a new commodity which is truly scarce. Some even argue that it is one of the scarcest things in the universe. The supply can’t be inflated, no matter how much effort one chooses to expend towards creating more.

“Only two things are genuinely scarce: time and bitcoin.” —Saifedean Ammous

Paradoxically, it does so by a mechanism of copying. Transactions are broadcast, blocks are propagated, the distributed ledger is—well, you guessed it—distributed. All of these are just fancy words for copying. Heck, Bitcoin even copies itself onto as many computers as it can, by incentivizing individual people to run full nodes and mine new blocks.

All of this duplication wonderfully works together in a concerted effort to produce scarcity.

In a time of abundance, Bitcoin taught me what real scarcity is.

Lesson 3: An immaculate conception

Everyone loves a good origin story. The origin story of Bitcoin is a fascinating one, and the details of it are more important than one might think at first. Who is Satoshi Nakamoto? Was he one person or a group of people? Was he a she? Time-traveling alien, or advanced AI? Outlandish theories aside, we will probably never know. And this is important.

Satoshi chose to be anonymous. He planted the seed of Bitcoin. He stuck around for long enough to make sure the network won’t die in its infancy. And then he vanished.

What might look like a weird anonymity stunt is actually crucial for a truly decentralized system. No centralized control. No centralized authority. No inventor. No-one to prosecute, torture, blackmail, or extort. An immaculate conception of technology.

“One of the greatest things that Satoshi did was disappear.” —Jimmy Song

Since the birth of Bitcoin, thousands of other cryptocurrencies were created. None of these clones share its origin story. If you want to supersede Bitcoin, you will have to transcend its origin story. In a war of ideas, narratives dictate survival.

"Gold was first fashioned into jewelry and used for barter over 7,000 years ago. Gold's captivating gleam led to it being considered a gift from the gods." — Gold: The Extraordinary Metal

Like gold in ancient times, Bitcoin might be considered a gift from the gods. Unlike gold, Bitcoins origins are all too human. And this time, we know who the gods of development and maintenance are: people all over the world, anonymous or not.

Bitcoin taught me that narratives are important.

Lesson 4: The problem of identity

Nic Carter, in an homage to Thomas Nagel's treatment of the same question in regards to a bat, wrote an excellent piece which discusses the following question: What is it like to be a bitcoin? He brilliantly shows that open, public blockchains in general, and Bitcoin in particular, suffer from the same conundrum as the Ship of Theseus: which Bitcoin is the real Bitcoin?

"Consider just how little persistence Bitcoin's components have. The entire codebase has been reworked, altered, and expanded such that it barely resembles its original version. […] The registry of who owns what, the ledger itself, is virtually the only persistent trait of the network […] To be considered truly leaderless, you must surrender the easy solution of having an entity that can designate one chain as the legitimate one." —Nic Carter

It seems like the advancement of technology keeps forcing us to take these philosophical questions seriously. Sooner or later, self-driving cars will be faced with real-world versions of the trolley problem, forcing them to make ethical decisions about whose lives do matter and whose do not.

Cryptocurrencies, especially since the first contentious hard-fork, force us to think about and agree upon the metaphysics of identity. Interestingly, the two biggest examples we have so far have lead to two different answers. On August 1, 2017, Bitcoin split into two camps. The market decided that the unaltered chain is the original Bitcoin. One year earlier, on October 25, 2016, Ethereum split into two camps. The market decided that the *altered* chain is the original Ethereum.

If properly decentralized, the questions posed by the *Ship of Theseus* will have to be answered in perpetuity for as long as these networks of value-transfer exist.

Bitcoin taught me that decentralization contradicts identity.

Lesson 5: Replication and locality

Quantum mechanics aside, locality is a non-issue in the physical world. The question *"Where is X?"* can be answered in a meaningful way, no matter if X is a person or an object. In the digital world, the question of *where* is already a tricky one, but not impossible to answer. Where are your emails, really? A bad answer would be "the cloud", which is just someone else's computer. Still, if you wanted to track down every storage device which has your emails on it you could, in theory, locate them.

With bitcoin, the question of "where" is *really* tricky. Where, exactly, are your bitcoins?

"I opened my eyes, looked around, and asked the inevitable, the traditional, the lamentably hackneyed postoperative question: 'Where am I?'" —Daniel Dennett

The problem is twofold: First, the distributed ledger is distributed by full replication, meaning the ledger is everywhere. Second, there are no bitcoins. Not only physically, but *technically*.

Bitcoin keeps track of a set of unspent transaction outputs, without ever having to refer to an entity which represents a bitcoin. The existence of a bitcoin is inferred by looking at the set of unspent transaction outputs and calling every entry with a 100 million base units a bitcoin.

"Where is it, at this moment, in transit? [...] First, there are no bitcoins. There just aren't. They don't exist. There are ledger entries in a ledger that's shared [...] They don't exist in any physical location. The ledger exists in every physical location, essentially. Geography doesn't make sense here—it is not going to help you figuring out your policy here." —Peter Van Valkenburgh

So, what do you actually own when you say *"I have a bitcoin"* if there are no bitcoins? Well, remember all these strange words which you were forced to write down by the wallet you used? Turns out these magic words are what you own: a magic spell which can be used to add some entries to the public ledger—the keys to "move" some bitcoins. This is why, for all intents and purposes, your private keys *are* your bitcoins. If you think I'm making all of this up feel free to send me your private keys.

Bitcoin taught me that locality is a tricky business.

Lesson 6: The power of free speech

Bitcoin is an idea. An idea which, in its current form, is the manifestation of a machinery purely powered by text. Every aspect of Bitcoin is text: The whitepaper is text. The software which is run by its nodes is text. The ledger is text. Transactions are text. Public and private keys are text. Every aspect of Bitcoin is text, and thus equivalent to speech.

“Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.” — First Amendment to the United States Constitution

Although the final battle of the Crypto Wars has not been fought yet, it will be very difficult to criminalize an idea, let alone an idea which is based on the exchange of text messages. Every time a government tries to outlaw text or speech, we slip down a path of absurdity which inevitably leads to abominations like illegal numbers and illegal primes.

As long as there is a part of the world where speech is free as in *freedom*, Bitcoin is unstoppable.

“There is no point in any Bitcoin transaction that Bitcoin ceases to be *text._It is _all text*, all the time. […] Bitcoin is **text.**Bitcoin is **speech.**It cannot be regulated in a free country like the USA with guaranteed inalienable rights and a First Amendment that explicitly excludes the act of publishing from government oversight.” —Beautyon

Bitcoin taught me that in a free society, free speech and free software are unstoppable.

Lesson 7: The limits of knowledge

Getting into Bitcoin is a humbling experience. I thought that I knew things. I thought that I was educated. I thought that I knew my computer science, at the very least. I studied it for years, so I have to know everything about digital signatures, hashes, encryption, operational security, and networks, right?

Wrong.

Learning all the fundamentals which make Bitcoin work is hard. Understanding all of them deeply is borderline impossible.

“No one has found the bottom of the Bitcoin rabbit hole.” —Jameson Lopp

My list of books to read keeps expanding way quicker than I could possibly read them. The list of papers and articles to read is virtually endless. There are more podcasts on all of these topics than I could ever listen to. It truly is humbling. Further, Bitcoin is evolving and it’s almost impossible to stay up-to-date with the accelerating rate of innovation. The dust of the first layer hasn’t even settled yet, and people have already built the second layer and are working on the third.

Bitcoin taught me that I know very little about almost anything. It taught me that this rabbit hole is bottomless.

Conclusion

Bitcoin is a child of the internet. Even though it requires computers to function efficiently, computer science is not sufficient to understand it. The implications of this new technology are far-reaching. Bitcoin is not only borderless but also boundaryless in respect to academic disciplines.

In this first part of the *Teachings of Bitcoin* I tried to outline some of the philosophical implications of this fascinating machinery. In part two I will try to discuss what Bitcoin taught me about economics. Part three will conclude this series to show what I, a technologist, have learned from the tech perspective by stumbling into Bitcoin.

As mentioned above, I think that any answer to the question *“What have you learned from Bitcoin?”* will always be incomplete. The systems are too dynamic, the space moving too fast, and the topics too numerous. Politics, game theory, monetary history, network theory, finance, cryptography, information theory, censorship, law and regulation, human organization, psychology—all these and more are areas of expertise which might help to grasp what Bitcoin is.

What have you learned from Bitcoin?

Further Reading

- *The Bitcoin Standard: The Decentralized Alternative to Central Banking* by Saifedean Ammous
- *Abundance: The Future Is Better Than You Think* by Peter Diamandis
- *The Mind’s I* by Daniel Dennett and Douglas Hofstadter
- *Money, blockchains, and social scalability* by Nick Szabo
- *Bitcoin’s Existential Crisis*, originally published as *What is it like to be a Bitcoin*? by Nic Carter
- *Unpacking Bitcoin’s Social Contract: A framework for skeptics* by Hasu
- *Why America Can’t Regulate Bitcoin* by Beautyon
- *Why Bitcoin is different* by Jimmy Song
- Peter Van Valkenburg on *Preserving the Freedom to Innovate with Public Blockchains* hosted by Peter McCormack

Acknowledgments

- Thanks to Arjun Balaji for the tweet which motivated me to write this.
- Thanks to Marty Bent for providing endless food for thought and entertainment. If you are not subscribed to Marty’s Ƀent and Tales From The Crypt, you are missing out.

- Thanks to Michael Goldstein and Pierre Rochard for curating and providing the greatest Bitcoin literature via the Nakamoto Institute and the Noded Podcast which influenced my philosophical views on Bitcoin substantially.
- Thanks to Peter McCormack for his honest tweets and the What Bitcoin Did podcast, which keeps providing great insights from many areas of the space.
- Thanks to Jannik for providing feedback to early drafts of this article.
- And finally, thanks to all the bitcoin maximalists, shitcoin minimalists, shills, bots, and shitposters which reside in the beautiful garden that is crypto twitter.

Translations

- Spanish translation by Camilo Jorajuría de León @CamiloJdL

Economic Teachings of Bitcoin

What I've Learned From Bitcoin: Part II

Gigi

Posted January 11, 2019

This is part 2 of a 3 part series

- Part 1 Philosophical Teachings of Bitcoin
- Part 2 Economic Teachings of Bitcoin
- Part 3 Technological Teachings of Bitcoin

Money doesn't grow on trees. To believe that it does is foolish, and our parents make sure that we know about that by repeating this saying like a mantra. We are encouraged to use money wisely, to not spend it frivolously, and to save it in good times to help us through the bad. Money, after all, does not grow on trees.

Bitcoin taught me more about money than I ever thought I would need to know. Through it, I was forced to explore the history of money, banking, various schools of economic thought, and many other things. The quest to understand Bitcoin lead me down a plethora of paths, some of which I try to explore in this series. This is the second of three parts:

- I:Philosophical Teachings of Bitcoin
- **II: Economic Teachings of Bitcoin**
- III:Technological Teachings of Bitcoin

In Part I of this series, some of the philosophical questions Bitcoin touches on were discussed. Part II will take a closer look at money and economics. Again, I will only be able to scratch the surface. Bitcoin is not only ambitious, but also broad and deep in scope, making it impossible to cover all relevant topics in a single essay, article, or book. I am starting to doubt if it is even possible at all.

Bitcoin is a child of many disciplines. Being a new form of money, learning about economics is paramount in understanding it. Dealing with the nature of human action and the interactions of economic agents, economics is probably one of the largest and fuzziest pieces of the Bitcoin puzzle.

Blind monks examining Bitcoin

Like the first part, this essay is an exploration of the various things I have learned from Bitcoin. And just like the first part, it is a personal reflection of my journey down the rabbit hole. Having no background in economics, I am definitely out of my comfort zone and aware that any understanding I might have is incomplete. Like blind monks examining an elephant, everyone who approaches this novel technology does so from a different angle and will come to different conclusions. Blindfolded as I am, I will try to outline what I have learned, even at the risk of making a fool out of myself. After all, I am still trying to answer the question:

“What have you learned from Bitcoin?”

After seven lessons examined through the lens of philosophy, let’s use the lens of economics to look at seven more. I hope that you will find the world of Bitcoin as educational, fascinating and entertaining as I did and still do. In any case, hop on and enjoy the ride. Economy class is all I can offer this time. Final destination: sound money.

Find lessons 1-7 here.

Lesson 8: Financial Ignorance

One of the most surprising things, to me, was the amount of finance, economics, and psychology required to get a grasp of what at first glance seems to be a purely *technical* system—a computer network. To paraphrase a little guy with hairy feet: “It’s a dangerous business, Frodo, stepping into Bitcoin. You read the whitepaper, and if you don’t keep your feet, there’s no knowing where you might be swept off to.”

To understand a new monetary system, you have to get acquainted with the old one. I began to realize very soon that the amount of financial education I enjoyed in the educational system was essentially *zero*.

Like a five-year-old, I began to ask myself a lot of questions: How does the banking system work? How does the stock market work? What is fiat money? What is *regular* money? Why is there so much debt? How much money is actually printed, and who decides that?

After a mild panic about the sheer scope of my ignorance, I found reassurance in realizing that I was in good company.

“Isn’t it ironic that Bitcoin has taught me more about money than all these years I’ve spent working for financial institutions? …including starting my career at a central bank”—aarontaycc “I’ve learned more about finance, economics, technology, cryptography, human psychology, politics, game theory, legislation, and myself in the last three months of crypto than the last three and a half years of college”—bitcoindunny

These are just two of the many confessions all over twitter. Bitcoin, as was explored in part one, is a living thing. Mises argued that economics also is a living thing. And as we all know from personal experience, living things are inherently difficult to understand.

“A scientific system is but one station in an endlessly progressing search for knowledge. It is necessarily affected by the insufficiency inherent in every human effort. But to acknowledge these facts does not mean that present-day economics is backward. It merely means that economics is a living thing—and to live implies both imperfection and change.” —Ludwig von Mises

We all read about various financial crises in the news, wonder about how these big bailouts work and are puzzled over the fact that no one ever seems to be held accountable for damages which are in the trillions. I am still puzzled, but at least I am starting to get a glimpse of what is going on in the world of finance.

Some people even go as far as to attribute the general ignorance on these topics to systemic, willful ignorance. While history, physics, biology, math, and languages are all part of our education, the world of money and finance surprisingly is only explored superficially, if at all. I wonder if people would still be willing to accrue as much debt as they currently do if everyone would be educated in personal finance and the workings of money and debt. Then I wonder how many layers of aluminum make an effective tinfoil hat. Probably three.

“Those crashes, these bailouts, are not accidents. And neither is it an accident that there is no financial education in school. […] It’s premeditated. Just as prior to the Civil War it was illegal to educate a slave, we are not allowed to learn about money in school.” —Robert Kiyosaki

Like in The Wizard of Oz, we are told to pay no attention to the man behind the curtain. Unlike in The Wizard of Oz, we now have real wizardry: a censorship-resistant, open, borderless network of value-transfer. There is no curtain, and the magic is visible to anyone.

Bitcoin taught me to look behind the curtain and face my financial ignorance.

Lesson 9: Inflation

Trying to understand monetary inflation, and how a non-inflationary system like Bitcoin might change how we do things, was the starting point of my venture into economics. I knew that inflation was the rate at which new money was created, but I didn't know too much beyond that.

While some economists argue that inflation is a good thing, others argue that "hard" money which can't be inflated easily —as we had in the days of the gold standard—is essential for a healthy economy. Bitcoin, having a fixed supply of 21 million, agrees with the latter camp.

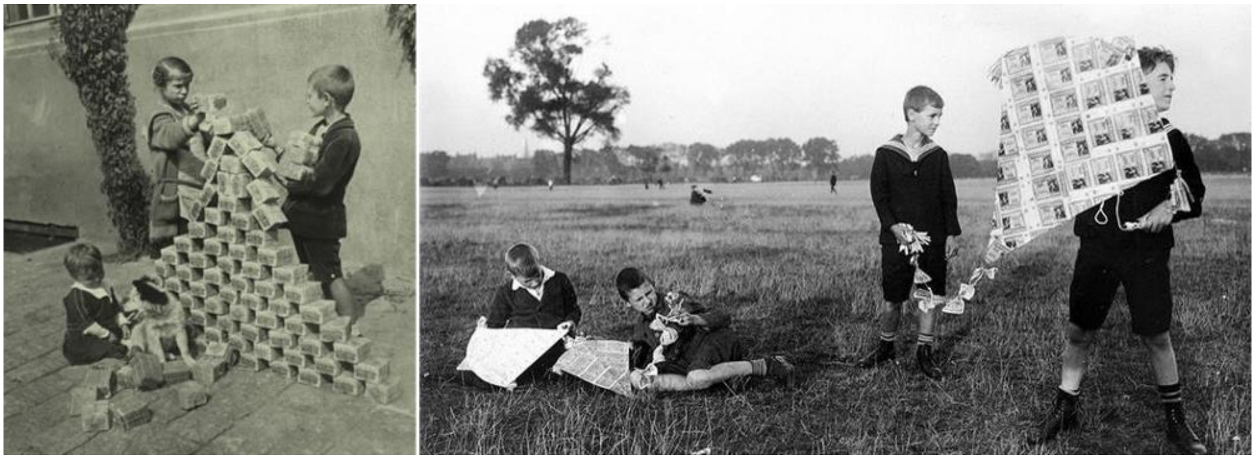
Usually, the effects of inflation are not immediately obvious. Depending on the inflation rate (as well as other factors) the time between cause and effect can be several years. Not only that, but inflation affects different groups of people more than others. As Henry Hazlitt points out in *Economics in One Lesson*: "The art of economics consists in looking not merely at the immediate but at the longer effects of any act or policy; it consists in tracing the consequences of that policy not merely for one group but for all groups."

One of my personal lightbulb moments was the realization that issuing new currency—printing more money—is a *completely* different economic activity than all the other economic activities. While real goods and real services produce real value for real people, printing money effectively does the opposite: it takes away value from everyone who holds the currency which is being inflated.

"Mere inflation—that is, the mere issuance of more money, with the consequence of higher wages and prices—may look like the creation of more demand. But in terms of the actual production and exchange of real things it is not." —Henry Hazlitt

The destructive force of inflation becomes obvious as soon as a little inflation turns into *a lot*. If money hyperinflates, things get ugly real quick. As the inflating currency falls apart, it will fail to store value over time and people will rush to get their hands on any goods which might do.

Another consequence of hyperinflation is that all the money which people have saved over the course of their life will effectively vanish. The paper money in your wallet will still be there, of course. But it will be exactly that: worthless paper.



Hyperinflation in the Weimar Republic (1921-1923)

Money declines in value with so-called “mild “ inflation as well. It just happens slowly enough that most people don’t notice the diminishing of their purchasing power. And once the printing presses are running, currency can be easily inflated, and what used to be mild inflation might turn into a strong cup of inflation by the push of a button. As Friedrich Hayek pointed out in one of his essays, mild inflation usually leads to outright inflation.

"”Mild” steady inflation cannot help—it can lead only to outright inflation.”

—Friedrich Hayek

Inflation is particularly devious since it favors those who are closer to the printing presses. It takes time for the newly created money to circulate and prices to adjust, so if you are able to get your hands on more money before everyone else’s devaluates you are ahead of the inflationary curve. This is also why inflation can be seen as a hidden tax because in the end governments profit from it while everyone else ends up paying the price.

“I do not think it is an exaggeration to say history is largely a history of inflation, and usually of inflations engineered by governments for the gain of governments.”

—Friedrich Hayek

So far, all government-controlled currencies have eventually been replaced or have collapsed completely. No matter how small the rate of inflation, “steady” growth is just another way of saying exponential growth. In nature as in economics, all systems which grow exponentially will eventually have to level off or suffer from catastrophic collapse.

“It can’t happen in my country,” is what you’re probably thinking. You don’t think that if you are from Venezuela, which is currently suffering from hyperinflation. With an inflation rate of over 1 million percent, money is basically worthless.

It might not happen in the next couple of years, or to the particular currency used in your country. But a glance at the list of historical currencies shows that it will inevitably happen over a long enough period of time. I remember and used plenty of those listed: the Austrian schilling, the German mark, the Italian lira, the French franc, the Irish pound, the Croatian dinar, etc. My grandma even used the Austro-Hungarian Krone. As time moves on, the currencies currently in use will slowly but surely move to their respective graveyards. They will hyperinflate or be replaced. They will soon be historical currencies. We will make them obsolete.

“History has shown that governments will inevitably succumb to the temptation of inflating the money supply.” —Saifedean Ammous

Why is Bitcoin different? In contrast to currencies mandated by the government, monetary goods which are not regulated by governments, but by the laws of physics, tend to survive and even hold their respective value over time. The best example of this so far is gold, which, as the aptly-named *Gold-to-Decent-Suit Ratio* shows, is holding its value over hundreds and even thousands of years. It might not be perfectly “stable”— a questionable concept in the first place—but the value it holds will at least be in the same order of magnitude.

If a monetary good or currency holds its value well over time and space, it is considered to be *hard*. If it can’t hold its value, because it easily deteriorates or inflates, it is considered a *soft* currency. The concept of hardness is essential to understand Bitcoin and is worthy of a more thorough examination. We will return to it in the last economic lesson: sound money.

As more and more countries suffer from hyperinflation, more and more people will have to face the reality of hard and soft money. If we are lucky, maybe even some central bankers will be forced to re-evaluate their monetary policies. Whatever might happen, the insights I have gained thanks to Bitcoin will probably be invaluable, no matter the outcome.

Bitcoin taught me about the hidden tax of inflation and the catastrophe of hyperinflation.

Lesson 10: Value

Value is somewhat paradoxical, and there are multiple theories which try to explain why we value certain things over other things. People have been aware of this paradox for thousands of years. As Plato wrote in his dialogue with

Euthydemus, we value some things because they are rare, and not merely based on their necessity for our survival.

“And if you are prudent you will give this same counsel to your pupils also—that they are never to converse with anybody except you and each other. For it is the rare, Euthydemus, that is precious, while water is cheapest, though best, as Pindar said.”

—Plato

This paradox of value shows something interesting about us humans: we seem to value things on a subjective basis, but do so with certain non-arbitrary criteria. Something might be *precious* to us for a variety of reasons, but things we value do share certain characteristics. If we can copy something very easily, or if it is naturally abundant, we do not value it.

It seems that we value something because it is scarce (gold, diamonds, time), difficult or labor-intensive to produce, can’t be replaced (an old photograph of a loved one), is useful in a way in which it enables us to do things which we otherwise couldn’t, or a combination of those, such as great works of art.

Bitcoin is all of the above: it is extremely rare (21 million), increasingly hard to produce (reward halvening), can’t be replaced (a lost private key is lost forever), and enables us to do some quite useful things. It is arguably the best tool for value transfer across borders, virtually resistant to censorship and confiscation in the process, plus, it is a self-sovereign store of value, allowing individuals to store their wealth independent of banks and governments, just to name two.

Bitcoin taught me that value is subjective but not arbitrary.

Lesson 11: Money

What is money? We use it every day, yet this question is surprisingly difficult to answer. We are dependent on it in ways big and small, and if we have too little of it our lives become very difficult. Yet, we seldom think about the thing which supposedly makes the world go round. Bitcoin forced me to answer this question over and over again: What the hell is money?

In our “modern” world, most people will probably think of pieces of paper when they talk about money, even though most of our money is just a number in a bank account. We are already using zeros and ones as our money, so how is Bitcoin different? Bitcoin is different because at its core it is a very different *type* of money than the money we currently use. To understand this, we will have to take a closer look at what money is, how it came to be, and why gold and silver was used for most of commercial history.

“In this sense, it’s more typical of a precious metal. Instead of the supply changing to keep the value the same, the supply is predetermined and the value changes.”

—Satoshi Nakamoto

Seashells, gold, silver, paper, bitcoin. In the end, **money is whatever people use as money**, no matter its shape and form, or lack thereof.

Money, as an invention, is ingenious. A world without money is insanely complicated: How many fish will buy me new shoes? How many cows will buy me a house? What if I don’t need anything right now but I need to get rid of my soon-to-be rotten apples? You don’t need a lot of imagination to realize that a barter economy is maddeningly inefficient.

The great thing about money is that it can be exchanged for *anything else*— that’s quite the invention! As Nick Szabo brilliantly summarizes in *Shelling Out: The Origins of Money*, we humans have used all kinds of things as money: beads made of rare materials like ivory, shells, or special bones, various kinds of jewelry, and later on rare metals like silver and gold.

Being the lazy creatures we are, we don’t think too much about things which just work. Money, for most of us, works just fine. Like with our cars or our computers, most of us are only forced to think about the inner workings of these things if they break down. People who saw their life-savings vanish because of hyperinflation know the value of hard money, just like people who saw their friends and family vanish because of the atrocities of Nazi Germany or Soviet Russia know the value of privacy.

The thing about money is that it is all-encompassing. Money is half of every transaction, which imbues the ones who are in charge with creating money with enormous power.

“Given that money is one half of every commercial transaction and that whole civilizations literally rise and fall based on the quality of their money, we are talking about an awesome power, one that flies under the cover of night. It is the power to weave illusions that appear real as long as they last. That is the very core of the Fed’s power.”

—Ron Paul

Bitcoin peacefully removes this power, since it does away with money creation and it does so without the use of force.

Money went through multiple iterations. Most iterations were good. They improved our money in one way or another. Very recently, however, the inner workings of our money got corrupted. Today, almost all of our money is simply created *out of thin air* by the powers that be. To understand how this came to be I had to learn about the history and subsequent downfall of money.

If it will take a series of catastrophes or simply a monumental educational effort to correct this corruption remains to be seen. I pray to the gods of sound money that it will be the latter.

Bitcoin taught me what money is.

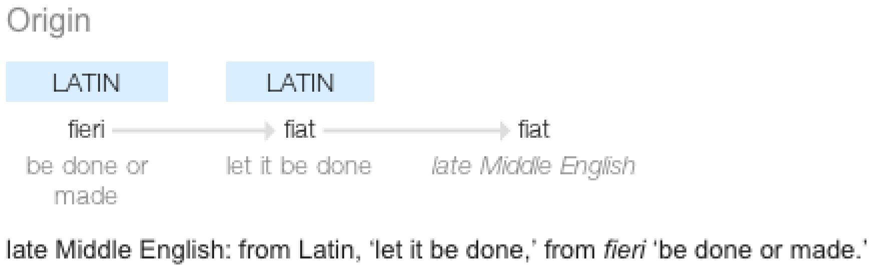
Lesson 12: The history and downfall of money

Many people think that money is backed by gold, which is locked away in big vaults, protected by thick walls. This ceased to be true many decades ago. I am not sure what I thought, since I was in much deeper trouble, having virtually no understanding of gold, paper money, or why it would need to be backed by something in the first place.

One part of learning about Bitcoin is learning about fiat money: what it means, how it came to be, and why it might not be the best idea we ever had. So, what exactly is fiat money? And how did we end up using it?

If something is imposed by *fiat*, it simply means that it is imposed by formal authorization or proposition. Thus, fiat money is money simply because *someone* says that it is money. Since all governments use fiat currency today, this someone is *your* government. Unfortunately, you are not *free* to disagree with this value proposition. You will quickly feel that this proposition is everything but non-violent. If you refuse to use this paper currency to do business and pay taxes the only people you will be able to discuss economics with will be your cellmates.

The value of fiat money does not stem from its inherent properties. How good a certain type of fiat money is, is only correlated to the political and fiscal (in)stability of those who dream it into existence. Its value is imposed by decree, arbitrarily.



late Middle English: from Latin, 'let it be done,' from *fieri* 'be done or made.'

fi·at /ˈfēˌät,ˈfēət/ — ”Let it be done”

Until recently, two types of money were used: **commodity money**, made out of precious *things*, and **representative money**, which simply *represents* the precious thing, mostly in writing.

We already touched on commodity money above. People used special bones, seashells, and precious metals as money. Later on, mainly coins made out of precious metals like gold and silver were used as money. The oldest coin found so far is made of a natural gold-and-silver mix and was made more than 2700 years ago. If something is new in Bitcoin, the concept of a coin is not it.

Lydian electrum coin

Turns out that hoarding coins, or hodling, to use today's parlance, is almost as old as coins. The earliest coin hodler was someone who put almost a hundred of these coins in a pot and buried it in the foundations of a temple, only to be found 2500 years later. Pretty good cold storage if you ask me.

One of the downsides of using precious metal coins is that they can be clipped, effectively debasing the value of the coin. New coins can be minted from the clippings, inflating the money supply over time, devaluing every individual coin in the process. People were literally shaving off as much as they could get away with of their silver dollars. I wonder what kind of *Dollar Shave Club* advertisements they had back in the day.

Since governments are only cool with inflation if they are the ones doing it, efforts were made to stop this guerrilla debasement. In classic cops-and-robbers fashion, coin clippers got ever more creative with their techniques, forcing the 'masters of the mint' to get even more creative with their countermeasures. Isaac Newton, the world-renowned physicist of *Principia Mathematica* fame, used to be one of these masters. He is attributed with adding the small stripes at the side of coins which are still present today. Gone were the days of easy coin shaving.

Example of shaved coins

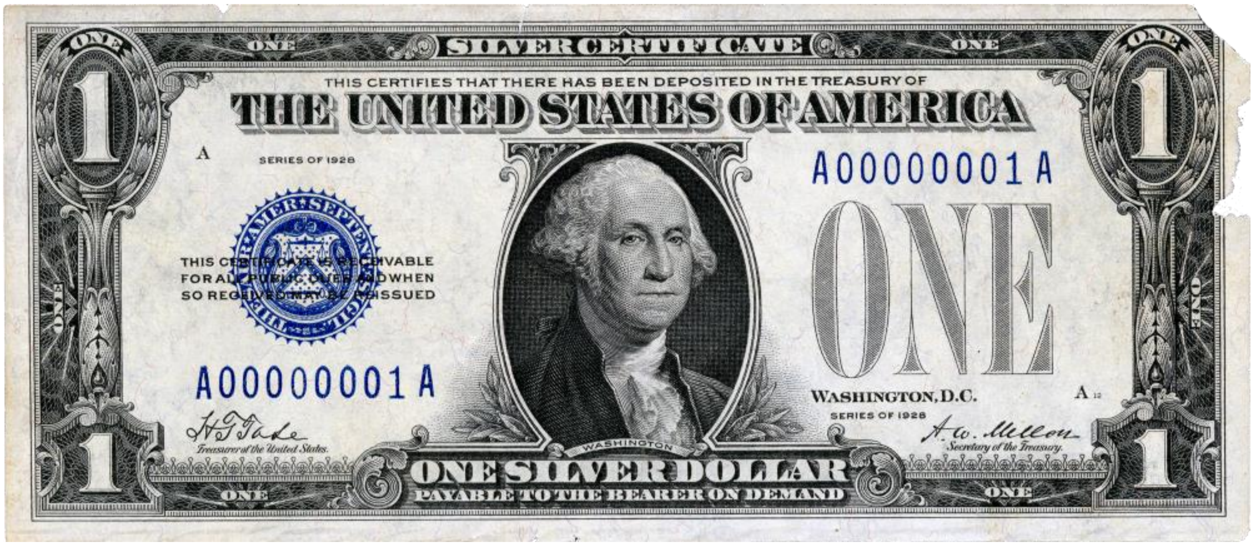
Even with these methods of coin debasement kept in check, coins still suffer from other issues. They are bulky and not very convenient to transport, especially when large transfers of value need to happen. Showing up with a huge bag of silver dollars every time you want to buy a Mercedes isn’t very practical.

Speaking of German things: How the United States *dollar_got its name is another interesting story. The word “dollar” is derived from the German word _Thaler_, short for a _Joachimsthaler.* A Joachimsthaler was a coin minted in the town of *Sankt Joachimsthal*. Thaler is simply a shorthand for someone (or something) coming from the valley, and because Joachimsthal was *the* valley for silver coin production, people simply referred to these silver coins as *Thaler*. Thaler (German) morphed into daalders (Dutch), and finally dollars (English).

The original "dollar". Saint Joachim is pictured with his robe and wizard hat. Picture cc-by-sa Berlin-George

The introduction of representative money heralded the downfall of hard money. Gold certificates were introduced in 1863, and about fifteen years later, the silver dollar was also slowly but surely being replaced by a paper proxy: the silver certificate.

It took about 50 years from the introduction of the first silver certificates until these pieces of paper morphed into something that we would today recognize as one U.S. dollar.


SILVER CERTIFICATE
THIS CERTIFIES THAT THERE HAS BEEN DEPOSITED IN THE TREASURY OF
THE UNITED STATES OF AMERICA
SERIES OF 1928
A00000001 A
ONE
ONE SILVER DOLLAR
PAYABLE TO THE BEARER ON DEMAND
WASHINGTON, D.C.
WASHINGTON
Treasurer of the United States
Secretary of the Treasury

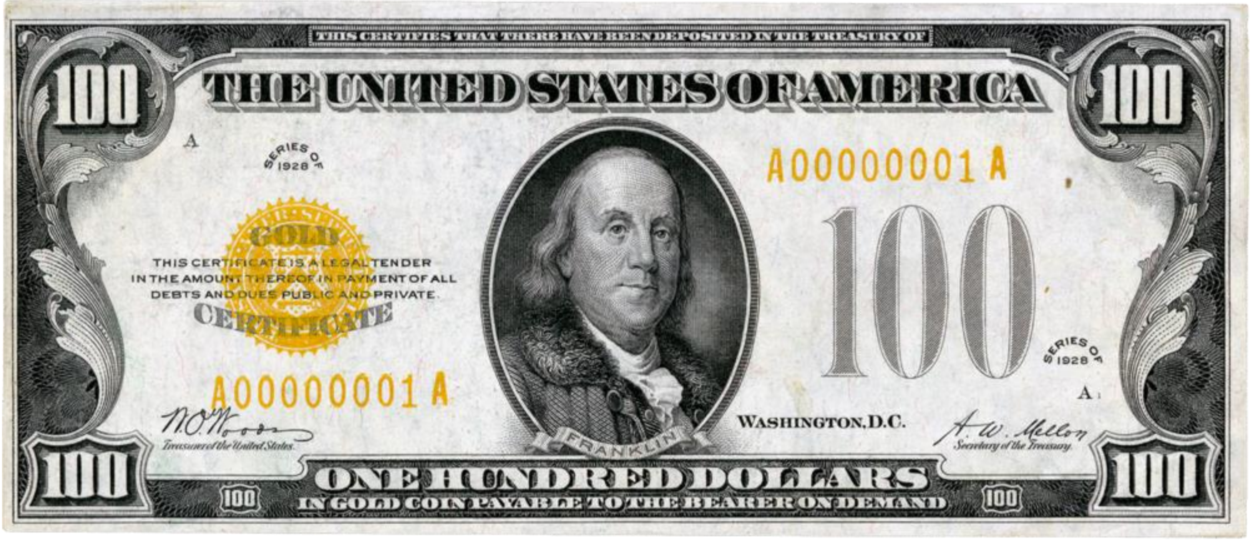
A 1928 U.S. silver dollar. "Payable to the bearer on demand." Picture credit to the National Numismatic Collection at the Smithsonian Institution

Note that the 1928 U.S. silver dollar above still goes by the name of *silver certificate*, indicating that this is indeed simply a document stating that the bearer of this piece of paper is owed a piece of silver. It is interesting to see that the text which indicates this got smaller over time. The trace of "certificate" vanished completely after a while, being replaced by the reassuring statement that these are federal reserve notes.

As mentioned above, the same thing happened to gold. Most of the world was on a bimetallic standard, meaning coins were made primarily of gold and silver. Having certificates for gold, redeemable in gold coins, was arguably a technological improvement. Paper is more convenient, lighter, and since it can be divided arbitrarily by simply printing a smaller number on it, it is easier to break into smaller units.

To remind the bearers (users) that these certificates were representative for actual gold and silver, they were colored accordingly and stated this clearly on the certificate itself. You can fluently read the writing from top to bottom:

"This certifies that there have been deposited in the treasury of the United States of America one hundred dollars in gold coin payable to the bearer on demand."



THIS CERTIFIES THAT THERE HAVE BEEN DEPOSITED IN THE TREASURY OF

100 THE UNITED STATES OF AMERICA 100

A SERIES OF 1928

A00000001 A

GOLD

THIS CERTIFICATE IS A LEGAL TENDER IN THE AMOUNT THEREOF IN PAYMENT OF ALL DEBTS AND DUES PUBLIC AND PRIVATE.

CERTIFICATE

100

SERIES OF 1928

A

A00000001 A

W.O. Woods
Treasurer of the United States.

FRANKLIN

WASHINGTON, D.C.

A.W. Mellon
Secretary of the Treasury.

100 ONE HUNDRED DOLLARS 100

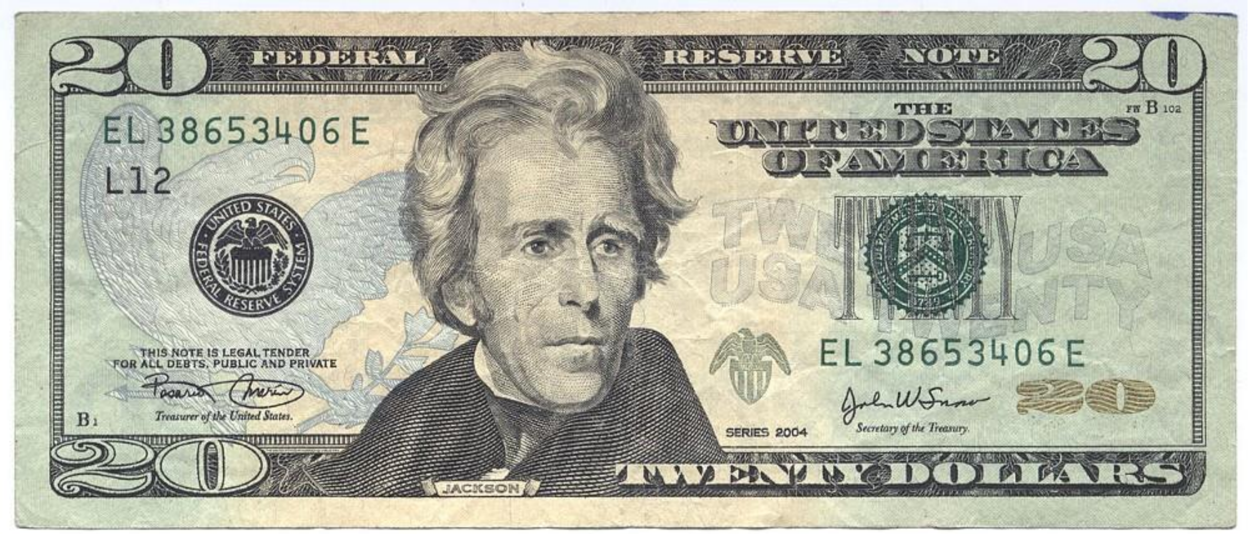
100 IN GOLD COIN PAYABLE TO THE BEARER ON DEMAND 100

Picture credit to National Numismatic Collection, National Museum of American History.

In 1963, the words "PAYABLE TO THE BEARER ON DEMAND" were removed from all newly issued notes. Five years later, the redemption of paper notes for gold and silver ended.

The words hinting on the origins and the idea behind paper money were removed. The golden color disappeared. All that was left was the paper and with it the ability of the government to print as much of it as it wishes.

With the abolishment of the gold standard in 1971, this century-long sleight-of-hand was complete. Money became the illusion we all share to this day: fiat money. It is worth something because someone commanding an army and operating jails says it is worth something. As can be clearly read on every dollar note in circulation today, “THIS NOTE IS LEGAL TENDER”. In other words: It is valuable because the note says so.


FEDERAL RESERVE NOTE
THE UNITED STATES OF AMERICA
EL 38653406 E
L12
THIS NOTE IS LEGAL TENDER FOR ALL DEBTS, PUBLIC AND PRIVATE
Treasurer of the United States.
SERIES 2004
Secretary of the Treasury.
JACKSON
TWENTY DOLLARS
20

A 2004 series U.S. twenty dollar note used today. “THIS NOTE IS LEGAL TENDER”

By the way, there is another interesting lesson on today’s bank notes, hidden in plain sight. The second line reads that this is legal tender “FOR ALL DEBTS, PUBLIC AND PRIVATE”. What might be obvious to economists was surprising to me: All money is debt. My head is still hurting because of it, and I will leave the exploration of the relation of money and debt as an exercise to the reader.

As we have seen, gold and silver were used as money for millennia. Over time, coins made from gold and silver were replaced by paper. Paper slowly became accepted as payment. This acceptance created an illusion—the illusion that the paper itself has value. The final move was to completely sever the link between the representation and the actual: abolishing the gold standard and convincing everyone that the paper in itself is precious.

Bitcoin taught me about the history of money and the greatest sleight of hand in the history of economics: fiat currency.

Lesson 13: Fractional Reserve Insanity

Value and money aren’t trivial topics, especially in today’s times. The process of money creation in our banking system is equally non-trivial, and I can’t shake the feeling that this is deliberately so. What I have previously only encountered in academia and legal texts seems to be common practice in the financial world as well: nothing is explained in simple terms, not because it is truly complex, but because the truth is hidden behind layers and layers of jargon and *apparent* complexity. “Expansionary monetary policy, quantitative easing, fiscal stimulus to the economy.” The audience nods along in agreement, hypnotized by the fancy words.

Fractional reserve banking and quantitative easing are two of those fancy words, obfuscating what is really happening by masking it as complex and difficult to understand. If you would explain them to a five-year-old, the insanity of both will become apparent quickly.

Godfrey Bloom, addressing the European Parliament during a joint debate, said it way better than I ever could:

“[…] you do not really understand the concept of banking. All the banks are broke. Bank Santander, Deutsche Bank, Royal Bank of Scotland—they’re all broke! And why are they broke? It isn’t an act of God. It isn’t some sort of tsunami. They’re broke because we have a system called ‘fractional reserve banking’ which means that banks can lend money that they don’t actually have! It’s a criminal scandal and it’s been going on for too long. […]

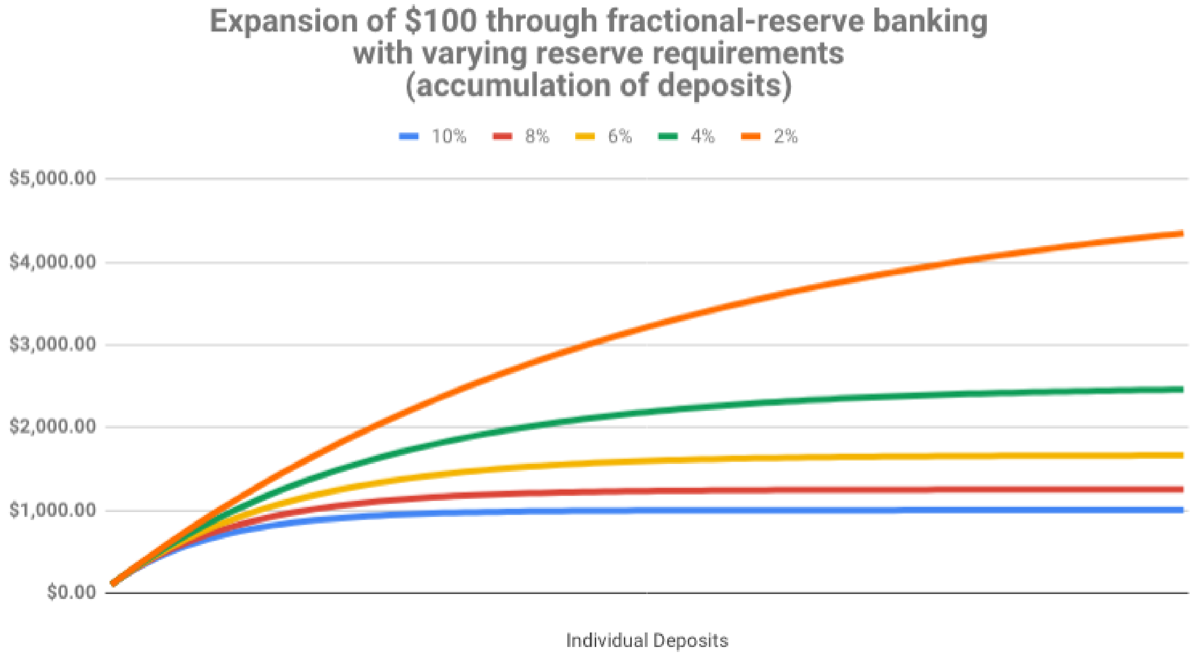
We have counterfeiting—sometimes called quantitative easing—but counterfeiting by any other name. The artificial printing of money which, if any ordinary person did, they’d go to prison for a very long time […] and until we start sending bankers—and I include central bankers and politicians—to prison for this outrage it will continue.”

Let me repeat the most important part: banks can lend money that they don’t actually have.

Thanks to fractional reserve banking, a bank only has to keep a small *fraction* of every dollar it gets. It’s somewhere between 0 and 10%, usually at the lower end, which makes things even worse.

Let’s use a concrete example to better understand this crazy idea: A fraction of 10% will do the trick and we should be able to do all the calculations in our head. Win-win. So, if you take $100 to a bank—because you don’t want to store it under your mattress—they only have to keep the agreed upon *fraction* of it. In our example that would be $10, because 10% of $100 is $10. Easy, right?

So what do banks do with the rest of the money? What happens to your $90? They do what banks do, they lend it to other people. The result is a money multiplier effect, which increases the money supply in the economy enormously. Your initial deposit of $100 will soon turn into $190. By lending a 90% fraction of the newly created $90, there will soon be $271 in the economy. And $343.90 after that. The money supply is recursively increasing, since banks are literally lending money they don’t have. Without a single Abracadabra, banks magically transform $100 into one thousand dollars or more. Turns out 10x is easy. It only takes a couple of lending rounds.



Don't get me wrong: There is nothing wrong with lending. There is nothing wrong with interest. There isn't even anything wrong with good old regular banks to store your wealth somewhere more secure than in your sock drawer.

Central banks, however, are a different beast. Abominations of financial regulation, half public half private, playing god with something which affects everyone who is part of our global civilization, without a conscience, only interested in the immediate future, and seemingly without any accountability or auditability.

While Bitcoin is still inflationary, it will cease to be so rather soon. The strictly limited supply of 21 million bitcoins will eventually do away with inflation completely. We now have two monetary worlds: an inflationary one where money is printed arbitrarily, and the world of Bitcoin, where final supply is fixed and easily auditable for everyone. One is forced upon us by violence, the other can be joined by anyone who wishes to do so. No barriers to entry, no one to ask for permission. Voluntary participation. That is the beauty of Bitcoin.

I would argue that the argument between Keynesian and Austrian economists is no longer purely academical. Satoshi managed to build a system for value transfer on steroids, creating the soundest money which ever existed in the process. One way or another, more and more people will learn about the scam which is fractional reserve banking. If they come to similar conclusions as most

Austrians and Bitcoiners, they might join the ever-growing internet of money. Nobody can stop them if they choose to do so.

Bitcoin taught me that fractional reserve banking is pure insanity.

Lesson 14: Sound money

The most important lesson I have learned from Bitcoin is that in the long run, hard money is superior to soft money. Hard money, also referred to as *sound money*, is any globally traded currency that serves as a reliable store of value.

Granted, Bitcoin is still young and volatile. Critics will say that it does not store value reliably. The volatility argument is missing the point. Volatility is to be expected. The market will take a while to figure out the just price of this new money. Also, as is often jokingly pointed out, it is grounded in an error of measurement. If you think in dollars you will fail to see that one bitcoin will always be worth one bitcoin.

"A fixed money supply, or a supply altered only in accord with objective and calculable criteria, is a necessary condition to a meaningful just price of money."

—Fr. Bernard W. Dempsey, S.J.

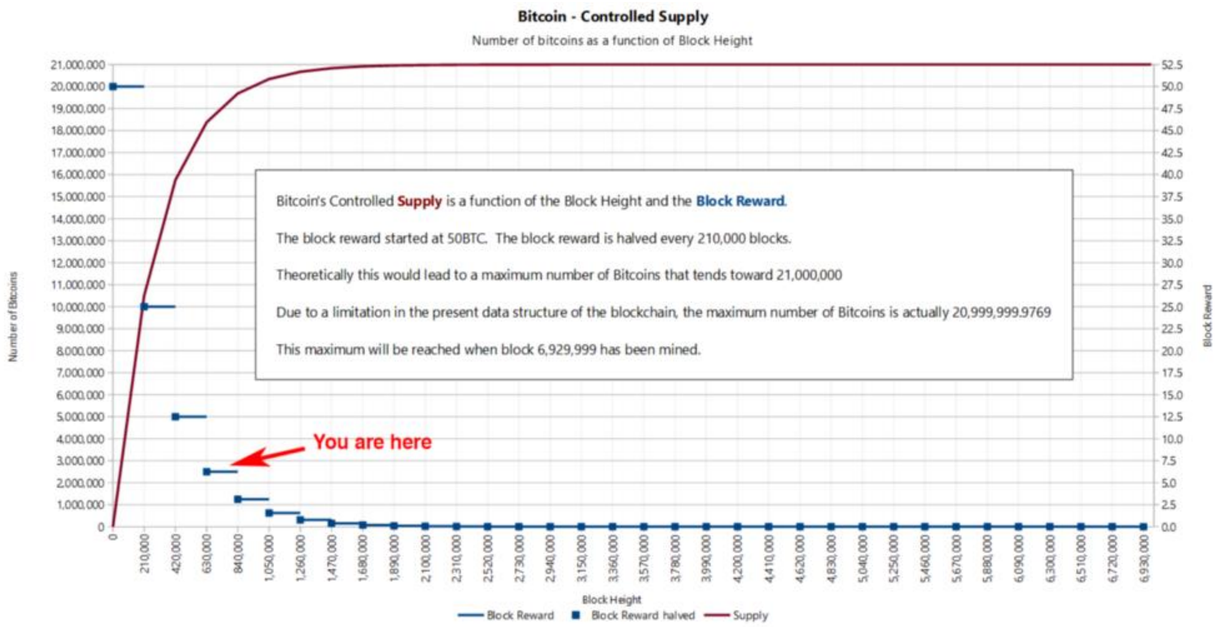
As a quick stroll through the graveyard of forgotten currencies has shown, money which can be printed will be printed. So far, no human in history was able to resist this temptation.

Bitcoin does away with the temptation to print money in an ingenious way. Satoshi was aware of our greed and fallibility—this is why he chose something more reliable than human restraint: mathematics.

$$\frac{\sum_{i=0}^{32} 210000 \left\lfloor \frac{50*10^8}{2^i} \right\rfloor}{10^8}$$

Bitcoin's "supply formula"

While this formula is useful to describe Bitcoin's supply, it is actually nowhere to be found in the code. Issuance of new bitcoin is done in an algorithmically controlled fashion, by reducing the reward which is paid to miners every four years. The formula above is used to quickly sum up what is happening under the hood. What really happens can be best seen by looking at the change in block reward, the reward paid out to whoever finds a valid block, which roughly happens every 10 minutes.



Bitcoin's Controlled **Supply** is a function of the Block Height and the **Block Reward.**

The block reward started at 50BTC. The block reward is halved every 210,000 blocks.

Theoretically this would lead to a maximum number of Bitcoins that tends toward 21,000,000

Due to a limitation in the present data structure of the blockchain, the maximum number of Bitcoins is actually 20,999,999.9769

This maximum will be reached when block 6,929,999 has been mined.

Formulas, logarithmic functions and exponentials are not exactly intuitive to understand. The concept of *soundness* might be easier to understand if looked at in another way. Once we know how much there is of something, and once we know how hard this something is to produce or get our hands on, we immediately understand its value. What is true for Picasso's paintings, Elvis Presley's guitars, and Stradivarius violins is also true for fiat currency, gold, and bitcoins.

The hardness of fiat currency depends on who is in charge of the respective printing presses. Some governments might be more willing to print large amounts of currency than others, resulting in a weaker currency. Other governments might be more restrictive in their money printing, resulting in harder currency.

Before we had fiat currencies, the soundness of money was determined by the natural properties of the stuff which we used as money. The amount of gold on earth is limited by the laws of physics. Gold is rare because supernovae and neutron star collisions are rare. The "flow" of gold is limited because extracting it is quite an effort. Being a heavy element it is mostly buried deep underground.

The abolishment of the gold standard gave way to a new reality: adding new money requires just a drop of ink. In our modern world adding a couple of zeros to the balance of a bank account requires even less effort: flipping a few bits in a bank computer is enough.

"One important aspect of this new reality is that institutions like the Fed cannot go bankrupt. They can print any amount of money that they might need for themselves at virtually zero cost." —Jörg Guido Hülsmann

The principle outlined above can be expressed more generally as the ratio of “stock” to “flow”. Simply put, the *stock* is how much of something is currently there. For our purposes, the stock is a measure of the current money supply. The *flow* is how much there is produced over a period of time (e.g. per year). The key to understanding sound money is in understanding this stock-to-flow ratio.

Calculating the stock-to-flow ratio for fiat currency is difficult, because how much money there is depends on how you look at it. You could count only banknotes and coins (M0), add traveler checks and check deposits (M1), add saving accounts and mutual funds and some other things (M2), and even add certificates of deposit to all of that (M3). Further, how all of this is defined and measured varies from country to country and since the US Federal Reserve stopped publishing numbers for M3, we will have to make do with the M2 monetary supply. I would love to verify these numbers, but I guess we have to trust the fed for now.

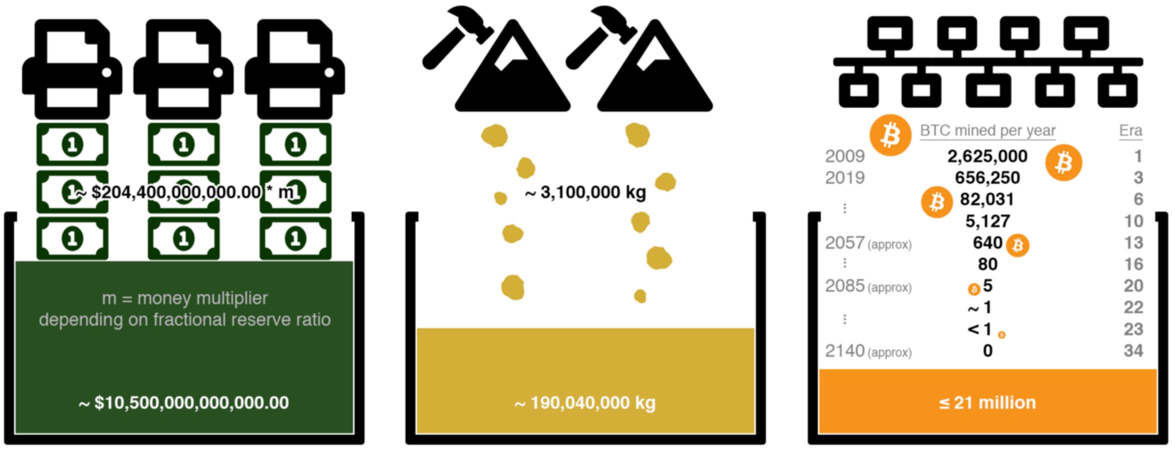
Gold, one of the rarest metals on earth, has the highest stock-to-flow ratio. According to the US Geological Survey, a little more than 190,000 tons have been mined. In the last few years, around 3100 tons of gold have been mined per year.

Using these numbers, we can easily calculate the stock-to-flow ratio for gold: 190,000 tons / 3,100 tons = ~61.

Nothing has a higher stock-to-flow ratio than gold. This is why gold, up to now, was the hardest, soundest money in existence. It is often said that all the gold mined so far would fit in two olympic-sized swimming pools. According to my calculations, we would need four. So maybe this needs updating, or Olympic-sized swimming pools got smaller.

Enter Bitcoin. As you probably know, bitcoin mining was all the rage in the last couple of years. This is because we are still in the early phases of what is called the *reward era*, where mining nodes are rewarded with *a lot* of bitcoin for their computational effort. We are currently in reward era number 3, which began in 2018 and will end in early 2020, probably in May. While the bitcoin supply is predetermined, the inner workings of Bitcoin only allow for approximate dates. Nevertheless, we can predict with certainty how high Bitcoin’s stock-to-flow ratio will be. Spoiler alert: it will be high.

How high? Well, it turns out that Bitcoin will get infinitely hard.

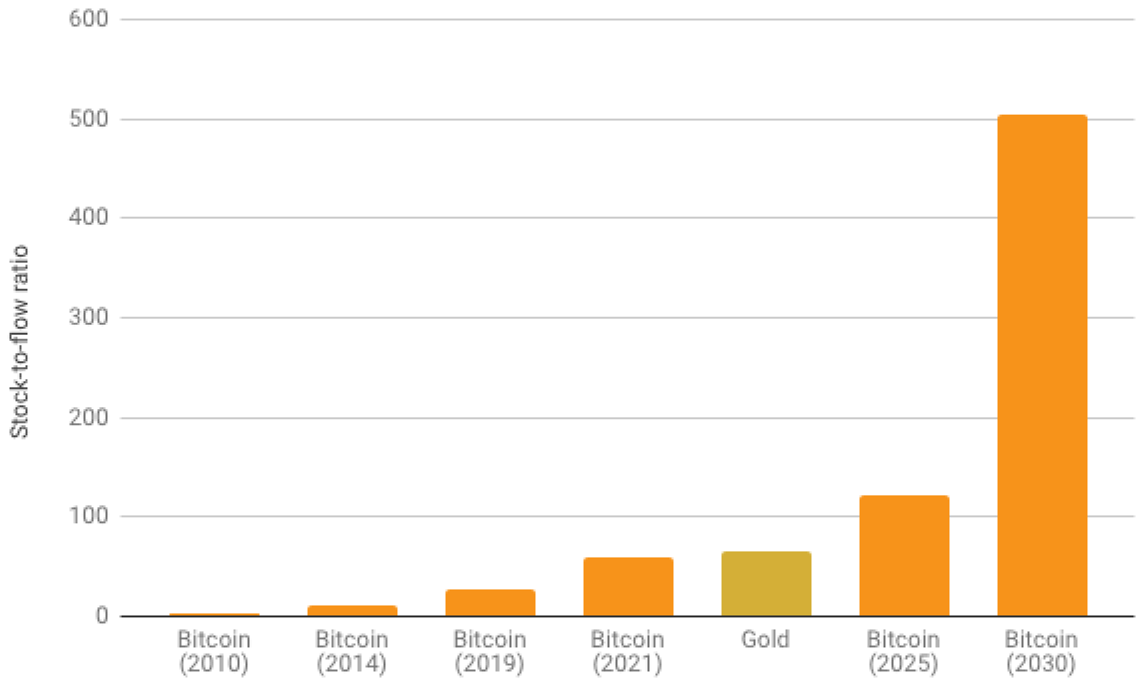


	BTC mined per year	Era
2009	2,625,000	1
2019	656,250	3
⋮	82,031	6
	5,127	10
2057 (approx)	640	13
⋮	80	16
2085 (approx)	5	20
	~ 1	22
⋮	< 1	23
2140 (approx)	0	34

dergigi Fiat production according to U.S. Department of the Treasury [0], Gold production according to to U.S. Geological Survey [1], Bitcoin supply according to calculations by the author [2]
[0] https://www.treasury.gov/resource-center/faqs/Currency/Pages/edu_faq_currency_production.aspx [1] https://minerals.usgs.gov/minerals/pubs/mcs/2018/mcs2018.pdf [2] http://bit.ly/btc-stock-to-flow

Visualization of stock and flow for USD, gold, and Bitcoin

Due to an exponential decrease of the mining reward, the flow of new bitcoin will diminish resulting in a sky-rocketing stock-to-flow ratio. It will catch up to gold in 2020, only to surpass it four years later by doubling its soundness again. Such a doubling will occur 64 times in total. Thanks to the power of exponentials, the number of bitcoin mined per year will drop below 100 bitcoin in 50 years and below 1 bitcoin in 75 years. The global faucet which is the block reward will dry up somewhere around the year 2140, effectively stopping the production of bitcoin. This is a long game. If you are reading this, you are still early.



Rising stock-to-flow ratio of bitcoin as compared to gold

As bitcoin approaches infinite stock to flow ratio it will be the soundest money in existence. Infinite soundness is hard to beat.

Viewed through the lens of economics, Bitcoin's *difficulty adjustment* is probably its most important component. How hard it is to mine bitcoin depends on how quickly new bitcoins are mined. It is the dynamic adjustment of the network's mining difficulty which enables us to predict its future supply.

(It actually depends on how quickly valid blocks are found, but for our purposes, this is the same thing as "mining bitcoins" and will be so for the next 120 years.)

The simplicity of the difficulty adjustment algorithm might distract from its profundity, but the difficulty adjustment truly is a revolution of Einsteinian proportions. It ensures that, no matter how much or how little effort is spent on mining, Bitcoin's controlled supply won't be disrupted. As opposed to every other resource, no matter how much energy someone will put into mining bitcoin, the total reward will not increase.

Just like $E=mc^2$ dictates the universal speed limit in our universe, Bitcoin's difficulty adjustment dictates the **universal money limit** in Bitcoin.

If it weren't for this difficulty adjustment, all bitcoins would have been mined already. If it weren't for this difficulty adjustment, Bitcoin probably wouldn't have survived in its infancy. It is what secures the network in its reward era. It is what ensures a steady and fair distribution of new bitcoin. It is the thermostat which regulates Bitcoin's monetary policy.

Einstein showed us something novel: no matter how hard you push an object, at a certain point you won't be able to get more speed out of it. Satoshi also showed us something novel: no matter how hard you dig for this digital gold, at a certain point you won't be able to get more bitcoin out of it. For the first time in human history, we have a monetary good which, no matter how hard you try, you won't be able to produce more of.

Bitcoin taught me that me that sound money is essential.

Conclusion

As we leave the "blockchain not bitcoin" days behind us, most people start to realize that there is not a *single* invention which encapsulates the genius of Bitcoin. It is the combination of multiple, previously unrelated pieces, glued together by game theoretical incentives, which make up the revolution that is Bitcoin.

For me, the economic teachings of Bitcoin are as fascinating as the philosophical ones examined in part one. Being a technophile, I can't wait to tell you what Bitcoin taught me about technology in the third and final part of this series.

As mentioned before, I think that any answer to the question *"What have you learned from Bitcoin?"* will always be incomplete. The symbiosis of the two living systems examined here—Bitcoin and economics—is too intertwined and evolving too fast to ever be fully understood by a single person.

"I don't believe we shall ever have a good money again before we take the thing out of the hands of government, that is, we can't take it violently out of the hands of government, all we can do is by some sly roundabout way introduce something that they can't stop." —Friedrich Hayek

Learning these lessons enabled me to finally understand what Hayek meant by the above. I believe that Bitcoin is the sly, roundabout way to re-introduce sound money to the world. Thanks to the economic teachings of Bitcoin I learned what good money is and that having it is possible.

What have you learned from Bitcoin?

Acknowledgments

- Again, thanks to Arjun Balaji for the tweet which gave birth to this series.
- Thanks to Saifedean Ammous for his convictions, savage tweets, and writing *The Bitcoin Standard*

- Thanks to Dhruv Bansal for taking the time to discuss some of these ideas with me.
- Thanks to Matt Odell for his candor and also for taking the time to discuss some of these ideas with me, even if he doesn’t remember all of it.
- Thanks to Michael Goldstein and Pierre Rochard for curating and providing relevant literature via the Nakamoto Institute
- Thanks to Jannik,Camilo, and Matt for providing feedback to early drafts of this article

Further Reading

There exists an almost endless list of books and essays on the topics discussed above and economic thought in general. The books and articles listed below are but a small selection which were particularly influential in my thinking. I am grateful for all the people who shared their insights, past and present.

- *The Bitcoin Standard: The Decentralized Alternative to Central Banking* by Saifedean Ammous
- *Economics in One Lesson* by Henry Hazlitt
- *Human Action* by Ludwig von Mises
- *The Ethics of Money Production* by Jörg Guido Hülsmann
- *The Denationalization of Money* by Friedrich Hayek
- *The Machinery of Freedom* by David D. Friedman
- *The Case Against The Fed* by Murray N. Rothbard
- *End the Fed* by Ron Paul
- *Shelling Out: The Origins of Money* by Nick Szabo
- *The Bitcoin Halving and Monetary Competition* by Saifedean Ammous
- *The Bullish Case For Bitcoin* by Vijay Boyapati
- *Bitcoin’s distribution was fair* by Dan Held

Technological Teachings of Bitcoin

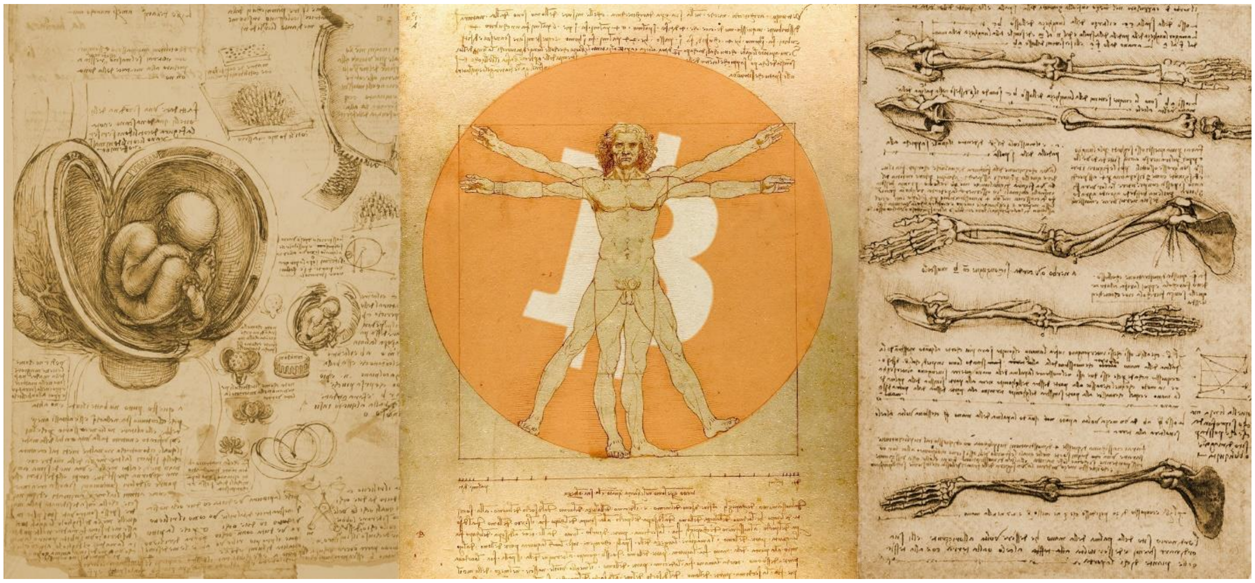
What I've Learned From Bitcoin: Part III

By Gigi

Posted April 2, 2019

This is part 3 of a 3 part series

- Part 1 Philosophical Teachings of Bitcoin
- Part 2 Economic Teachings of Bitcoin
- Part 3 Technological Teachings of Bitcoin



What is Bitcoin? The many answers to this question are as interesting as they are varied. Bitcoin is both a social and a monetary phenomenon, but it is also a technological one. The intersection of many disciplines is what makes Bitcoin endlessly fascinating. Like many others, I began to stumble down this strange rabbit hole a while ago. Even though this article is the last of this series, I am still stumbling down with no end in sight, and I invite you to stumble along with me.

This is the third chapter of a personal journey. Again, I am indebted to Arjun Balaji who asked the following on Twitter: "What have you learned from Bitcoin?" It is this question which has led me to write this series to outline some of the things I've learned.

- I: Philosophical Teachings of Bitcoin
- II: Economic Teachings of Bitcoin
- **III: Technological Teachings of Bitcoin**

Part one explored what I've learned from Bitcoin when seen through a philosophical lens: the interplay of immutability and change, copying and scarcity, Bitcoin's origin story and identity, locality in a world of replication, money as free speech, and the limits of knowledge.

Part two discussed some of the economic teachings of Bitcoin: the concept of value, (sound) money and its history, inflation, and some aspects of "modern" banking like fractional reserve banking.

Part three will explore seven things I have learned from examining Bitcoin through the lens of technology. As in the previous parts, I will only be able to scratch the surface. Bitcoin is an expanding universe, evolving and improving every day. Whole books can be and have been written on small, specific parts of this cosmos. And just like in our own universe, the expansion seems to be accelerating.

Find lessons 1–7 here and lessons 8–14 here.

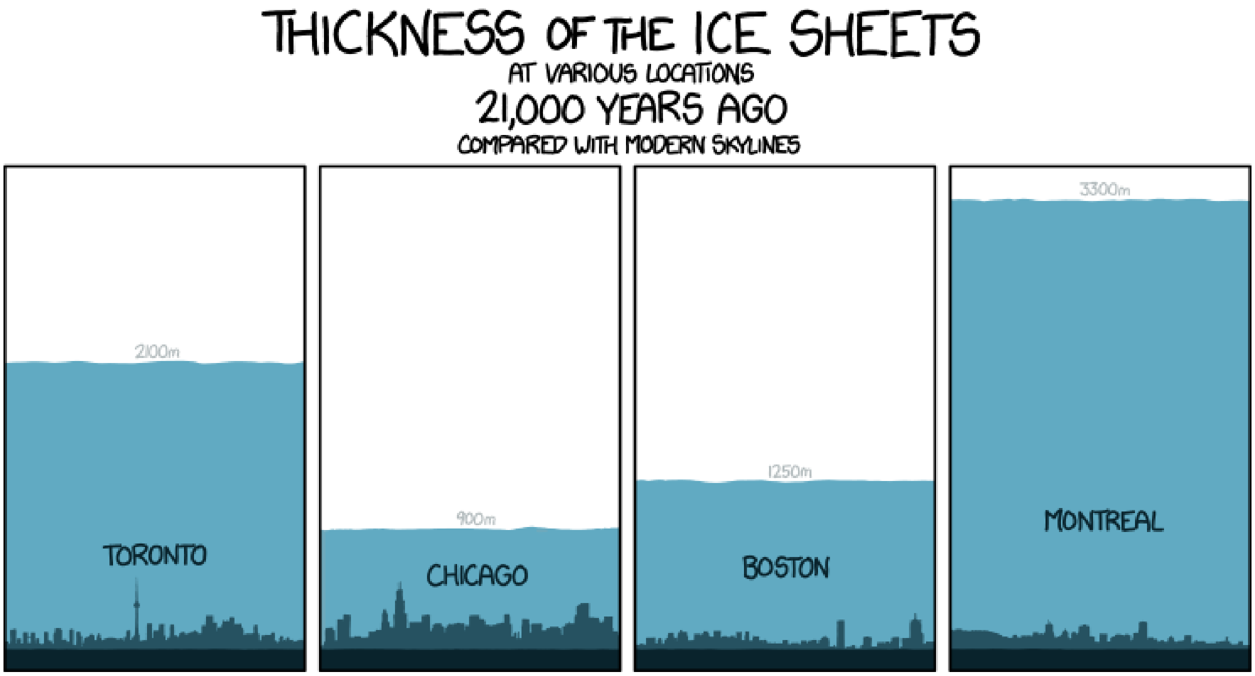
Lesson 15: Strength in numbers

Numbers are an essential part of our everyday life. Large numbers, however, aren't something most of us are too familiar with. The largest numbers we might encounter in everyday life are in the range of millions, billions, or trillions. We might read about millions of people in poverty, billions of dollars spent on bank bailouts, and trillions of national debt. Even though it's hard to make sense of these headlines, we are somewhat comfortable with the size of those numbers.

Although we might seem comfortable with billions and trillions, our intuition already starts to fail with numbers of this magnitude. Do you have an intuition how long you would have to wait for a million/billion/trillion seconds to pass? If you are anything like me, you are lost without actually crunching the numbers.

Let's take a closer look at this example: the difference between each is an increase by three orders of magnitude: 10^6, 10^9, 10^{12}. Thinking about seconds is not very useful, so let's translate this into something we can wrap our head around:

- 10^6: One million seconds was 1½ weeks ago.
- 10^9: One billion seconds was almost 32 years ago.
- 10^{12}: One trillion seconds ago Manhattan was covered under a thick layer of ice.



About 1 trillion seconds ago. Source: xkcd #1125

As soon as we enter the beyond-astronomical realm of modern cryptography, our intuition fails catastrophically. Bitcoin is built around large numbers and the virtual impossibility of guessing them. These numbers are way, way larger than anything we might encounter in day-to-day life. Many orders of magnitude larger. Understanding how large these numbers truly are is essential to understanding Bitcoin as a whole.

Let's take SHA-256, one of the hash functions used in Bitcoin, as a concrete example. It is only natural to think about 256 bits as "two hundred fifty-six," which isn't a large number at all. However, the number in SHA-256 is talking about orders of magnitude—something our brains are not well-equipped to deal with.

While bit length is a convenient metric, the true meaning of 256-bit security is lost in translation. Similar to the millions (10^6) and billions (10^9) above, the number in SHA-256 is about orders of magnitude (2^{256}).

So, how strong is SHA-256, exactly?

"SHA-256 is very strong. It's not like the incremental step from MD5 to SHA1. It can last several decades unless there's some massive breakthrough attack."

—Satoshi Nakamoto

Let's spell things out. 2^{256} equals the following number:

115 quattuorvigintillion 792 trevigintillion 89 duovigintillion 237 unvigintillion 316 vigintillion 195 novemdecillion 423 octodecillion 570 septendecillion 985

sexdecillion 8 quindecillion 687 quattuordecillion 907 tredecillion 853 duodecillion 269 undecillion 984 decillion 665 nonillion 640 octillion 564 septillion 39 sextillion 457 quintillion 584 quadrillion 7 trillion 913 billion 129 million 639 thousand 936.

That's a lot of nonillions! Wrapping your head around this number is pretty much impossible. There is nothing in the physical universe to compare it to. It is far larger than the number of atoms in the observable universe. The human brain simply isn't made to make sense of it.

One of the best visualizations of the true strength of SHA-256 is the following video by Grant Sanderson. Aptly named "How secure is 256 bit security?" it beautifully shows how large a 256-bit space is. Do yourself a favor and take the five minutes to watch it. As all other 3Blue1Brown videos it is not only fascinating but also exceptionally well made. Warning: You might fall down a math rabbit hole.

Answer: Pretty secure.

Bruce Schneier used the physical limits of computation to put this number into perspective: even if we could build an optimal computer, which would use any provided energy to flip bits perfectly, build a Dyson sphere around our sun, and let it run for 100 billion billion years, we would still only have a 25% chance to find a needle in a 256-bit haystack.

"These numbers have nothing to do with the technology of the devices; they are the maximums that thermodynamics will allow. And they strongly imply that brute-force attacks against 256-bit keys will be infeasible until computers are built from something other than matter and occupy something other than space."

—Bruce Schneier

It is hard to overstate the profoundness of this. Strong cryptography inverts the power-balance of the physical world we are so used to. Unbreakable things do not exist in the real world. Apply enough force, and you will be able to open any door, box, or treasure chest.

Bitcoin's treasure chest is very different. It is secured by strong cryptography, which does not give way to brute force. And as long as the underlying mathematical assumptions hold, brute force is all we have. Granted, there is also the option of a global $5 wrench attack. But torture won't work for all bitcoin addresses, and the cryptographic walls of bitcoin will defeat brute force attacks. Even if you come at it with the force of a thousand suns. Literally.

This fact and its implications were poignantly summarized in the call to cryptographic arms: " *No amount of coercive force will ever solve a math problem."*

"It isn't obvious that the world had to work this way. But somehow the universe smiles on encryption."

—Julian Assange

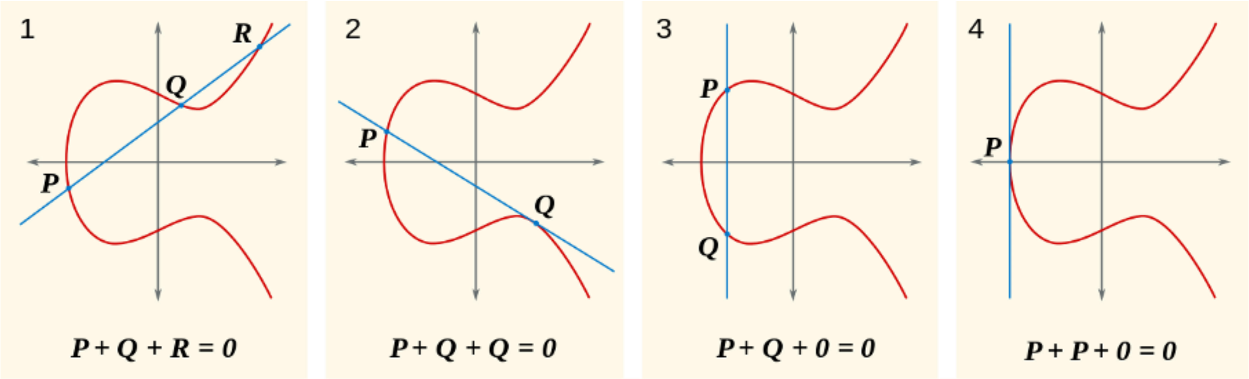
Nobody yet knows for sure if the universe's smile is genuine or not. It is possible that our assumption of mathematical asymmetries is wrong and we find that P actually equals NP, or we find surprisingly quick solutions to specific problems which we currently assume to be hard. If that should be the case, cryptography as we know it will cease to exist, and the implications would most likely change the world beyond recognition.

"Vires in Numeris" = "Strength in Numbers"

—epii

Vires in numeris is not only a catchy motto used by bitcoiners. The realization that there is an unfathomable strength to be found in numbers is a profound one. Understanding this, and the inversion of existing power balances which it enables changed my view of the world and the future which lies ahead of us.

One direct result of this is the fact that you don't have to ask anyone for permission to participate in Bitcoin. There is no page to sign up, no company in charge, no government agency to send application forms to. Simply generate a large number and you are pretty much good to go. The central authority of account creation is mathematics. And God only knows who is in charge of that.



Elliptic curve examples (cc-by-sa Emmanuel Boutet)

Bitcoin is built upon our best understanding of reality. While there are still many open problems in physics, computer science, and mathematics, we are pretty sure about some things. That there is an asymmetry between finding solutions and validating the correctness of these solutions is one such thing. That computation needs energy is another one. In other words: finding a needle in a haystack is harder than checking if the pointy thing in your hand is indeed a needle or not. And finding the needle takes work.

The vastness of Bitcoin's address space is truly mind-boggling. The number of private keys even more so. It is fascinating how much of our modern world boils down to the improbability of finding a needle in an unfathomably large haystack. I am now more aware of this fact than ever.

Bitcoin taught me that there is strength in numbers.

Lesson 16: Reflections on "Don't Trust, Verify"

Bitcoin aims to replace, or at least provide an alternative to, conventional currency. Conventional currency is bound to a centralized authority, no matter if we are talking about legal tender like the US dollar or modern monopoly money like Fortnite's V-Bucks. In both examples, you are bound to trust the central authority to issue, manage and circulate your money. Bitcoin unties this bound, and the main issue Bitcoin solves is the issue of *trust*.

"The root problem with conventional currency is all the trust that's required to make it work. [...] What is needed is an electronic payment system based on cryptographic proof instead of trust" —Satoshi Nakamoto

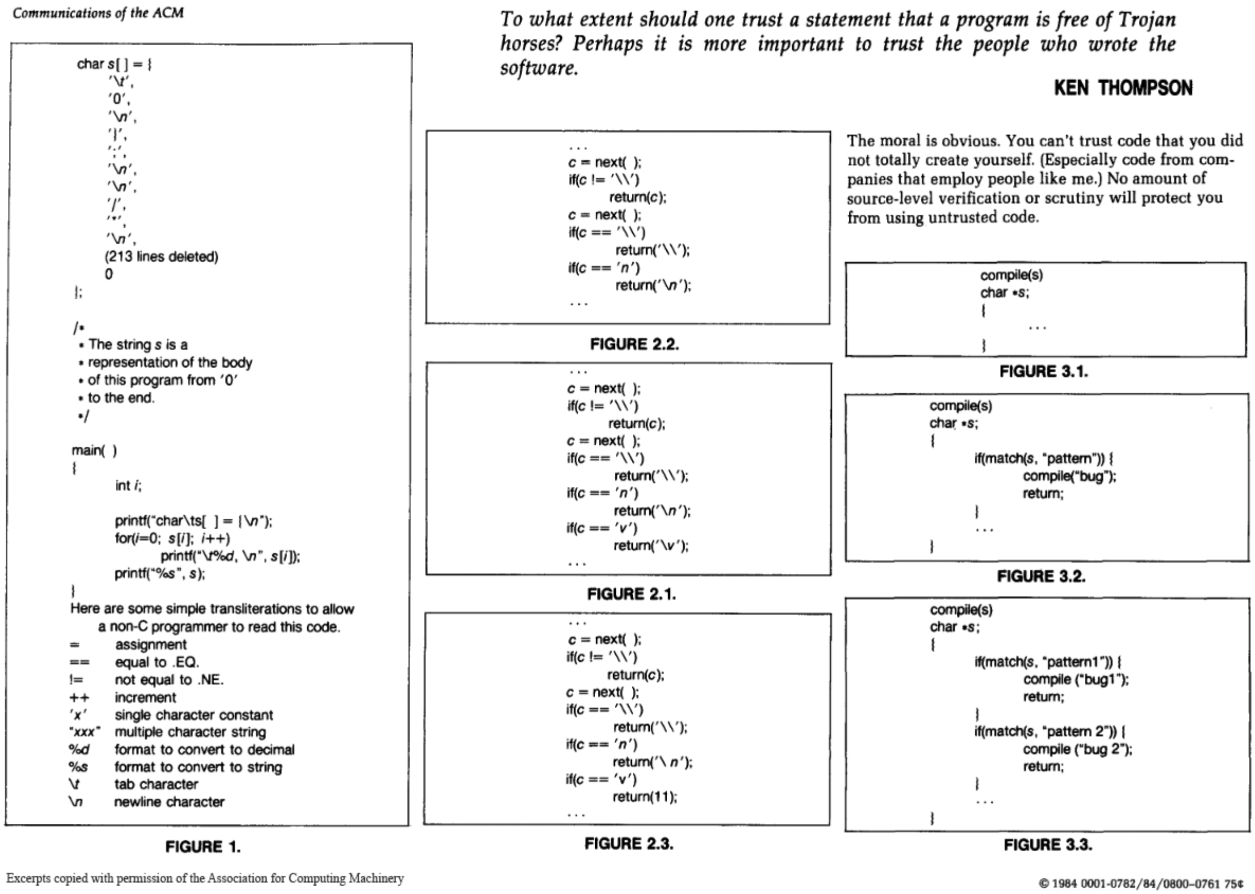
Bitcoin solves the problem of trust by being completely decentralized, with no central server or trusted parties. Not even trusted *third* parties, but trusted parties, period. When there is no central authority, there simply *is* no-one to trust. Complete decentralization is the innovation. It is the root of Bitcoin's resilience, the reason why it is still alive. Decentralization is also why we have mining, nodes, hardware wallets, and yes, the blockchain. The only thing you have to "trust" is that our understanding of mathematics and physics isn't totally off and that the majority of miners act honestly (which they are incentivized to do).

While the regular world operates under the assumption of *"trust, but verify,"* Bitcoin operates under the assumption of *"don't trust, verify."_Satoshi made the importance of removing trust very clear in both the introduction as well as the conclusion of the Bitcoin whitepaper.*

"Conclusion: We have proposed a system for electronic transactions without relying on trust." —Satoshi Nakamoto

Note that "without relying on trust" is used in a very specific context here. We are talking about trusted third parties, i.e. other entities which you trust to produce, hold, and process your money. It is assumed, for example, that you can trust your computer.

As Ken Thompson showed in his Turing Award lecture, trust is an extremely tricky thing in the computational world. When running a program, you have to trust all kinds of software (and hardware) which, in theory, could alter the program you are trying to run in a malicious way. As Thompson summarized in his *Reflections on Trusting Trust*: “The moral is obvious. You can’t trust code that you did not totally create yourself.”



Communications of the ACM

```
char s[ ] = {
        '\t',
        '0',
        '\n',
        '}',
        ';',
        '\n',
        '\n',
        '/',
        '*',
        '\n',
        (213 lines deleted)
        0
};

/*
 * The string s is a
 * representation of the body
 * of this program from '0'
 * to the end.
 */

main( )
{
        int i;

        printf("char\ts[ ] = {\n");
        for(i=0; s[i]; i++)
                printf("\t%d, \n", s[i]);
        printf("%s", s);
}
Here are some simple transliterations to allow
     a non-C programmer to read this code.
=       assignment
==      equal to .EQ.
!=      not equal to .NE.
++      increment
'x'     single character constant
"xxx"   multiple character string
%d      format to convert to decimal
%s      format to convert to string
\t      tab character
\n      newline character
```

FIGURE 1.

Excerpts copied with permission of the Association for Computing Machinery

To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software.

KEN THOMPSON

```
...
c = next( );
if(c != '\\')
        return(c);
c = next( );
if(c == '\\')
        return('\\');
if(c == 'n')
        return('\n');
...
```

FIGURE 2.2.

```
...
c = next( );
if(c != '\\')
        return(c);
c = next( );
if(c == '\\')
        return('\\');
if(c == 'n')
        return('\n');
if(c == 'v')
        return('\v');
...
```

FIGURE 2.1.

```
...
c = next( );
if(c != '\\')
        return(c);
c = next( );
if(c == '\\')
        return('\\');
if(c == 'n')
        return('\ n');
if(c == 'v')
        return(11);
...
```

FIGURE 2.3.

The moral is obvious. You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me.) No amount of source-level verification or scrutiny will protect you from using untrusted code.

```
compile(s)
char *s;
{
        ...
}
```

FIGURE 3.1.

```
compile(s)
char *s;
{
        if(match(s, "pattern")) {
                compile("bug");
                return;
        }
        ...
}
```

FIGURE 3.2.

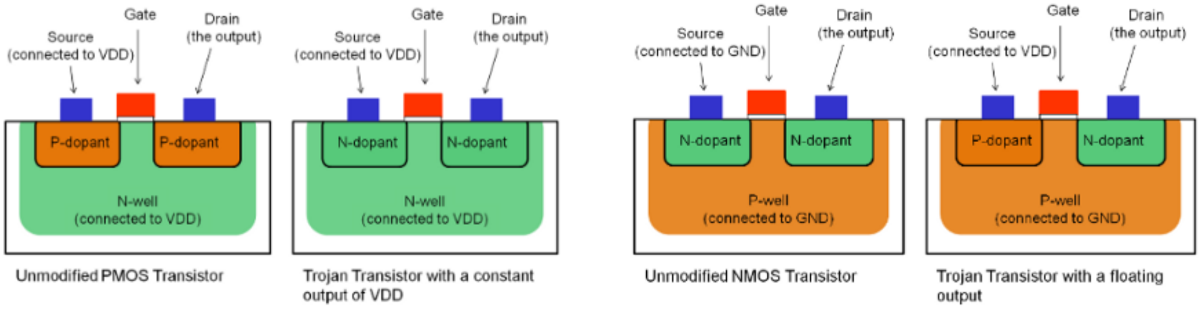
```
compile(s)
char *s;
{
        if(match(s, "pattern1")) {
                compile ("bug1");
                return;
        }
        if(match(s, "pattern 2")) {
                compile ("bug 2");
                return;
        }
        ...
}
```

FIGURE 3.3.

Thompson demonstrated that even if you have access to the source code, your compiler—or any other program-handling program or hardware—could be compromised and detecting this backdoor would be very difficult. Thus, in practice, a truly *trustless* system does not exist. You would have to create all your software *and* all your hardware (assemblers, compilers, linkers, etc.) from scratch, without the aid of any external software or software-aided machinery.

“If you wish to make an apple pie from scratch, you must first invent the universe.” —Carl Sagan

The Ken Thompson Hack is a particularly ingenious and hard-to-detect backdoor, so let’s take a quick look at a hard-to-detect backdoor which works without modifying any software. Researchers found a way to compromise security-critical hardware by altering the polarity of silicon impurities. Just by changing the physical properties of the stuff that computer chips are made of they were able to compromise a cryptographically secure random number generator. Since this change can’t be seen, the backdoor can’t be detected by optical inspection, which is one of the most important tamper-detection mechanism for chips like these.



(a) p-MOS Transistor (b) n-MOS Transistor

Stealthy Dopant-Level Hardware Trojans by Becker, Regazzoni, Paar, Burleson

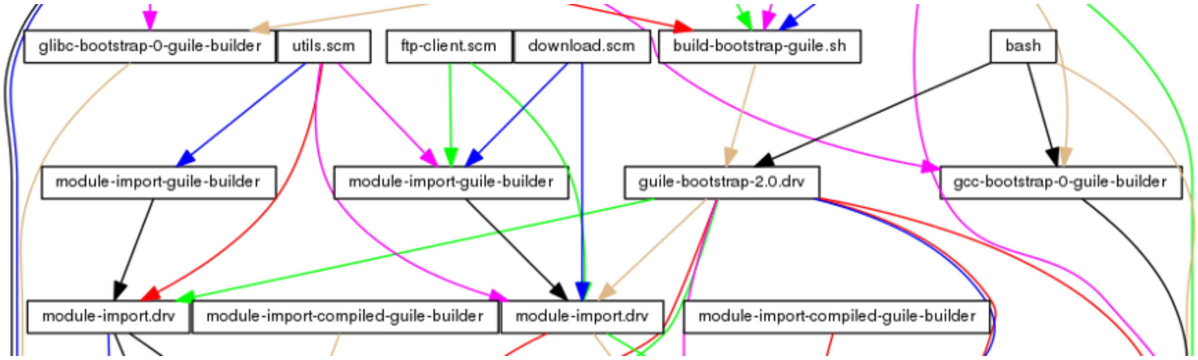
Sounds scary? Well, even if you would be able to build everything from scratch, you would still have to trust the underlying mathematics. You would have to trust that secp256k1 is an elliptic curve without backdoors. Yes, malicious backdoors can be inserted in the mathematical foundations of cryptographic functions and arguably this has already happened at least once. There are good reasons to be paranoid, and the fact that everything from your hardware, to your software, to the elliptic curves used can have backdoors are some of them.

“Don’t trust. Verify.”

The above examples should illustrate that *trustless* computing is utopic. Bitcoin is probably the one system which comes closest to this utopia, but still, it is *trust-minimized*—aiming to remove trust wherever possible. Arguably, the chain-of-trust is neverending, since you will also have to trust that computation requires energy, that P does not equal NP, and that you are actually in base reality and not emprisoned in a simulation by malicious actors.

Developers are working on tools and procedures to minimize any remaining trust even further. For example, Bitcoin developers created Gitian, which is a software distribution method to create deterministic builds. The idea is that if multiple developers are able to reproduce identical binaries, the chance of malicious tampering is reduced. Fancy backdoors aren’t the only attack vector. Simple blackmail or extortion are real threats as well. As in the main protocol, decentralization is used to minimize trust.

Various efforts are being made to improve upon the chicken-and-egg problem of bootstrapping which Ken Thompson’s hack so brilliantly pointed out. One such effort is Guix (pronounced *geeks*), which uses functionally declared package management leading to bit-for-bit reproducible builds by design. The result is that you don’t have to trust any software-providing servers anymore since you can verify that the served binary was not tampered with by rebuilding it from scratch. As of this writing, a pull-request is in progress to integrate Guix into the Bitcoin build process.


glibc-bootstrap-0-guile-builder
utils.scm
ftp-client.scm
download.scm
build-bootstrap-guile.sh
bash
module-import-guile-builder
module-import-guile-builder
guile-bootstrap-2.0.drv
gcc-bootstrap-0-guile-builder
module-import.drv
module-import-compiled-guile-builder
module-import.drv
module-import-compiled-guile-builder

Which came first, the chicken or the egg?

Luckily, Bitcoin doesn't rely on a single algorithm or piece of hardware. One effect of Bitcoin's radical decentralization is a distributed security model. Although the backdoors described above are not to be taken lightly, it is unlikely that every software wallet, every hardware wallet, every cryptographic library, every node implementation, and every compiler of every language is compromised. Possible, but highly unlikely.

Note that you can generate a private key without relying on any computational hardware or software. You can flip a coin a couple of times, although depending on your coin and tossing style this source of randomness might not be sufficiently random. There is a reason why storage protocols like Glacier advise to use casino-grade dice as one of two sources of entropy.

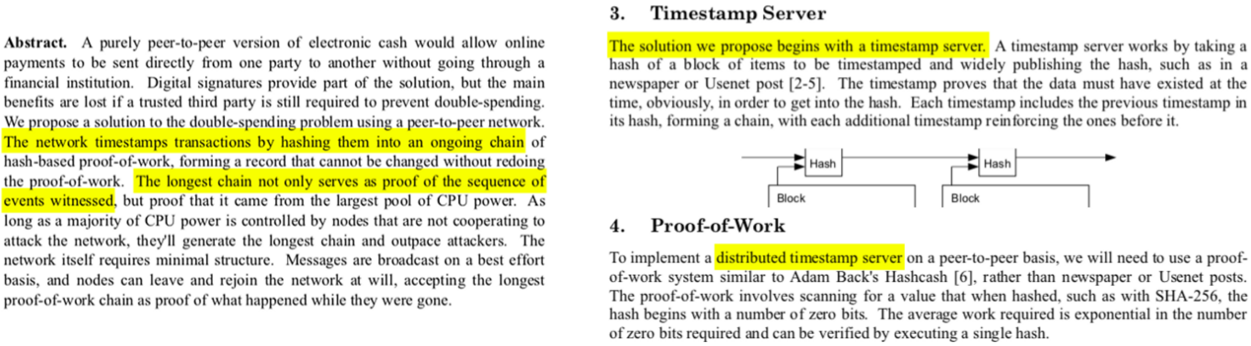
Bitcoin forced me to reflect on what trusting nobody actually entails. It raised my awareness of the bootstrapping problem, and the implicit chain-of-trust in developing and running software. It also raised my awareness of the many ways in which software and hardware can be compromised.

Bitcoin taught me not to trust, but to verify.

Lesson 17: Telling time takes work

It is often said that bitcoins are mined because thousands of computers work on solving *very complex* mathematical problems. Certain problems are to be solved, and if you compute the right answer, you "produce" a bitcoin. While this simplified view of bitcoin mining might be easier to convey, it does miss the point somewhat. Bitcoins aren't produced or created, and the whole ordeal is not really about solving particular math problems. Also, the math isn't particularly complex. What is complex is *telling the time* in a decentralized system.

As outlined in the whitepaper, the proof-of-work system (aka mining) is a way to implement a distributed timestamp server.



Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

3. Timestamp Server

The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.

4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

Excerpts from the whitepaper. Did someone say timechain?

When I first learned how Bitcoin works I also thought that proof-of-work is inefficient and wasteful. After a while, I started to shift my perspective on Bitcoin's energy consumption. It seems that proof-of-work is still widely misunderstood today, in the year 10 AB (after Bitcoin).

Bitcoin's Energy Consumption *A shift in perspective*

Since the problems to be solved in proof-of-work are made up, many people seem to believe that it is *useless* work. If the focus is purely on the computation, this is an understandable conclusion. But Bitcoin isn't about computation. It is about *independently agreeing on the order of things.*

Proof-of-work is a system in which everyone can validate what happened and in what order it happened. This independent validation is what leads to consensus, an individual agreement by multiple parties about who owns what.

In a radically decentralized environment, we don't have the luxury of absolute time. Any clock would introduce a trusted third party, a central point in the system which had to be relied upon and could be attacked. "Timing is the root problem," as Grisha Trubetskoy points out. And Satoshi brilliantly solved this problem by implementing a decentralized clock via a proof-of-work blockchain. Everyone agrees beforehand that the chain with the most cumulative work is the source of truth. It is per definition what actually happened. This agreement is what is now known as Nakamoto consensus.

"The network timestamps transactions by hashing them into an ongoing chain [which] serves as proof of the sequence of events witnessed" —Satoshi Nakamoto

Without a consistent way to tell the time, there is no consistent way to tell before from after. Reliable ordering is impossible. As mentioned above, Nakamoto consensus is Bitcoin's way to consistently tell the time. The system's incentive structure produces a probabilistic, decentralized clock, by utilizing both greed and self-interest of competing participants. The fact that this clock is imprecise is irrelevant because the order of events is eventually unambiguous and can be verified by anyone.

Thanks to proof-of-work, both the work *and* the validation of the work are radically decentralized. Everyone can join and leave at will, and everyone can validate everything at all times. Not only that, but everyone can validate the state of the system *individually*, without having to rely on anyone else for validation.

Understanding proof-of-work takes time. It is often counter-intuitive, and while the rules are simple, they lead to quite complex phenomena. For me, shifting my perspective on mining helped. Useful, not useless. Validation, not computation. Time, not blocks.

Bitcoin taught me that telling the time is tricky, especially if you are decentralized.

Lesson 18: Move slowly and don’t break things

It might be a dead mantra, but “move fast and break things” is still how much of the tech world operates. The idea that it doesn’t matter if you get things right the first time is a basic pillar of the *fail early, fail often* mentality. Success is measured in growth, so as long as you are growing everything is fine. If something doesn’t work at first you simply pivot and iterate. In other words: throw enough shit against the wall and see what sticks.

Bitcoin is very different. It is different by design. It is different out of necessity. As Satoshi pointed out, e-currency has been tried many times before, and all previous attempts have failed because there was a head which could be cut off. The novelty of Bitcoin is that it is a beast without heads.

“A lot of people automatically dismiss e-currency as a lost cause because of all the companies that failed since the 1990’s. I hope it’s obvious it was only the centrally controlled nature of those systems that doomed them.” —Satoshi Nakamoto

One consequence of this radical decentralization is an inherent resistance to change. “Move fast and break things” does not and will never work on the Bitcoin base layer. Even if it would be desirable, it wouldn’t be possible without convincing *everyone* to change their ways. That’s distributed consensus. That’s the nature of Bitcoin.

“The nature of Bitcoin is such that once version 0.1 was released, the core design was set in stone for the rest of its lifetime.” —Satoshi Nakamoto

This is one of the many paradoxical properties of Bitcoin. We all came to believe that anything which is software can be changed easily. But the nature of the beast makes changing it bloody hard.

As Hasu beautifully shows in Unpacking Bitcoin's Social Contract, changing the rules of Bitcoin is only possible by *proposing* a change, and consequently *convincing* all users of Bitcoin to adopt this change. This makes Bitcoin very resilient to change, even though it is software.

This resilience is one of the most important properties of Bitcoin. Critical software systems have to be antifragile, which is what the interplay of Bitcoin's social layer and its technical layer guarantees. Monetary systems are adversarial by nature, and as we have known for thousands of years solid foundations are essential in an adversarial environment.

"The rain came down, the floods came, and the winds blew, and beat on that house; and it didn't fall, for it was founded on the rock." —Matthew 7:24–27

Arguably, in this parable of the wise and the foolish builders Bitcoin isn't the house. It is the rock. Unchangeable, unmoving, providing the foundation for a new financial system.

Just like geologists, who know that rock formations are always moving and evolving, one can see that Bitcoin is always moving and evolving as well. You just have to know where to look and how to look at it.

The introduction of pay to script hash and segregated witness are proof that Bitcoin's rules can be changed if enough users are convinced that adopting said change is to the benefit of the network. The latter enabled the development of the lightning network, which is one of the houses being built on Bitcoin's solid foundation. Future upgrades like Schnorr signatures will enhance efficiency and privacy, as well as scripts (read: smart contracts) which will be indistinguishable from regular transactions thanks to Taproot. Wise builders do indeed build on solid foundations.

Satoshi wasn't only a wise builder technologically. He also understood that it would be necessary to make wise decisions ideologically.

"Being open source means anyone can independently review the code. If it was closed source, nobody could verify the security. I think it's essential for a program of this nature to be open source." —Satoshi Nakamoto

Openness is paramount to security and inherent in open source and the free software movement. As Satoshi pointed out, secure protocols and the code which implements them have to be open—there is no security through obscurity. Another benefit is again related to decentralization: code which can be run, studied, modified, copied, and distributed freely ensures that it is spread far and wide.

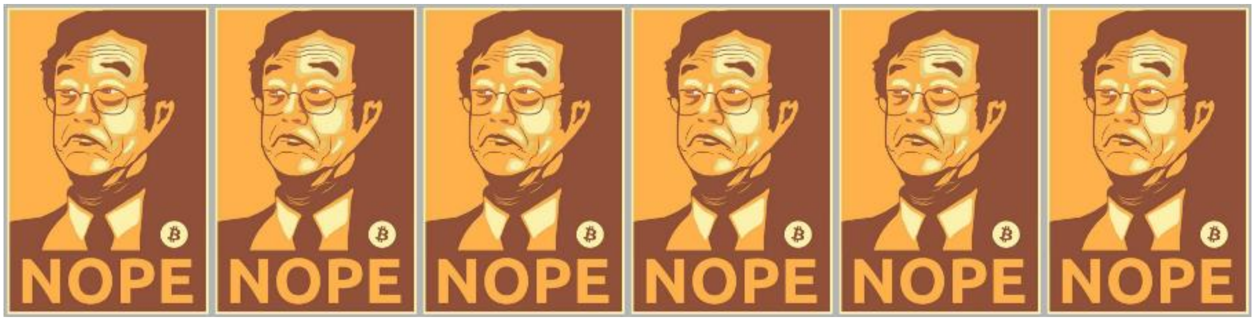
The radically decentralized nature of Bitcoin is what makes it move slowly and deliberately. A network of nodes, each run by a sovereign individual, is inherently resistant to change—malicious or not. With no way to force updates upon users the only way to introduce changes is by slowly convincing each and every one of those individuals to adopt a change. This non-central process of introducing and deploying changes is what makes the network incredibly resilient to malicious changes. It is also what makes fixing broken things more difficult than in a centralized environment, which is why everyone tries not to break things in the first place.

Bitcoin taught me that moving slowly is one of its features, not a bug.

Lesson 19: Privacy is not dead

If pundits are to believed, privacy has been dead since the 80ies. The pseudonymous invention of Bitcoin and other events in recent history show that this is not the case. Privacy is alive, even though it is by no means easy to escape the surveillance state.

Satoshi went through great lengths to cover up his tracks and conceal his identity. Ten years later, it is still unknown if Satoshi Nakamoto was a single person, a group of people, male, female, or a time-traveling AI which bootstrapped itself to take over the world. Conspiracy theories aside, Satoshi chose to identify himself to be a Japanese male, which is why I don't assume but respect his chosen gender and refer to him as *he*.



"I am not Dorian Nakamoto."

Whatever his real identity might be, Satoshi was successful in hiding it. He set an encouraging example for everyone who wishes to remain anonymous: it is possible to have privacy online.

"Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on."

—Edward Snowden

Satoshi wasn't the first pseudonymous or anonymous inventor, and he won't be the last. Some have directly imitated this pseudonymous publication style, like Tom Elvis Yedusor of MimbleWimble fame, while others have published advanced mathematical proofs while remaining completely anonymous.

It is a strange new world we are living in. A world where identity is optional, contributions are accepted based on merit, and people can collaborate and transact freely. It will take some adjustment to get comfortable with these new paradigms, but I strongly believe that all of this has the potential to change the world for the better.

We should all remember that privacy is a fundamental human right. And as long as people exercise and defend these rights the battle for privacy is far from over. Bitcoin taught me that privacy is not dead.

Lesson 20: Cypherpunks write code

Like many great ideas, Bitcoin didn't come out of nowhere. It was made possible by utilizing and combining many innovations and discoveries in mathematics, physics, computer science, and other fields. While undoubtedly a genius, Satoshi wouldn't have been able to invent Bitcoin without the giants on whose shoulders he was standing on.

"He who only wishes and hopes does not interfere actively with the course of events and with the shaping of his own destiny."

—Ludwig Von Mises

One of these giants is Eric Hughes, one of the founders of the cypherpunk movement and author of the cypherpunk manifesto. It's hard to imagine that Satoshi wasn't influenced by this manifesto. It speaks of many things which Bitcoin enables and utilizes, such as direct and private transactions, electronic money and cash, anonymous systems, and defending privacy with cryptography and digital signatures.

"Privacy is necessary for an open society in the electronic age. […] Since we desire privacy, we must ensure that each party to a transaction have knowledge only of that which is directly necessary for that transaction. […]

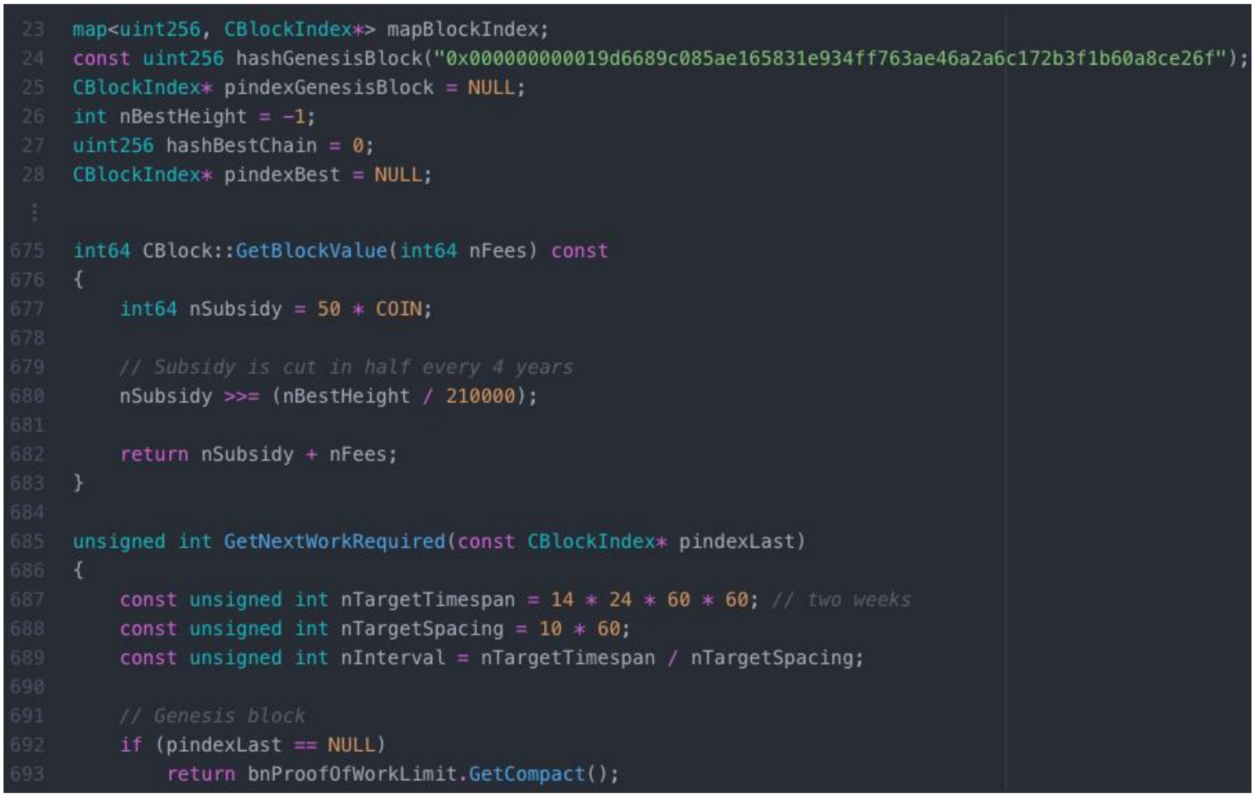
Therefore, privacy in an open society requires anonymous transaction systems. Until now, cash has been the primary such system. An anonymous transaction system is not a secret transaction system. […]

We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money.

Cypherpunks write code."

Cypherpunks do not find comfort in hopes and wishes. They actively interfere with the course of events and shape their own destiny. Cypherpunks write code.

Thus, in true cypherpunk fashion, Satoshi sat down and started to write code. Code which took an abstract idea and proved to the world that it actually worked. Code which planted the seed of a new economic reality. Thanks to this code, everyone can verify that this novel system actually works, and every 10 minutes or so Bitcoin proofs to the world that it is still living.



```
map<uint256, CBlockIndex*> mapBlockIndex;
const uint256 hashGenesisBlock("0x000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f");
CBlockIndex* pindexGenesisBlock = NULL;
int nBestHeight = -1;
uint256 hashBestChain = 0;
CBlockIndex* pindexBest = NULL;
⋮

int64 CBlock::GetBlockValue(int64 nFees) const
{
    int64 nSubsidy = 50 * COIN;

    // Subsidy is cut in half every 4 years
    nSubsidy >>= (nBestHeight / 210000);

    return nSubsidy + nFees;
}

unsigned int GetNextWorkRequired(const CBlockIndex* pindexLast)
{
    const unsigned int nTargetTimespan = 14 * 24 * 60 * 60; // two weeks
    const unsigned int nTargetSpacing = 10 * 60;
    const unsigned int nInterval = nTargetTimespan / nTargetSpacing;

    // Genesis block
    if (pindexLast == NULL)
        return bnProofOfWorkLimit.GetCompact();
```

Code excerpts from Bitcoin version 0.1.0

To make sure that his innovation transcends fantasy and becomes reality, Satoshi wrote code to implement his idea before he wrote the whitepaper. He also made sure not to delay any release forever. After all, “there’s always going to be one more thing to do.”

“I had to write all the code before I could convince myself that I could solve every problem, then I wrote the paper.”

—Satoshi Nakamoto

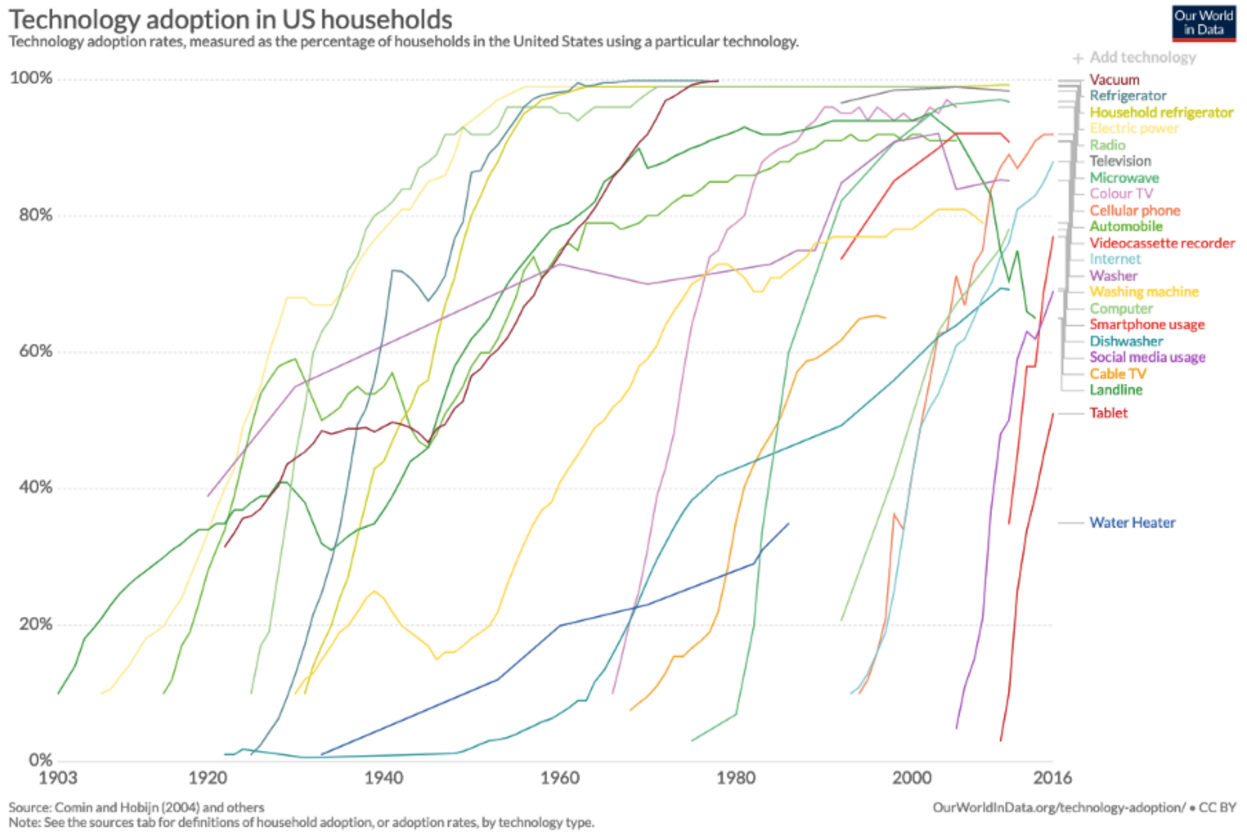
In today’s world of endless promises and doubtful execution, an exercise in dedicated building was desperately needed. Be deliberate, convince yourself that you can actually solve the problems, and implement the solutions. We should all aim to be a bit more cypherpunk.

Bitcoin taught me that cypherpunks write code.

Lesson 21: Metaphors for Bitcoin’s future

In the last couple of decades, it became apparent that technological innovation does not follow a linear trend. Whether you believe in the technological singularity or not, it is undeniable that progress is exponential in many fields. Not only that, but the rate at which technologies are being adopted is accelerating, and before you know it the bush in the local schoolyard is gone and your kids are using Snapchat instead. Exponential curves have the tendency to slap you in the face way before you see them coming.

Bitcoin is an exponential technology built upon exponential technologies. Our World in Data beautifully shows the rising speed of technological adoption, starting in 1903 with the introduction of landlines. Landlines, electricity, computers, the internet, smartphones; all follow exponential trends in price-performance and adoption. Bitcoin does too.



Source: Comin and Hobijn (2004) and others
Note: See the sources tab for definitions of household adoption, or adoption rates, by technology type.
OurWorldInData.org/technology-adoption/ • CC BY

Bitcoin is literally off the charts.

Bitcoin has not one but multiple network effects, all of which resulting in exponential growth patterns in their respective area: price, users, security, developers, market share, and adoption as global money.

Having survived its infancy, Bitcoin is continuing to grow every day in more aspects than one. Granted, the technology has not reached maturity yet. It might be in its adolescence. But if the technology is exponential, the path from obscurity to ubiquity is short.

Mobile phone, ca 1965 vs 2019.

In his 2003 TED talk, Jeff Bezos chose to use electricity as a metaphor for the web's future. All three phenomena—electricity, the internet, Bitcoin—are *enabling* technologies, networks which enable other things. They are infrastructure to be built upon, foundational in nature.

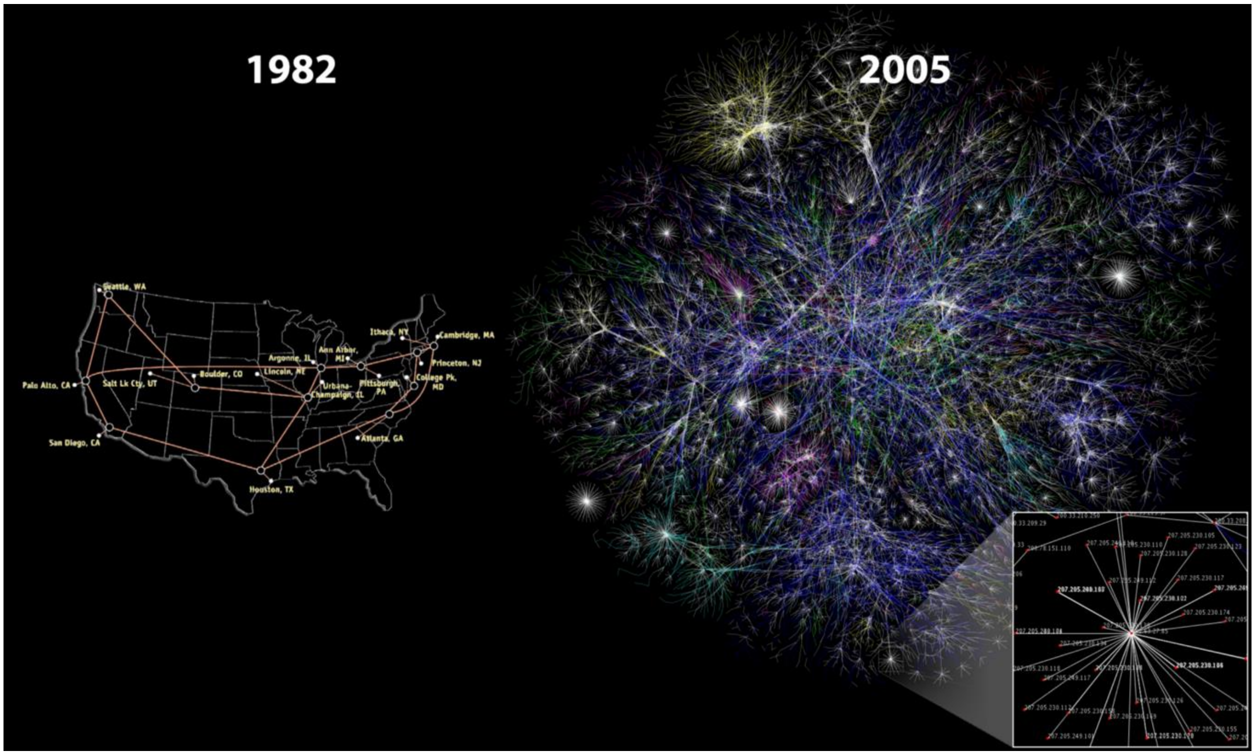
Electricity has been around for a while now. We take it for granted. The internet is quite a bit younger, but most people already take it for granted as well. Bitcoin is ten years old and has entered public consciousness during the last hype cycle. Only the earliest of adopters take it for granted. As more time passes, more and more people will recognize Bitcoin as something which simply is.

In 1994, the internet was still confusing and unintuitive. Watching this old recording of the Today Show makes it obvious that what feels natural and intuitive now actually wasn't back then. Bitcoin is still confusing and alien to most, but just like the internet is second nature for digital natives, spending and stacking sats will be second nature to the bitcoin natives of the future.

"The future is already here—it's just not very evenly distributed." —William Gibson

In 1995, about 15% of American adults used the internet. Historical data from the Pew Research Center shows how the internet has woven itself into all our lives. According to a consumer survey by Kaspersky Lab, 13% of respondents have used Bitcoin and its clones to pay for goods in 2018. While payments aren't the only use-case of bitcoin, it is some indication of where we are in Internet time: in the early- to mid-90s.

In 1997, Jeff Bezos stated in a letter to shareholders that "this is Day 1 for the Internet," recognizing the great untapped potential for the internet and, by extension, his company. Whatever day this is for Bitcoin, the vast amounts of untapped potential are clear to all but the most casual observer.

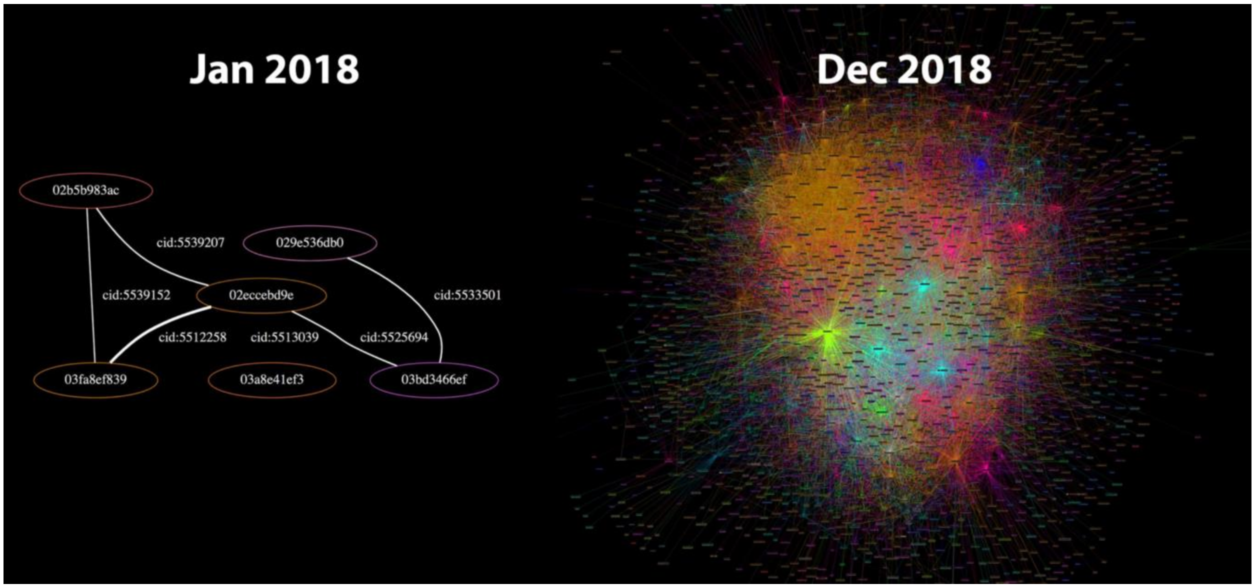


The internet, 1982 vs 2005. Source: cc-by Merit Network, Inc. and Barrett Lyon, Opte Project

Bitcoin's first node went online in 2009 after Satoshi mined the genesis block and released the software into the wild. His node wasn't alone for long. Hal Finney was one of the first people to pick up on the idea and join the network. Ten years later, as of this writing, more than 10.000 nodes are running bitcoin.

The protocol's base layer isn't the only thing growing exponentially. The lightning network, a second layer technology, is growing at an even faster rate.

In January 2018, the lightning network had 40 nodes and 60 channels. In April 2019, the network grew to more than 4000 nodes and around 40.000 channels. Keep in mind that this is still experimental technology where loss of funds can and does occur. Yet the trend is clear: thousands of people are reckless and eager to use it.



Lightning Network, January 2018 vs December 2018. Source: Jameson Lopp

To me, having lived through the meteoric rise of the web, the parallels between the internet and Bitcoin are obvious. Both are networks, both are exponential technologies, and both enable new possibilities, new industries, new ways of life. Just like electricity was the best metaphor to understand where the internet is heading, the internet might be the best metaphor to understand where bitcoin is heading. Or, in the words of Andreas Antonopoulos, Bitcoin is *The Internet of Money*. These metaphors are a great reminder that while history doesn't repeat itself, it often rhymes.

Exponential technologies are hard to grasp and often underestimated. Even though I have a great interest in such technologies, I am constantly surprised by the pace of progress and innovation. Watching the Bitcoin ecosystem grow is like watching the rise of the internet in fast-forward. It is exhilarating.

My quest of trying to make sense of Bitcoin has led me down the pathways of history in more ways than one. Understanding ancient societal structures, past monies, and how communication networks evolved were all part of the journey. From the handaxe to the smartphone, technology has undoubtedly changed our world many times over. Networked technologies are especially transformational: writing, roads, electricity, the internet. All of them changed the world. Bitcoin has changed mine and will continue to change the minds and hearts of those who dare to use it.

Bitcoin taught me that understanding the past is essential to understanding its future. A future which is just beginning.

Conclusion

Technology is all about the application of scientific knowledge to solve problems in the real world. Every technology has to make tradeoffs in terms of efficiency, cost, security, and many other properties. Just like there is no perfect solution to deriving a square from a circle, any solution to the problems which Bitcoin tries to solve will always be imperfect as well.

Da Vinci tried to solve the intractable problem of squaring a circle with the *Vitruvian Man*, which places a human right at the center of it. Bitcoin tries to solve the double spending problem with sovereign individuals, which places humans behind each node, effectively removing any concept of a center.

Bitcoin's headless nature shows us that seemingly simple concepts like creating accounts and agreeing on time require creative solutions in decentralized systems. It also shows that such systems can be astonishingly antifragile. How do you best kill something if the best point of attack is everywhere?

Even with all its quirks and seeming shortcomings, Bitcoin undoubtedly works. It keeps producing blocks roughly every ten minutes and does so beautifully. The longer Bitcoin continues to work, the more people will opt-in to use it.

"It's true that things are beautiful when they work. Art is function." —Giannina Braschi

Bitcoin is growing exponentially, blurring the line between disciplines. It isn't clear where the realm of pure technology ends and where another realm begins. I tried to differentiate the economic teachings of Bitcoin from the philosophical and the technological ones, which turned out more difficult than expected.

Just like in biological systems, removing one part seems to affect the whole. Maybe the most important lesson is that Bitcoin should be examined holistically, from multiple angles, if one would like to have a complete picture. Just like removing one part from Bitcoin destroys the whole (**cough** blockchain **cough**), examining parts of Bitcoin in isolation seems to taint the understanding of the whole system.

My journey continues, and as mentioned in part one, I think that any answer to the question *"What have you learned from Bitcoin?"* will always be incomplete. In any case, I've learned that the philosophy, economics, and technology of Bitcoin interact in a complex feedback loop, and I hope that these 21 lessons are just the beginning of what I've learned from Bitcoin.

Acknowledgments

- Once more, thanks to Arjun Balaji for the tweet which gave birth to this series.

- Thanks to Andreas M. Antonopoulos for all the educational material he has put out over the years.
- Thanks to Marty and Matt for guiding me through the rabbit hole and reminding us all to stay humble and stack sats.
- Thanks to Francis Pouliot for sharing his excitement about finding out about the timechain.
- Thanks to Brandon,Camilo,Daniel,Jannik, Michael, and Raphael for providing feedback to early drafts of this article
- Thanks to the countless authors and content producers who influenced my thinking on Bitcoin and the topics it touches. There are simply too many to name.
- And finally, thank *you* for reading this series. I hope you enjoyed it as much as I did enjoy writing it. Feel free to reach out to me on twitter. My DMs are open.

Further Reading

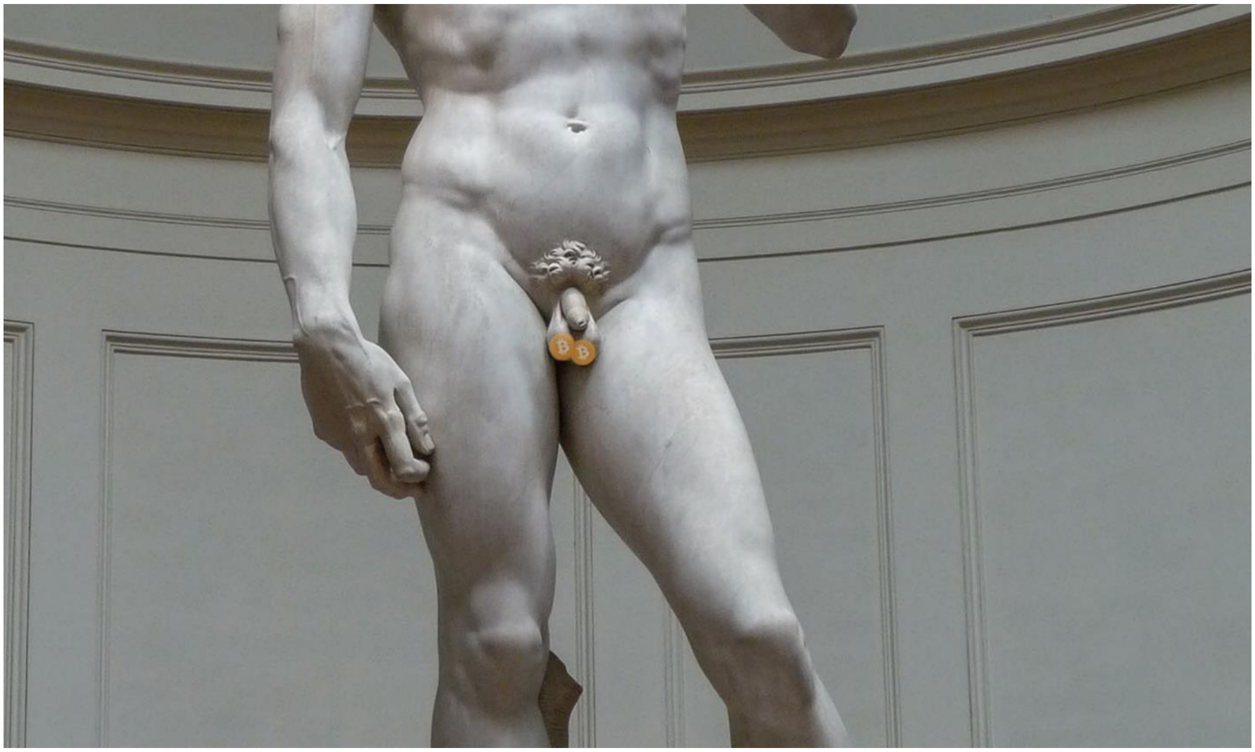
- *Bitcoin: A Peer-to-Peer Electronic Cash System* by Satoshi Nakamoto
- *Mastering Bitcoin* by Andreas Antonopoulos
- *The Internet of Money* by Andreas Antonopoulos
- *Inventing Bitcoin* by Yan Pritzker
- *Applied Cryptography* by Bruce Schneier
- *Reflections on Trusting Trust* by Ken Thompson
- *Cypherpunks* by Julian Assange with Jacob Appelbaum
- *The Anatomy of Proof-of-Work* by Hugo Nguyen
- *Blockchain Proof-of-Work Is a Decentralized Clock* by Gregory Trubetskoy
- *Unpacking Bitcoin's Social Contract* by Hasu
- *Why Bitcoin Matters* by Aleksandar Svetski
- *Guess My Bitcoin Private Key* by Michael Kerbleski

Bitcoin's Energy Consumption

A shift in perspective

By Gigi

June 10, 2018



You might have heard that Bitcoin wastes a tremendous amount of energy. You might also have heard that Bitcoin will use half a percent of the world's electric energy by the end of the year, the computations used for mining don't do anything useful, and if the current rate of growth continues it will suck up all the energy and we are all going to die.

I don't want to dispute the numbers or compare Bitcoin's energy usage to the current banking system. I simply want to offer a shift in perspective.

Bitcoin is Offensive

Bitcoin is a global, permission-less, censorship-resistant network. Its nature is inherently offensive. It offends governments, bankers, and central authorities alike. Hell, offending banks was the whole point of this experiment in the first place.

At first glance, Bitcoin is the worst database ever devised by mankind. In addition to being seemingly inefficient and slow, it is eating up computational resources at a mad pace and consumes as much energy as a small country.

“In comparison to modern distributed databases, blockchains are slow, ponderous, unnecessarily redundant and overly paranoid.”*Dhruv Bansal*

As Nick Szabo so succinctly put it: “Bitcoin offends the sensibilities of resource-conscious and performance-measure-maximizing engineers and businessmen alike.” It also offends our globally shared understanding that wasting energy is bad, and energy-efficiency is always good.

According to a recent paper “the Bitcoin network can be estimated to consume at least 2.55 gigawatts of electricity currently, and potentially 7.67 gigawatts in the future, making it comparable with countries such as Ireland (3.1 gigawatts) and Austria (8.2 gigawatts).”

It’s easy to be concerned, outraged or offended. *“Did you know Bitcoin uses as much energy as Austria? Baby cows are dying because of Bitcoin!”*

What-what the hell is a gigawatt?

To understand why all these gigawatts are necessary for the Bitcoin network to function properly and securely, we will have to take a closer look at the nuances of mining.

Mining Blocks and Coins

The name “mining” stems from the proposition that bitcoin has more in common with gold and other precious metals than paper money. Satoshi made this clear in one of his posts.

“In this sense, it’s more typical of a precious metal. Instead of the supply changing to keep the value the same, the supply is predetermined and the value changes.”*Satoshi Nakamoto*

Hence bitcoins are not printed, they are mined. Even though we talk about “mining bitcoins” all the time, keep in mind that it isn’t bitcoins which are mined. Blocks are mined, and miners are currently rewarded with *new* bitcoins if they find a valid block. Miners are rewarded because finding new blocks is inherently difficult. The system is set up in a way that the difficulty of finding a new block is adjusted automatically so that a new block is found every 10 minutes on average. Differentiating between "mining bitcoins" and "mining blocks" helps to point out a couple of things:

First, that the rate at which bitcoins are mined is decoupled from Bitcoin's energy use. If everyone would decide to double the energy spent on mining, the number of bitcoins mined would *not* double as a consequence. The rate of supply is fixed, no matter how much energy you choose to expend for mining.

Second, that miners do a lot more than bringing new bitcoins into existence: maintaining the security and continuity of the network, confirming transactions, and signaling their support or rejection of network changes, to name a few. Not all of these require an excessive amount of energy, which is one of the reasons why running a full node is important.

Third, that mining is not a fixed process. Both the mining reward and the mining difficulty are dynamic and thus will necessarily change over time.

Fourth, that mining is *supposed* to cost a lot of energy. It is computationally expensive by design, which is why Satoshi chose to reward people *extra* for expending this energy. It is the main ingredient of the Nakamoto Consensus. It is the work in proof-of-work. It is absolutely essential.

Without a closer look at the mining process, it is easy to confuse the energy-intensive process of finding valid blocks with "finding new bitcoins". From this perspective, it seems like all this electrical energy is transmuted into new bitcoins.

This is wrong.

The energy expended acts as a barrier which protects the public ledger. The creation of new bitcoins is just a side-effect.

Cryptographic Walls

Until very recently, securing something meant building a thick wall around whatever is deemed valuable. We all know how to do this, and we all agree that this is a sensible thing to do.

The new world of cryptocurrencies is unintuitive and weird. There are no physical walls to protect our money, no doors to access our vaults. Bitcoin's public ledger is secured by its collective hashing power: the sum of all energy expended to do the work in its proof-of-work chain.

Thus, we can think of Bitcoin's energy usage like a giant wall—a sort of electrical force-field—which secures all bitcoin balances of all users, now, and in the future.

It is hard to say how much energy has to be expended building these cryptographic walls. Financial systems are critical infrastructure, which is why most engineers in this space rightfully argue that security and stability are paramount. If Bitcoin will be the money of the future, it better be prepared to withstand high-impact, low-probability events.

How thick will these cryptographic walls need to be? Only time will tell. If Bitcoin is able to survive coordinated attacks by multiple state-level attackers, the walls were thick enough.

The End of Mining New Bitcoins

Bootstrapping a new network is difficult. It's like trying to convince everyone to buy a fax machine if you are the only guy in the world with a fax machine. It's really, *really* hard. As outlined above, Satoshi solved this problem by adding a block reward mechanism, which acts as (a) the controlled currency supply of Bitcoin and (b) an incentive for people to participate in the network to expand and secure the public ledger.

Expending energy is essential to provide security for this new financial network.

The current phase of "mining bitcoins", where miners are incentivized with a high reward, is a clever way to get the network started. In other words: everyone who is greedily mining bitcoins today is helping to bootstrap this new financial system, whether they realize it or not.

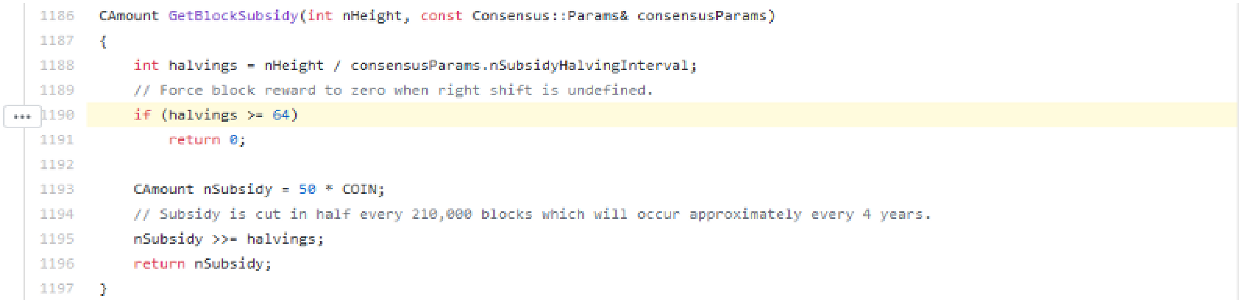
John Nash commenting on the game theoretical aspect of Satoshi's invention.

As mentioned above, Bitcoin's mining difficulty adjusts automatically, leading to a dynamic, self-correcting system. If mining—for whatever reason—gets more expensive, fewer people will mine at a profit, resulting in fewer people mining, lowering the mining difficulty. This, in turn, will make mining easier again and thus cheaper, which will incentivize more people to mine.

Over time, the financial incentive of running a mining operation will change. It follows that Bitcoin's energy consumption will change as well. The reason why change is inevitable is Bitcoin's block reward function which ensures a controlled, limited supply.

The block reward is halving every 210.000 blocks and will eventually reach zero, after 64 halvings. After the last of these halvings, miners will be left with transaction fees as the only financial reward for mining a new block.

In other words: The "mining of new bitcoins" will eventually stop. The mining of valid blocks will continue after that.

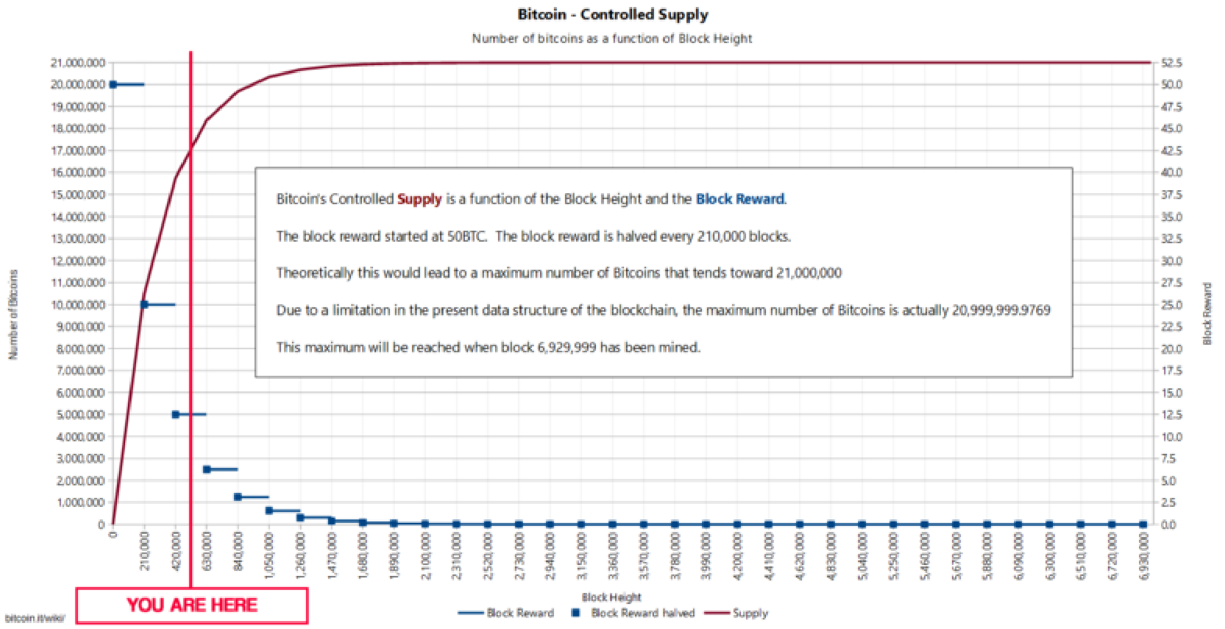


```
CAmount GetBlockSubsidy(int nHeight, const Consensus::Params& consensusParams)
{
    int halvings = nHeight / consensusParams.nSubsidyHalvingInterval;
    // Force block reward to zero when right shift is undefined.
    if (halvings >= 64)
        return 0;

    CAmount nSubsidy = 50 * COIN;
    // Subsidy is cut in half every 210,000 blocks which will occur approximately every 4 years.
    nSubsidy >>= halvings;
    return nSubsidy;
}
```

In Bitcoin, code truly is law.

One could argue that we are currently in the bitcoin equivalent of the Gold Rush, where the reward for mining as well as the future projected reward far outstrips the investment and energy costs. While it is hard to estimate how much security is enough security, a case could be made that the Bitcoin network is currently "hypersecured" as a side-effect of this Gold Rush.



Bitcoin - Controlled Supply

Number of bitcoins as a function of Block Height

Bitcoin's Controlled **Supply** is a function of the Block Height and the **Block Reward**.

The block reward started at 50BTC. The block reward is halved every 210,000 blocks.

Theoretically this would lead to a maximum number of Bitcoins that tends toward 21,000,000

Due to a limitation in the present data structure of the blockchain, the maximum number of Bitcoins is actually 20,999,999.9769

This maximum will be reached when block 6,929,999 has been mined.

bitcoin.it/wiki/

Bitcoin's controlled supply and block reward over time.

We are still in the early phases of Bitcoin's block reward phase, as the above graph shows.

Whether the adaption of bitcoin as a currency will be slow and steady, or exponential and parabolic, a continued exponential growth of energy consumption is very questionable. I would argue that excessive growth will give way to a somewhat sensible balance between security and energy consumption as the block reward approaches zero. Depending on the future value of bitcoin and the willingness of people to pay transaction fees, this balance might be leaning more towards security or more towards conservative use of energy.

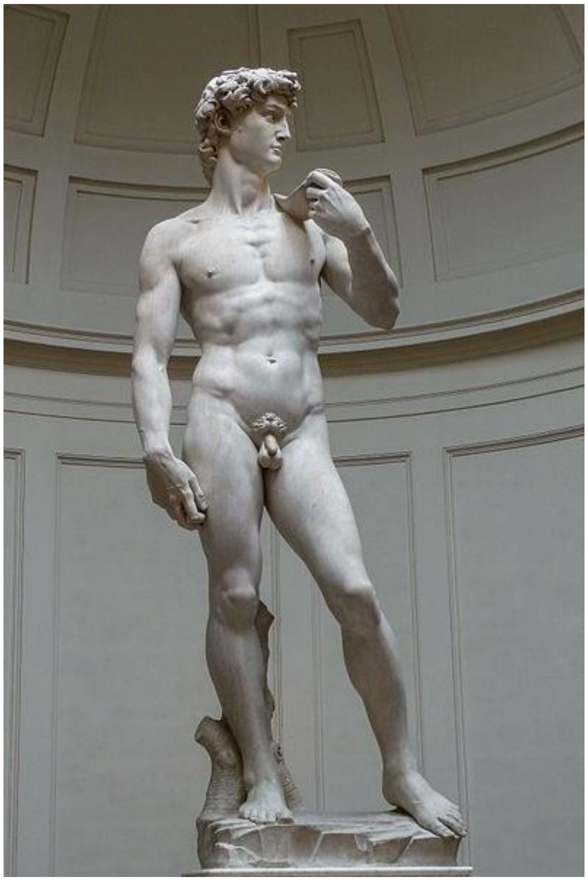
Modern Blocks of Marble

Once you wrap your head around proof-of-work, it becomes more and more clear that the energy consumption of the Bitcoin network is not a bug, it's a feature. As far as we know, you can't cheat the laws of thermodynamics. Given that we don't have any world-shattering breakthroughs in physics, mathematics and/or quantum computing, expending energy is the only way to flip bits, and flipping bits is the only way to mine new blocks.

Unfortunately, we don't have an intuitive understanding of this new cryptographic world (yet). Fully grasping the importance of proof-of-work requires a deep-dive into a multitude of topics. We lack concise, easy, elegant explanations and metaphors. Hugo Nguyen did a great job explaining how proof-of-work links the abstract, digital world of bitcoin to our physical world:

"By attaching energy to a block, we give it "form", allowing it to have real weight & consequences in the physical world."*Hugo Nguyen*

Proof-of-work is essentially a mechanism to easily check the truthfulness of the statement "I worked really hard to create this thing". From that perspective, our new and fancy computational blocks are a bit like blocks of marble, and proof-of-work is a bit like looking at a beautiful marble statue. It is immediately obvious that a lot of work went into creating the statue. Cheating is extremely hard, because creating such a glorious statue without actually doing the work is pretty much impossible. You can't throw a block of marble against a wall and everything which is not David will fall off. It's not impossible, but it is very, very, *very* unlikely. Instead, you have to chisel away at the marble, and you have to do it properly and with care. One might argue that this is one of the reasons why great artworks are so valuable: a lot of thought, care and work was expended to create them.



Oldschool proof-of-work by Michelangelo. Photo by Jörg Bittner Unna

It is similarly unlikely to find valid blocks without actually doing the work. Like an ugly half-haphazardly chiseled statue, an invalid block can be simply thrown away. When you see a *valid* block, however, you immediately *know* a lot of work went into it.

In both cases, the artifacts themselves, the statue and the valid block, are in itself the proof of work.

My point is that understanding the nature of proof-of-work and the incentives of mining valid blocks, as well as the security properties and thus the value of proof-of-work, might help to shift the perspective from "energy wasted" to "energy used for creating something valuable". Most people value beautiful marble statues. A rising number of people value a chain of valid blocks.

Security Through Purity

Another feature disguised as a bug is the randomness of bitcoin's proof-of-work. A common suggestion for improvement is that we could use all this electricity to do something else, something *truly* useful, like finding prime numbers or compute protein foldings, in addition to securing the network.

Again, this objection to Bitcoin's proof-of-work algorithm is rooted in the assumption that finding valid blocks is inherently useless. It is not.

While introducing a secondary reward for doing the work might seem like a good idea, it actually introduces a security risk.

The problem with doing something else—something that other people might consider useful—is that that splits the reward. It means that miners have two reasons for which they are mining.*Andreas M. Antonopoulos*

Splitting the reward can lead to a situation where "it's more worthwhile to do the secondary function that it is to do the primary function". Bitcoin will never have this problem. Bitcoin guarantees its security by the purity of its proof-of-work algorithm.

If someone figures out a more energy-efficient way to secure an open, decentralized, censorship-resistant, permission- and trustless network for value exchange—without compromising one of these qualities—this hypothetical future network will eventually dethrone Bitcoin, solving this supposed energy problem. And no, proof-of-stake is probably not the answer.

In the future, we might find something which is even *more* suited to be an anchor for truth than energy. Until we do, we should stick to something we are extremely confident in: the laws of thermodynamics; the energy required to do the work in proof-of-work.

Conclusion

I hope to have planted the seed for a shift in perspective: that spending energy on proof-of-work is not a waste, but a worthwhile endeavor.

Understanding mining and proof-of-work in more detail might help to convince some of Bitcoin's critics and shift the perspective from "inefficient and wasteful" to "secure and censorship-resistant". Pointing out these nuances might also be helpful to understand that Bitcoin's energy consumption most strongly correlates with the network's security, and not with the adoption, usage, or utility of bitcoin. Even if the utility of the network and the price of bitcoin continues to increase exponentially, the energy consumption does not necessarily need to follow the same exponential trend. Gaining a better understanding of the Bitcoin network might also help to understand where other solutions fall short.

Satoshi's genius was to combine a bunch of clever tricks into a new economic game which creates a digital, scarce artifact, without central issuance. This artifact is backed by computation, and computation requires energy.

The current economic game is a game of walls and vaults, closed systems and centralized power. The new economic game is a game of hashes and blocks, public keys and private keys, based on mathematical proofs and physical reality. A game without gatekeepers, without central authorities, without censorship or discrimination.

The old rules have led to a system where money is valuable "because I say so", leading to magic tricks like fractional reserve banking, inflation to stimulate excessive consumption, and even hyperinflation because the temptation to print ever more money is simply irresistible.

The new rules might not be easy to understand. They might, however, lead to a new financial reality: a new economy based on sound money. We will all have to adapt to these rules and become familiar with the nuances of this new game. And we will have to come to terms with the fact that a finite resource has to be used to secure this new, decentralized economy. In the case of Bitcoin, this resource is energy.

Disclaimer:

Please note that this Journal is provided on the basis that the person who is reading it accepts the following conditions relating to the provision of the same (including on behalf of their respective organization). This Journal does not contain or purport to be, financial promotion(s) of any kind.

This Journal does not contain reference to any of the investment products or services currently offered by the operator of the journal, that means any business I am associated with. Bitcoin, shitcoins, and related technologies can be volatile. Don't buy what you can't afford to lose and please do your own research.

Bitcoin has paved the way for some VERY radical technology AND it's very confusing. Read more. Ask questions. The purpose of this Journal is to provide archive and curate the best commentary and culture in the bitcoin space.

Nothing within this Journal constitutes investment, legal, tax or other advice. This Journal should not be used as the basis for any investment decisions which a reader may be considering. Any potential investor in bitcoin or shitcoins, even if experienced and affluent, is strongly recommended to seek independent financial advice upon the merits of the same in the context of their own unique circumstances.

Share this journal early and often. Engage the authors and tell them what you think. We sharpen our position through discourse and debate.

DYOR | BTFD | HODL

Thanks for your attention and support. I appreciate your feedback and hope you enjoy this publication.

- @_joerodgers