Chapter 10

Bitcoin Is King

Andrew M. Bailey* and Craig Warmke**

*Yale-NUS College, **Northern Illinois University

I. Introduction

Kerrygold® butter is legendary. For a time, it was the only butter Americans could find from grass-fed cows. Rich yellow, flavor dense, and imbued with magical Irish qualities. Best butter in the world, and suitable even for blending with morning coffee. Unique.

But a visit to Ireland shows something else. Go there and you might be served *Connacht* Gold for breakfast. Connacht—a province, much like Kerry, a county. If this doesn't shake your confidence in the uniqueness of Kerrygold, just wait till you see the wall of butters at the Supervalu in Dingle. They're all yellow, and Irish, and seem quite nice. Perhaps Kerrygold isn't as special as it might seem.

This essay isn't about Kerrygold. It isn't about bovine "gold" in general, either. It's about digital gold—Bitcoin. Many think that Bitcoin is even less special among cryptoassets than Kerrygold is among Irish butters. After all, 13,457 such assets now have some kind of market value. Many have charismatic leaders, slicker marketing, more apparent utility, and, from time to time, more appealing trading opportunities. Some pundits think Bitcoin's best days are over. A boomer coin. Perhaps Bitcoin isn't as special as it might seem.[*]

[*] For some comparisons among cryptocurrencies and their design tradeoffs, see Bailey et al. (2021a, 2021b).

Yet Bitcoin has enjoyed the top spot in market capitalization among cryptocurrencies for 13 years. The market knows something. What it knows, in our view, is that Bitcoin *is* special. But its intrinsic machinery—what it is in itself—doesn't fully explain why.* Bitcoin is also special because of its founding, culture, and product-market fit. Nothing else comes close on these points of comparison. This gap between Bitcoin and everything else has implications for policy-making, journalism, and academic research.

So, in what follows, we'll explain why Bitcoin is the king of cryptocurrencies—as of today, all 13,457 of them—and what that crown signifies. We begin with a brief description of what Bitcoin is and how it works.

II. Function

The Bitcoin network offers final settlement without authorities.† It offers final settlement in the sense that transactions are effectively irreversible—Bitcoin has no chargebacks, for example. And it offers this finality without authorities like banks or payment providers to oversee, settle, and clear transactions. The network's transactions occur in the network's native asset, also known as Bitcoin. The network has three main players:

1. Users, who send and receive Bitcoin to and from each other.
2. Nodes, computers that run the Bitcoin software and serve as the network's referees. They reject any invalid transactions and curate the Bitcoin ledger.
3. Miners, computers that run the Bitcoin software and compete to produce blocks of valid transactions for the ledger. About every 10 minutes, a miner successfully produces a block and thereby enjoys that block's transaction fees, as well as a predefined amount of Bitcoin in accordance with Bitcoin's automated issuance schedule. A successful block requires a trial-and-error search for the solution to a mathematical puzzle.

Network incentives promote honest behavior among these participants. Nodes reject transactions that attempt to spend already spent Bitcoin. They also reject any blocks that reward miners beyond the permitted amount.

Someone could conceivably spend the same Bitcoin twice by writing a new version of the ledger—an alternative chain of blocks—that erases the original spend and then inserts a new one. But this would likely require a cost-prohibitive amount of energy. Nodes on the network endorse the version of the ledger most likely to be the most energy-intensive—a probabilistic calculation stemming from the difficulty required to mine each block in the chain. So in order to succeed, the

* For the different pieces that came together in Bitcoin, see Narayanan and Clark (2017).

† For technical explainers, see Antonopoulos (2017), Rosenbaum (2019), and Warmke (2021).

attacker would have to re-mine all the intervening blocks from the original spend and then outpace the rest of the network in creating new blocks. With that kind of energy expenditure, the attacker would likely profit much more from forgoing the attack altogether to net the rewards from mining honestly.

You might have heard that the cultivation of Bitcoin's ledger makes it slow and expensive. In one sense, this is true. Bitcoin's ledger updates, on average, every 10 minutes, and each transaction includes a fee to whichever miner produces the block that includes it. But each block is small—due to Bitcoin's consensus rules, the maximum block size is somewhere between two and four megabytes. At today's average transaction size of around 650 bytes, users shouldn't expect to squeeze much more than around 2,000–3,000 transactions in a typical block.[*] With blocks every 10 minutes, this averages to about three to five transactions per second.

There is, accordingly, a fee market: transaction fees are bids for space in the ledger. The more data your transaction involves, the more space on the ledger it'll take and the more you'll have to pay. When the network buzzes with activity, users bid over one another—no matter how big or small a payment one seeks. Small value payments become uneconomical. So Bitcoin's blockchain lacks the transaction throughput of a global payments network. Visa® alone handles, on average, about 1,400 transactions per second, at a cost most are willing to pay.

However, unlike Bitcoin, Visa doesn't offer transaction finality. They can and do reverse transactions. Visa isn't a final settlement layer. Visa transactions settle, instead, through banks and, ultimately, master accounts with the Federal Reserve. So we can think of Visa as a payments layer built atop the Federal Reserve.[†] In much the same way, Bitcoin has payment layers built atop, and which ultimately settle on, its blockchain. So we should instead compare Visa to one of these, the most important of which is the *lightning network.*

Technical details aside, users on the lightning network enjoy the security of Bitcoin's ledger to send and receive Bitcoin nearly instantaneously and practically for free.[‡] The current median fee of one satoshi (the smallest unit of Bitcoin) means that transactions cost a fraction of a penny.[§] And its theoretical throughput far exceeds Visa's own. Amazingly, lightning accomplishes this feat without trusted intermediaries. Consequently, apples to apples and oranges to oranges; Bitcoin is to Fedwire as lightning is to Visa. The main difference in each case is that the Bitcoin side works without trusted intermediaries.

[*] https://bitcoinvisuals.com/chain-tx-size

[†] Benson et. al. (2017)

[‡] Poon and Dryja (2016) first described the network. See Antonopoulos et. al. (2021) for a book-length technical guide.

[§] https://1ml.com/statistics

But there's one more main difference between Bitcoin and the world of traditional finance. Unlike the U.S. dollar and other fiat currencies, Bitcoin has a non-discretionary monetary policy. Whereas the Federal Reserve manipulates the money supply by tinkering with interest rates, Bitcoin has an automated issuance schedule. Bitcoin has a maximum supply of 21 million Bitcoin, which it'll reach around the year 2140. Issuance consists in the above-mentioned mining block rewards. At network launch in 2009, the reward was 50 BTC every block. Every four years, this reward halves; today it sits at 6.25 BTC. All of this is auditable—anyone may run the Bitcoin software to verify that the rules have been followed—and the result is an asset with capped supply and highly predictable issuance. As a result, no one can trade on insider knowledge about Bitcoin's monetary policy. And yet in the last year alone, three highly ranked officials with the Federal Reserve have resigned due to several, let's say, well-timed trades.[*]

There is one important point of commonality between Bitcoin's monetary network and the dollar's. If you wish to send value using dollars (via cash, a Visa transaction, a bank transfer, PayPal®, etc.), you must first acquire the native token of that network—the dollar. So also with Bitcoin. If you wish to send value using the Bitcoin network, you must first acquire some Bitcoin. And once you have some, you may send it (via an on-chain transaction, via lightning, or through some other method). One enters the Bitcoin network just as one enters the dollar network—by earning, purchasing, being gifted, finding, stealing, or otherwise coming into possession of its native token.

In sum, Bitcoin is growing into a self-sufficient monetary stack without trusted intermediaries: the software automates monetary policy, the network effects final settlement, and second-layer solutions like lightning enable fast and cheap payments.

III. Fit

To understand Bitcoin's appeal, it is helpful to grasp two things: how Bitcoin works and what the world is like. Without the first, you might think that Bitcoin is an odd technological fad—little more than an append-only document, as some critics allege. Without the second, you might think that Bitcoin is a solution in search of a problem, a Rube Goldberg® machine whose main purpose is to enrich early adopters at the expense of naïve investors.

Critics such as Paul Krugman fall into this second camp. In a June 2022 column, 11 years after his first critical post about Bitcoin, Krugman writes: "Bitcoin—which

[*] https://www.nytimes.com/2022/01/10/business/economy/richard-clarida-fed-resign.html

was introduced in 2009 (!)—has yet to find any significant real-world uses. In my experience, the answers are always word salad devoid of concrete examples."[*] Despite Krugman's credentials—including a Nobel Prize in economics, the very field which should help him recognize Bitcoin's utility—he fails to appreciate certain aspects of how the world works. This leaves him unable to discern Bitcoin's appeal. We'll describe these aspects when we cover Bitcoin's real-world uses with concrete examples—no word salad.[†]

Venture capitalist Alyse Killeen says Bitcoin is "fintech for poor people."[‡] This is largely what Krugman and other critics fail to understand. A 2021 Chainalysis® study found that adoption of Bitcoin and other cryptocurrencies had skyrocketed 881% in the prior year.[§] And, remember, Bitcoin and USD stablecoins (synthetic versions of the U.S. dollar, which do not compete with Bitcoin) together account for well over half of the entire cryptocurrency market value, with Bitcoin itself accounting for 45%. So this growth has not been led by serious competitors to Bitcoin.

Chainalysis calculates an adoption index using peer-to-peer exchange trade volume, weighted by purchasing power parity per capita and number of internet users. To data-starved critics like Krugman who think Bitcoin is for Silicon Valley "white tech bros" or alt-right libertarians and anarchists,[¶] these facts must come as something of a surprise (see Figure 10.1 on next page).

This is not a list of the world's strongest economies.[**] The Chainalysis team summarizes their findings:

> Our research suggests that reasons for this increased adoption differ around the world—in emerging markets, many turn to cryptocurrency to preserve their

[*] https://www.nytimes.com/2022/06/06/opinion/cryptocurrency-bubble-fraud.html

[†] Some alleged uses for "blockchain"—especially those involving exogenous assets and information—are a bit too coleslaw-like for comfort. For incisive critique of such, see Schuster (2021).

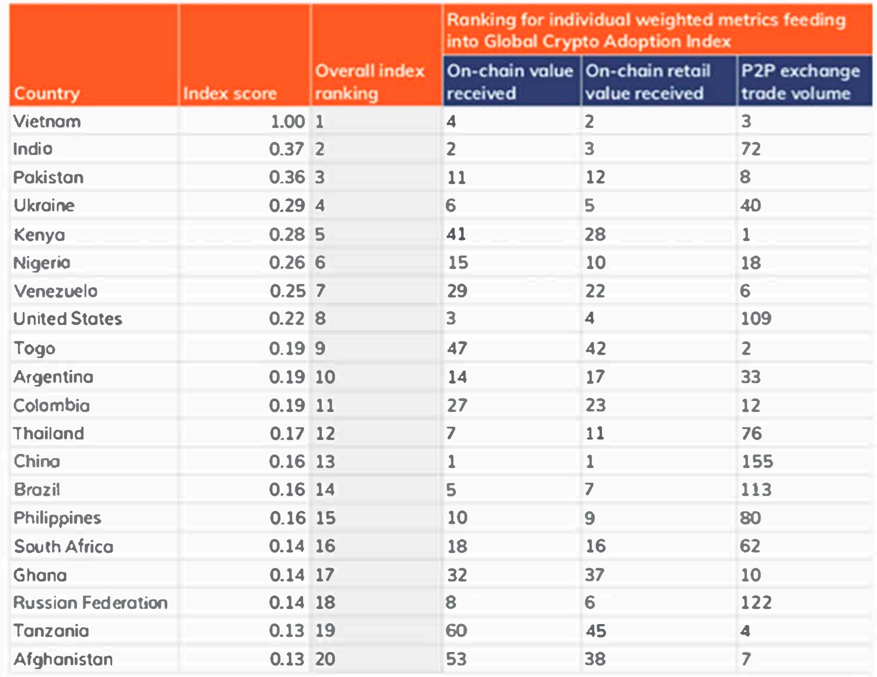
[‡] On a June 2021 Bitcoin Fundamentals Podcast (with host Preston Pysh), Episode 31, Killeen says: "I think Bitcoin is not political. So it shouldn't be a Republican, Democrat, libertarian sort of thing. It's not that. Bitcoiners are not a monolith. And my hope is that it doesn't become a sort of political U.S. versus them thing. Because I see Bitcoin as fintech for poor people. I understand that that's not how it's often spoken about on Bitcoin Twitter and social media spaces, but that's how I see it. And my hope is that the United States doesn't miss the opportunity here, or my hope is that folks don't choose to politicize this." (https://www.theinvestorspodcast.com/bitcoin-fundamentals/investments-in-bitcoin-tech-w-alyse-killeen/).

[§] https://blog.chainalysis.com/reports/2021-global-crypto-adoption-index/

[¶] https://www.nytimes.com/2022/06/06/opinion/cryptocurrency-bubble-fraud.html

[**] https://blog.chainalysis.com/reports/2021-global-crypto-adoption-index/

savings in the face of currency devaluation, send and receive remittances, and carry out business transactions, while adoption in North America, Western Europe, and Eastern Asia over the last year has been powered largely by institutional investment.



Country	Index score	Overall index ranking	Ranking for individual weighted metrics feeding into Global Crypto Adoption Index		
			On-chain value received	On-chain retail value received	P2P exchange trade volume
Vietnam	1.00	1	4	2	3
India	0.37	2	2	3	72
Pakistan	0.36	3	11	12	8
Ukraine	0.29	4	6	5	40
Kenya	0.28	5	41	28	1
Nigeria	0.26	6	15	10	18
Venezuela	0.25	7	29	22	6
United States	0.22	8	3	4	109
Togo	0.19	9	47	42	2
Argentina	0.19	10	14	17	33
Colombia	0.19	11	27	23	12
Thailand	0.17	12	7	11	76
China	0.16	13	1	1	155
Brazil	0.16	14	5	7	113
Philippines	0.16	15	10	9	80
South Africa	0.14	16	18	16	62
Ghana	0.14	17	32	37	10
Russian Federation	0.14	18	8	6	122
Tanzania	0.13	19	60	45	4
Afghanistan	0.13	20	53	38	7

Figure 10.1 Global Crypto Adoption Index

People use Bitcoin because it solves their problems. Problems like these:

Lack of Banking

According to the most recent Global Findex database from the World Bank, aproximately 31% of adults globally lack a traditional bank account. Of these unbanked, 26% blame the cost of banking, 21% blame distance, and 16% distrust traditional banks. Many worldwide lack access to banking for more reasons than that they just don't have the money.[*] But everyone can access Bitcoin's open monetary network essentially for free, without traveling anywhere, as long as they have an internet-connected device.

[*] https://globalfindex.worldbank.org/chapters/unbanked

High Inflation

Around one billion people worldwide live with runaway inflation.[*] Many live with hyperinflation. Recently, the value of currencies in places like Venezuela and Lebanon have been worse than decimated, literally. In these places, using Bitcoin as a medium- to long-term savings vehicle makes sense. Despite wild volatility—sometimes dropping as much as 50% within months—Bitcoin's purchasing power remains in a steep up-trend against these subpar fiat currencies.

Over longer time-frames, Bitcoin has outperformed every national currency. And, in shorter time-frames, even cherry-picking its worst months of performance, it still outperforms many national currencies. Since Bitcoin is also easier to attain, verify, transfer, and hide than physical gold, we can respect why some use it to help preserve their purchasing power.

Transaction Costs

Intermediaries exist in part to detect, prevent, and reverse fraud. Their bottom lines require that they levy fees on every transaction. In traditional systems, different kinds of transfers call for different plumbing through the financial system and specialized business models.[†] One familiar kind of transfer in the United States is consumer spending through credit cards. A credit card transaction ultimately involves several intermediaries—the card's issuing bank (e.g., Chase), the credit card company (e.g., Visa), and the merchant's bank (e.g., PNC). Clearance and settlement of the payment usually takes a few days. So multiple companies with large payrolls need to skim off the top. As a result, consumers often pay 1.5–3% in transaction fees.[‡]

Remittances take another route through the world's financial plumbing. Someone in one country sends funds to someone in another country, and depending on the particular route one takes, this usually involves at least the money transfer operator as well as the intermediaries that send and receive the funds on each end, respectively. Everyone takes a cut, especially if an intermediary exchanges one currency for another.

Although remittance costs have slowly come down over the years, they remain high. The World Bank's most recent quarterly report on remittance costs still puts the average global costs at about 6%. But many country pairs face double-digit remittance

[*] https://data.worldbank.org/indicator/FP.CPI.TOTL.ZG

[†] See Benson et. al. (2017).

[‡] https://www.fool.com/the-ascent/research/average-credit-card-processing-fees-costs-america/

fees. Remittances from Tanzania, for example, remain extremely high when they're directed to Kenya (31.45%), Rwanda (24.37%), and Uganda (29.68%).*

How does Bitcoin help? Transactions over both Bitcoin and the lightning network have their own network topologies and don't "care" whether you're buying a coffee at your local Starbucks® or sending money to your relative in Ghana. The plumbing is the same. Since lightning is basically free and instantaneous regardless of the location of sender and recipient, lightning threatens to obsolete intermediaries involved in both consumer payments and remittances. Lightning is not an incremental improvement over these traditional payment systems. It is a 100× improvement in convenience, speed, and cost.

Capital Controls

Suppose you want to flee a totalitarian regime. You might be an independent journalist, a whistleblower, an activist, or a persecuted religious minority. How will you preserve your family's wealth? Bank accounts can be frozen. You can't take your house with you. Physical cash is bulky and subject to theft. Gold shows up in metal detectors and is easily confiscated. Since Bitcoin is massless and possession involves nothing more than access to a secret passphrase, Bitcoin will often be the most effective way to protect your family's wealth.

Bitcoin serves as a lifeline to many people worldwide. In a recent letter to Congress, 21 human rights advocates from 20 countries write:

> We can personally attest—as do the enclosed reports from top global media outlets—that when currency catastrophes struck Cuba, Afghanistan, and Venezuela, Bitcoin gave our compatriots refuge. When crackdowns on civil liberties befell Nigeria, Belarus, and Hong Kong, Bitcoin helped keep the fight against authoritarianism afloat. After Russia invaded Ukraine, these technologies (which the critics allege are "not built for purpose") played a role in sustaining democratic resistance—especially in the first few days, when legacy financial systems faltered.†

The full letter includes references to several such examples with the more detailed reports from the news media—the very kinds of "concrete examples" that Krugman has requested.

Overall, then, Bitcoin is not a solution in search of a problem. It solves real problems for people in dire need. These problems generate demand for Bitcoin. Since Bitcoin has a capped supply, increased demand for Bitcoin has but one release

* https://remittanceprices.worldbank.org/sites/default/files/rpw_main_report_and_annex_q421.pdf

† https://www.financialinclusion.tech/

valve: price.[*] The people who have speculated on Bitcoin profitably have largely seemed to recognize two things: the true breadth of Bitcoin's total addressable market as a credibly neutral money and the world's desire for such a thing. As many elites still fail to grasp—largely because they haven't needed to—Bitcoin has remarkable product-market fit.

It is consistent with all this, to be sure, that Bitcoin's design involves serious tradeoffs or negative externalities. Its public ledger makes privacy difficult, though not impossible. It requires energy for its security. And its fixed supply engenders truly spectacular volatility in its market price. A complete evaluation of Bitcoin would weigh all of its costs and benefits, a project beyond the scope of this chapter.[†]

IV. Founding

Bootstrapping Money

As with legacy institutions, Bitcoin's appeal doesn't lie only in its intrinsic or technical features, or even in its capacity to solve problems. It also lies in its history and founding values.[‡]

Imagine that you wanted to create a new money. The goal here would be twofold: to craft a new monetary species and to nurture its network—to grow the class of people who treated it as money. These are not easy goals. You might mint a batch of units—magical beans, as it were—and award them all to yourself. Without doing much more, those beans would be about as useful as an invented language known only to you. Somehow those beans need to get into other hands, and circulate from there. So you might instead give them away. That would assure some distribution. But distribution isn't enough. You also need to get people to value your beans *as money.* And it's hard to get people to value something that they've only ever freely received.

Perhaps, then, you could sell them, first to friends and family, and later to others. But this, too, would have limits. Why should anyone want to treat as money these magical beans you sold or dispensed to your inner circle? And why should anyone trust you not to mint more beans and dilute the value of the ones

[*] For an argument that a volatile but non-zero price for Bitcoin is to be expected given its fundamentals—and the needs they satisfy—see Andolfatto and Spewak (2019).

[†] For an attempt at such a synoptic evaluation, see Bailey et. al. (forthcoming).

[‡] On the cypherpunk movement that gave birth to Bitcoin and informed its founding anti-authoritarian values, see Brunton (2020) and Beltramini (2021).

you just sold? It makes sense to many that a startup business should have and benefit insiders: the reward for taking the risks inherent in starting a productive enterprise is selling shares. But, for very good reason, we don't treat shares as money. Money is supposed to be more neutral—more like public market infrastructure than shares in a private firm. So it would be fair to ask: who died and made you king of the money? Overall, why should anyone treat as money those beans that you both created and continued to influence?

It's a real pickle, one long studied by monetary economists and historians. How can we bootstrap a new money?[*] The problem is especially pressing for new *private* monies. States can force citizens to pay taxes in a given monetary species, thus ensuring non-zero demand for that species, no matter its origins or intrinsic technical features. Not so for typical non-state actors; they must find another way to persuade others to treat their new units as money.

Here is how Satoshi Nakamoto, Bitcoin's pseudonymous creator, approached the problem:

Fair Distribution

Bitcoin's creator didn't freely mint money for himself, his friends, or other insiders. There is exactly one way to mint new Bitcoin: to complete proofs of work—that is, to burn electricity and processor cycles in the discovery of new blocks and to claim the accompanying reward of newly minted Bitcoin. No exceptions.

So Satoshi had to *pay* for his Bitcoin, just like anyone else. He did not make magic beans out of thin air and hawk them at the local market. He bought them from nature, just like anyone else, and the price was energy. Minting requires mining. So the marginal cost of production for Bitcoin is non-zero, and it's a price anyone must pay if they wish to mine it. Mining has also been open to all since the network launched. So although Bitcoin has early adopters, it has no insiders.

Not all cryptocurrencies follow this model. Some, in stark contrast to Bitcoin, involve early rewards or pre-mines for their creators and other insiders. Here, the marginal cost of production for new monetary units is effectively zero, and early insiders acquire their units under different rules than others. Under a so-called "pre-mine," creators do not purchase their coins from nature in a free and open competition. Instead, they mint their units for free and sell some to others. Here is a typical allocation of tokens from a new network called Optimism (see Figure 10.2), one that many prominent voices have heralded as a partial solution to Ethereum®'s scaling issues:

[*] Luther (2019).

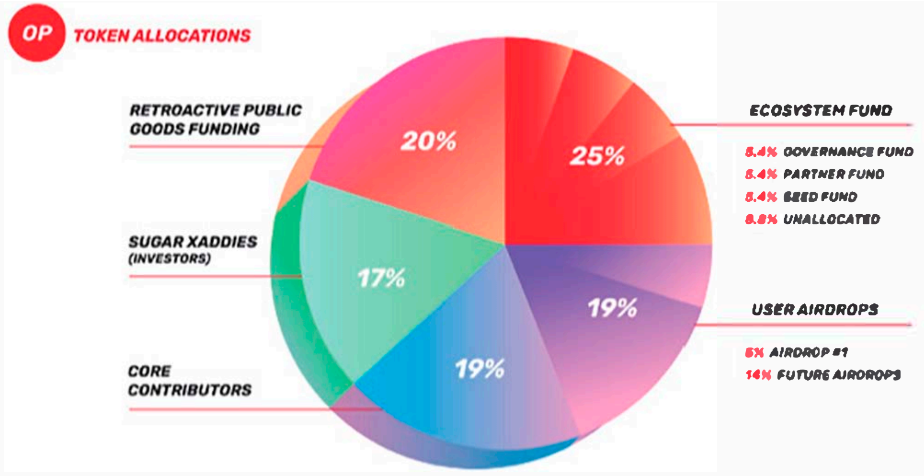


Figure 10.2 Of Just over Four Billion OP Tokens at Launch, 5–19% Go to Everyday Users (*Source:* Chart and data available at https://community.optimism.io/docs/governance/allocations/)

The lesson we draw is partly normative and partly descriptive. The normative point is this: Bitcoin's founding is fair in one very important respect: the rules of its monetary system apply to all. We do not claim that pre-mines and the like are always morally wrong or dubious. We do not even claim that they are universally undesirable for investors. But a founding history without insiders and with creators who obey the same rules as anyone else is attractive.

The descriptive point follows from this: the market has recognized Bitcoin as king for 13 years. Participants know that it is more fair than many alternatives and accordingly favor Bitcoin in their market behavior. Bitcoin's fair launch has, we suspect, played an important though subtle role in resolving the bootstrapping problem. It has credibility because it came to be in a credibly neutral way.

Leaderless Money

Satoshi—like Keyser Söze—walked away.

A creator's ongoing influence or control poses a risk. Think about it: would *you* accept some magic internet beans as money, if you knew full well that their creator could later alter them, dilute their supply, or push for technical modifications? You *might* if you trusted the creator or simply had to accept that creator's edicts (as with sovereign fiat money).

But this is not a viable path for a private money. Gadgets like Bitcoin aim primarily to be neutral money without trusted authorities.[*] For any would-be monetary engineer, this is a real bind. You want to make something useful whose usefulness doesn't rely on *you.* Failure on this front risks creating a cult of personality or a legacy monetary institution of the kind we all know well, one that relies on trusted authorities.

Satoshi did the one thing he could to resolve it: he left. Without pomp or ceremony, he removed his name from the Bitcoin website, handed over its keys to the community of developers, and quietly exited the spotlight. No one can say that Satoshi exerts undue influence over Bitcoin development, or monetary policy, or culture. Satoshi exerts no influence over those things, not under the Satoshi name, at any rate.

In this way, Bitcoin became leaderless. It is not a sovereign currency—and yet despite being private in that sense, it is not a company money. It is private in the sense of being a non-state money and public in the sense of being non-corporate and open to participation by all. Bitcoin's leaderless status has made it more robust and resilient. Its central bankers can't fiddle with its supply. Its CEO cannot, in a drunken haze, accidentally tweet out something foolish, tanking market confidence. Bitcoin, Inc., cannot go bankrupt or have its assets frozen. There is no Bitcoin Federal Reserve, no Bitcoin CEO, no Bitcoin, Inc.

Charismatic leaders are sometimes cited as being an advantage for other cryptocurrencies. Just as Elon Musk or Steve Jobs were great for their companies' marketing, so also a magnetic or gifted founder can drive interest in a cryptocurrency. But here the Bitcoin network stands apart in its promise to host neutral money. This promise is credible to the extent that Bitcoin is leaderless. And Satoshi seems to have realized that Bitcoin's success required his departure.

From Founding to Now

Our description of Bitcoin's founding may sound lofty and idealistic. But does it have much to do with the real world, now? We think so, and we cite two examples.

First, Bitcoin has been, for the entirety of its existence, the most valued, most studied, most used, and most widely known cryptocurrency. This is no accident. After all, there are plenty of alternatives—over 13,000, recall. And many of those alternatives have been around for over a decade; their existence is no mystery, and market participants can easily access them. We suspect that Bitcoin's top ranking among cryptocurrencies reveals a preference for a leaderless cryptocurrency with a fair initial mechanism of distribution.

[*] See the whitepaper, Nakamoto (2008).

Second, Bitcoin has a unique and healthy coin distribution. For the entirety of its existence, Bitcoin's ownership has become more decentralized. Two metrics, in particular, support this claim.* First, we have supply equality ratio (SER)—the ratio of "supply held by addresses with less than one ten-millionth of the current supply of native units to the supply held by the top one percent of addresses."†

Comparing Bitcoin's SER to a few competitors is instructive (Figure 10.3):

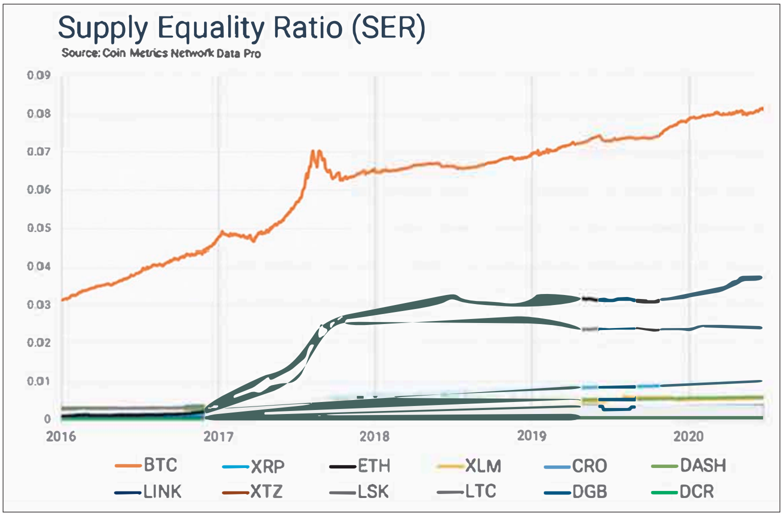


Figure 10.3 Bitcoin Supply Equality Ratio

As explained by CoinMetrics:

> A high SER signifies high distribution of supply. As hypothesized, Bitcoin has the highest SER out of the assets evaluated, followed by Ether and Litecoin. This is remarkable, since Bitcoin is also the primary cryptoasset being custodied by large financial institutions; a trend that increases SER's denominator and puts overall downward pressure on the ratio. The sustained increase in Bitcoin's SER shows that, in spite of large institutions entering the space, Bitcoin is still very much a grassroots movement.‡

A second metric is network distribution factor (NDF), which is the "ratio of supply held by addresses with at least one ten-thousandth of the current supply

* We're following this CoinMetrics report here in pointing to both of these metrics: https://coinmetrics.io/bitcoin-an-unprecedented-experiment-in-fair-distribution/

† https://docs.coinmetrics.io/asset-metrics/supply/ser

‡ https://coinmetrics.io/bitcoin-an-unprecedented-experiment-in-fair-distribution/

of native units to the current supply."[*] Here, again, is how Bitcoin fares against a few competitors (Figure 10.4):

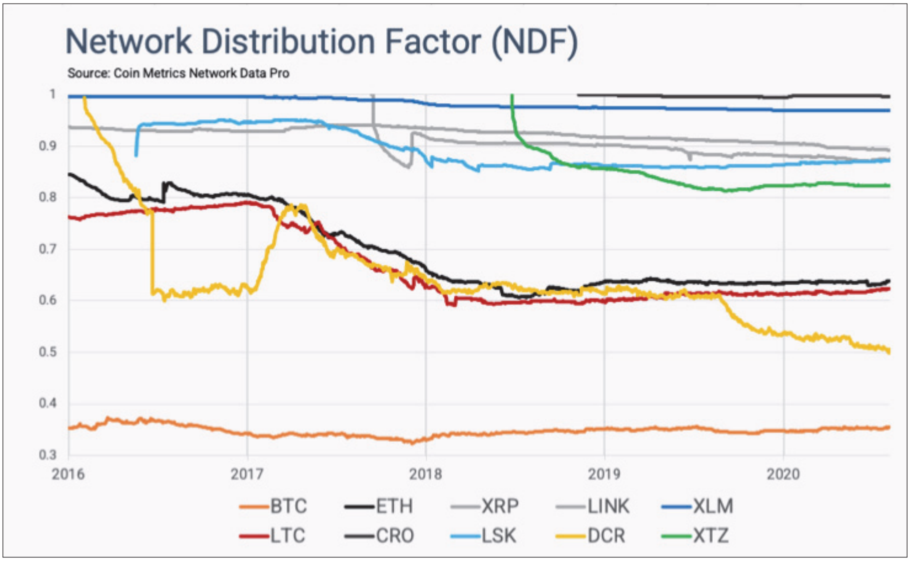


Figure 10.4 Bitcoin Network Distribution Factor

Lower is presumably better. Bitcoin shines again. As CoinMetrics explains: "A low NDF signifies better distribution as there are fewer entities at the top 0.01%. Conversely, a NDF close to 1 signifies a very low cryptoasset distribution."[†]

More and more people own Bitcoin. A network of one—Satoshi—has blossomed into an ecosystem involving millions. Bitcoin is young, of course, and it remains a niche money. Its distribution is not nearly as wide as the dollar's, say, or many other fiat currencies. But it seems to be trending in one direction—global adoption.

The point here is not just that Bitcoin is the most valuable cryptocurrency or the most widely used. Rather, its distribution trends in a direction that will be attractive from a wide range of views about apt patterns in the distribution of goods. One need not be an unqualified egalitarian to suppose that wider distribution of a good is itself good, for example. And any view affirming as much will see Bitcoin's distribution as trending in the right direction.

[*] https://docs.coinmetrics.io/asset-metrics/supply/ndf

[†] https://coinmetrics.io/bitcoin-an-unprecedented-experiment-in-fair-distribution/

V. Layer Zero

Whereas lightning network is layer 2 and the Bitcoin network is layer 1, we can think of “layer 0” as the people who develop and support the entire Bitcoin ecosystem. There are several such groups: software developers, node runners, miners, users, companies, and, finally, the group of hedge funds, traders, and venture capitalists. These aren’t mutually exclusive, but the groups often have competing interests. Some of these competing interests relate to Bitcoin’s history as a credibly neutral money.

Bitcoin’s software developers have a reputation for moving slowly precisely so that they don’t break things. One major reason for caution: nodes that run different versions of the software risk a chain split that creates a new ledger with a new cryptocurrency. So it’s of utmost importance that proposed changes don’t split the network, whether by accident or disagreement. But, as other networks develop newer technology, some Bitcoin users fear that Bitcoin adoption will lag behind, leading to consistently low transaction fees on the main network.

This is important because, in a decade, the Bitcoin mining subsidy will drop below a single Bitcoin. If fees don’t increase quickly enough, some fear that Bitcoin will become less secure and lose market share.[*] The main counter is that, even if fees don’t increase rapidly enough, Bitcoin’s price will, with the result that, though the Bitcoin-denominated mining subsidy decreases, its value when denominated in the U.S. dollar will suffice to make attacks on the network uneconomical. Given Bitcoin’s product-market fit, as described above, we suspect that concerns about Bitcoin’s security budget are slightly overblown.

Bitcoin’s consensus rules (about who has which amounts of Bitcoin) have changed around 20 times. And they seem to occur less frequently as Bitcoin ages—only one such change has occurred in the last five years.[†] The software is open source, available for all to poke and prod, and proposed changes undergo rigorous testing.[‡] Bitcoin’s software has a stellar history, especially when we compare it to the hacks, exploits, outages, and unfulfilled promises of other cryptocurrency protocols.[§]

Leading up to 2017, a civil war broke out in the Bitcoin community about whether to increase the block size for higher transaction throughput.[¶] The “big blockers”—which included some of the biggest miners and Bitcoin companies—argued that bigger blocks would hasten adoption by leading to lower transaction

[*] For a classic statement of the worry, see Carlsten et. al. (2016).

[†] https://blog.bitmex.com/a-complete-history-of-Bitcoins-consensus-forks-2022-update/

[‡] Lopp (2018).

[§] For a list of costly exploits, see https://rekt.news/leaderboard/

[¶] Bier (2021).

fees. The “small blockers” argued that more transactions per block would increase the bandwidth and memory requirements for running a node, leading to fewer nodes on the network and more centralization (and, as you’d expect, more revenue for the companies and miners who pushed for bigger blocks). The small blockers won handily and signaled an overwhelming commitment to network decentralization. Their victory owed, in part, to the commitment from node runners to reject bigger blocks. Today, around 15,000 Bitcoin full nodes operate the world over (Figure 10.5).

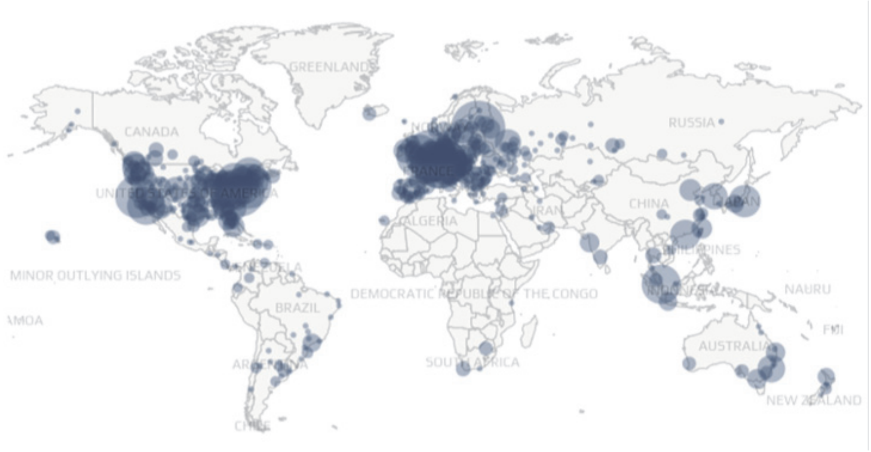


Figure 10.5 Global Map of Bitcoin Node Distribution (*Source:* https://bitnodes.io/)

Bitcoin nodes more than double the number of nodes currently on the Ethereum network (the second largest cryptocurrency network).* But the requirements for Ethereum nodes are high and increasing, which has led to a substantial proportion of them being run on centralized servers. For example, AWS® alone handles around 25% of Ethereum work loads.† The more centralized a network is, the more vulnerable it is to attacks on central points of failure.

Some criticize Bitcoin for being similarly vulnerable thanks to miners who pool resources to share block rewards. Given Bitcoin’s consensus mechanism, anyone can hijack the network and attempt to double-spend coins with some reliability once they reach 51% of the network’s hashrate. Currently, mining is an industrial process. As a result, miners often pool resources to operate in pools.

For most of Bitcoin’s history, a few pools have had enough hashrate to collude in this way (see Figure 10.6). Although miners and pools have a tradition

[*] According to https://ethernodes.org/, there are currently about 6,000 Ethereum nodes online.

[†] https://aws.amazon.com/blockchain/

of avoiding such a high hashrate for fear of devaluing Bitcoin and their large expenditures on specialized mining hardware,[*] they could conceivably face pressure from the state to, say, blacklist certain addresses if enough pools reside within the same borders. But those involved in the vulnerable pools could leave and join other pools. And technical solutions are also in development.

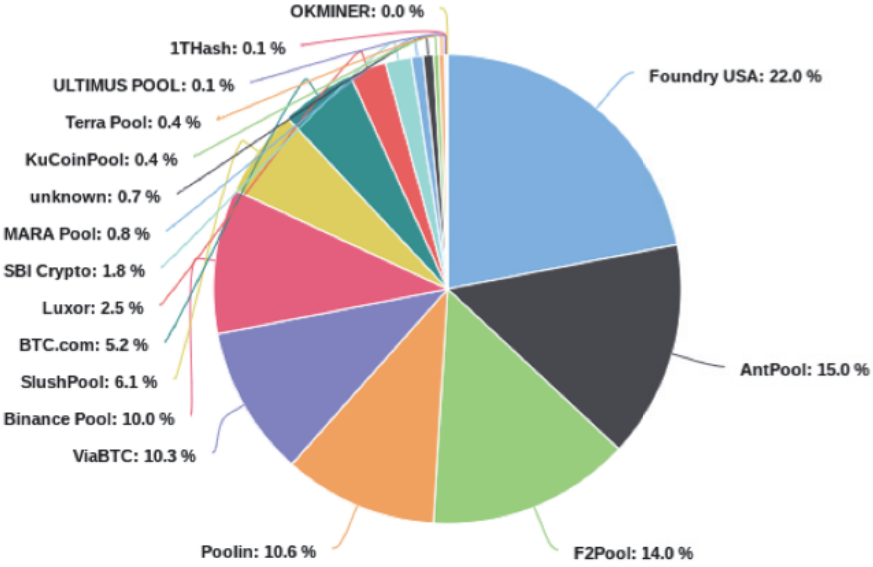


Figure 10.6 Bitcoin's Hashrate Distribution across Mining Pools, for Mid-May Through Mid-June, 2022.

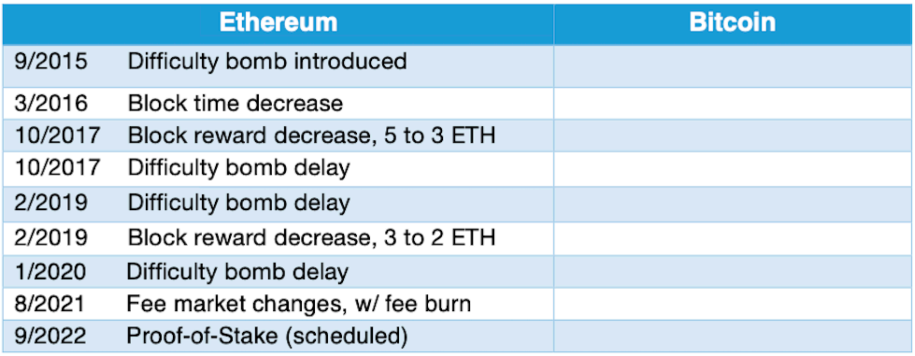
Industrial miners have also recently kept most of their mined Bitcoin. When price drops rapidly, and the block reward doesn't cover the cost of producing a block, they might also need to sell the Bitcoin on their balance sheets to bridge the difference, leading to a kind of price death spiral.[†]

But, though this is a risk, we suppose that these industrial miners will have hedged through derivatives, not too dissimilar from how farmers hedge their future yield. So far, Bitcoin has survived severe price drops. And, as we write, Bitcoin has dropped more than 60%. But, in all these market sell-offs, Bitcoin drops less on a percentage basis than the rest of the cryptocurrency market. In these sell-offs, participants treat Bitcoin, alongside stablecoins, as a safe-haven asset.[‡]

[*] See, for example, the case of Bitfury, as detailed in Popper (2015: p. 299)

[†] Shinobi (2021).

[‡] You can see this in any "Bitcoin dominance" chart.



Ethereum		Bitcoin
9/2015	Difficulty bomb introduced	
3/2016	Block time decrease	
10/2017	Block reward decrease, 5 to 3 ETH	
10/2017	Difficulty bomb delay	
2/2019	Difficulty bomb delay	
2/2019	Block reward decrease, 3 to 2 ETH	
1/2020	Difficulty bomb delay	
8/2021	Fee market changes, w/ fee burn	
9/2022	Proof-of-Stake (scheduled)	

Figure 10.7 A History of Changes to Ethereum's and Bitcoin's Monetary Policies

Bitcoin is also special in how users of all stripes stridently commit to its automated issuance schedule. The schedule has never changed in design, though developers have had to patch bugs to ensure that it behaves as intended. Bitcoin stands in stark contrast to Ethereum in this regard. The latter has changed its monetary policy routinely throughout its existence. (See Figure 10.7.)

Ethereum's ever-changing monetary policy owes, in large part, to pockets of influence within its own community—the presence and continuing involvement of founder Vitalik Buterin, as well as the sway of the Ethereum Foundation, which has had a trademark on the 'Ethereum' name since the network originally launched.[*]

Centralized sources of influence have exercised their power in ways small and large throughout its history. The most famous is the DAO hard fork of 2016, which left the old network ("Ethereum classic") behind and instituted a new network ("Ethereum"), all to undo an exploit that, though permissible within the stated rules, resulted in unexpected and wide losses among DAO participants.[†] We have no opinion on whether this was a good decision, but it speaks to the centralization and manipulability of the second largest cryptocurrency network.

In contrast, Bitcoin's more robust commitment to decentralization has led to more trust in the stability of its native asset. In recent years, we've begun to see commitments to hold Bitcoin in the treasuries of publicly traded companies (e.g., Tesla®, Microstrategy®, and Square/Block) and efforts to make Bitcoin legal tender in nation-states like El Salvador and the Central African Republic.

[*] https://trademarks.justia.com/866/34/ethereum-86634529.html

[†] Shin (2022).

VI. Implications

We began with the slogan that Bitcoin is digital gold. The slogan isn't literally true, and isn't intended to be. It's an analogy or comparison. Is the analogy useful? Is it more illuminating than misleading? We're now in a position to evaluate such questions.

To state the obvious points of disanalogy: Bitcoin is synthetic and digital, whereas gold is a naturally occurring physical element. Human beings have used gold as a monetary good for thousands of years; Bitcoin is a little more than a decade old. Bitcoin and gold do not behave the same in markets, either. Gold's price isn't *that* far off today (around $1,800/oz) from where it was 10 years ago (around $1,500/oz), and it has traded between $1,000 and $2,000 for the entire interval.

Bitcoin's price, by contrast, has shown *tremendous* volatility. It traded below $20 10 years ago, reached a high of over $69,000 in 2021, and trades around $20,000 today (Summer 2022), over 75% down from the peak—a point not missed in mainstream price coverage.[*] This volatility limits Bitcoin's potential as a short-term medium of exchange and sets its market reception apart from gold's, which is tame by comparison.

The points of analogy are perhaps more interesting: like gold and other physical commodities, Bitcoin has a non-zero marginal cost of production. No one can mine more gold or more Bitcoin without *paying* (whether by paying to blast through rock, as with gold, or for electricity and processor cycles, as with Bitcoin).[†] Bitcoin is finite in both stock and flow: its total supply is capped, and additions to that supply in the meantime remain slow and steady. Gold is often thought to have similar properties—a finite total supply, with additions via mining of perhaps 2% per year (though new ore discoveries could change these expectations and shock markets accordingly).

Gold and Bitcoin are, furthermore, censorship resistant in an important sense. One can transfer physical gold without relying on mediating authorities: simply hand over a gold coin to your counterparty. (However, the point does not apply to paper claims for gold). So, too, can one transfer Bitcoin without relying on mediating authorities. Simply sign a transaction and broadcast it to the Bitcoin network. These points of similarity reveal something important: Bitcoin is, like gold, neutral. Neutral in initial issuance, neutral in ongoing monetary policy, neutral in transfer. And this makes Bitcoin special—perhaps unique—among cryptocurrencies.

In sum: the slogan that Bitcoin is or could be digital gold isn't just a metaphor, and it isn't mainly about Bitcoin's market reception. It's about Bitcoin as

[*] https://www.nytimes.com/2022/05/12/technology/cryptocurrencies-crash-bitcoin.html

[†] Selgin (2015), accordingly, classifies Bitcoin as a "synthetic commodity" money.

a piece of neutral infrastructure—rather more like a natural physical element than, say, the U.S. dollar. Suppose that's right. Suppose that Bitcoin is digital gold. What might follow? We'll offer a few suggestions under the categories of policy-making, journalism, and academic research.

Policy-Making

Bitcoin has, in fact, already won as a globally neutral monetary network. Nurturing the Bitcoin network, using Bitcoin as a reserve asset, or making payments over Bitcoin would be analogous to deploying gold within the monetary system—only digital, more portable, more divisible, easier to audit and verify, and more difficult to confiscate.

So attempts to ban Bitcoin or limit its use will meet strong resistance.[*] It is native to the internet and, as a result, extremely difficult to tamp down. In this regard, we liken Bitcoin to cryptography. Whereas cryptography provides censorship-resistant communication, Bitcoin provides censorship-resistant communication of value. And just as the efforts to limit the strength and spread of cryptography failed in the 1990s, we expect that it will be similarly difficult to limit the strength and spread of Bitcoin.[†]

Whether this is good or bad overall is the subject for another time. But there's widespread evidence that Bitcoin is helping the underbanked, as well as those who suffer under authoritarian rule and runaway inflation.[‡] There's also wisdom in not wasting resources fighting the inevitable.

Journalism

We must not assume that cryptocurrencies share more in common than they, in fact, do. Bitcoin leads them all precisely because no one leads it. The policy must begin here from a place of understanding—not of cryptocurrency in general, but of Bitcoin in particular. The general category isn't going anywhere precisely because Bitcoin, itself, isn't going anywhere. We owe it special attention. Too often, journalists lump Bitcoin in with all other cryptocurrency projects. And while these other projects benefit from the association, Bitcoin's reputation suffers from it. More often, journalists should distinguish between Bitcoin and "crypto." Our slogan: not Bitcoin only, but Bitcoin first.

[*] On the high cost of banning Bitcoin, see Hendrickson and Luther (2017).

[†] For a history of the battle between cryptographers and cypherpunks against the U.S. Government, see Levy (2001).

[‡] See https://www.financialinclusion.tech/

Research

Bitcoin's victory as neutral money should have downstream consequences for academic research, too. Presently, there is only one research center mostly devoted to Bitcoin—MIT's Digital Currency Initiative—and it has a near-exclusive focus on computer science. There are several other research centers devoted to cryptocurrency overall, with very few researchers working on Bitcoin exclusively. If we were to apportion research and research centers to importance and long-lasting impact, however, we'd find the reverse.

We need more Bitcoin-first research and research centers precisely because Bitcoin is, by far, the most likely to have a long-lasting impact on our world. And, since Bitcoin is so highly interdisciplinary, such centers should be full of experts from all the different disciplines that touch on it—economics and computer science, of course, as well as law, philosophy, political science, and business. And we should devote more resources to understanding it rather than projects which, like Icarus, fly too close to the sun before flaming out.

VII. Conclusion

Bitcoin is not the king of money. That honor goes to the U.S. dollar. But Bitcoin is the king of cryptocurrencies. Bitcoin is the most valuable, most secure, and most credibly neutral internet-native asset in the world. Arguably, it is the most valuable cryptocurrency precisely because it is the most secure and credibly neutral.

Yet all kings pass away. How long, then, will the dollar or Bitcoin reign over their respective domains? And in the meantime, how far will Bitcoin extend its boundaries? This question inspires several others, for those who have an imagination. How many more countries will adopt it as legal tender? Will countries use it to evade sanctions someday? Will Bitcoin serve as a major reserve asset, used in international trade? Will countries look to sign treaties to limit each other's hashrate? How many lives will it save? Will it overtake physical gold's market capitalization? Will the lightning network make other payment processors and remittance services obsolete? What new kinds of crime might it enable—or disable, for that matter? How many central banks will it undermine? These questions strike some as silly. But we take them quite seriously. And we'd like to encourage others to take them seriously, too.[*]

[*] We thank Bradley Rettler and Troy Cross for helpful comments and critique. Disclosures: The authors are both fellows with the Bitcoin Policy Institute, a Bitcoin research think tank. In addition, Craig Warmke writes for Atomic.Finance, a Bitcoin finance startup company. The authors regularly use Bitcoin and fiat currencies, including USD and SGD.

References

Andolfatto, D., and Spewak, A. (2019). Whither the price of Bitcoin? *Economic Synapses,* 1. Federal Reserve Bank of St. Louis.

Antonopoulos, A. M. (2017). *Mastering Bitcoin: Programming the Open Blockchain*. O'Reilly Media, Inc.

Antonopoulos, A. M., Osuntokun, O., and Pickhardt, R. (2021). *Mastering the Lightning Network*. O'Reilly Media, Inc.

Bailey, A. M., Rettler, B., and Warmke, C. (2021a). Philosophy, politics, and economics of cryptocurrency I: Money without state. *Philosophy Compass*, 16(11).

Bailey, A. M., Rettler, B., and Warmke, C. (2021b). Philosophy, politics, and economics of cryptocurrency II: The moral landscape of monetary design. *Philosophy Compass*, 16(11).

Bailey, A. M., Rettler, B. and Warmke, C. (forthcoming). *Resistance Money: A Qualified Philosophical Defense of Bitcoin*. Routledge.

Beltramini, E. (2021). Against technocratic authoritarianism. A short intellectual history of the cypherpunk movement. *Internet Histories,* 5: 101–118.

Benson, C. C., Jones, R., and Loftesness, S. (2017). *Payments Systems in the US: A Guide for the Payments Professional* (3rd Edition). Glenbrook Press.

Bier, J. (2021). The Blocksize War: The battle over who controls Bitcoin's protocol rules. https://blog.bitmex.com/the-blocksize-war-chapter-1-first-strike/

Brunton, F. (2020). *Digital Cash: The Unknown History of the Anarchists, Utopians, and Technologists Who Created Cryptocurrency.* Princeton University Press.

Carlsten, M., Kalodner, H., Weinberg, S. M., and Narayanan, A. (2016, October). On the instability of Bitcoin without the block reward. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security,* 154–167.

Hendrickson, J., and Luther, W. J. (2017). Banning Bitcoin. *Journal of Economic Behavior & Organization,*. 141: 188–195.

Levy, S. (2001). *Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age*. Penguin.

Lopp, J. (2018). Who controls Bitcoin Core? https://blog.lopp.net/who-controls-bitcoin-core-/

Luther, W. J. (2019). Getting off the ground: The case of Bitcoin. *Journal of Institutional Economics*, 15(2): 189–205.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/Bitcoin.pdf.

Narayanan, A., and Clark, J. (2017). Bitcoin's academic pedigree. *Communications of the ACM,* 60(12): 36–45.

Poon, J., and Dryja, T. (2016). The Bitcoin lightning network: Scalable off-chain instant payments. Lightning Network Paper.

Popper, N. (2015). *Digital Gold: The Untold Story of Bitcoin*. Penguin UK.

Selgin, G. (2015). Synthetic commodity money. *Journal of Financial Stability,* 17: 92–99.

Rosenbaum, K. (2019). *Grokking Bitcoin*. Manning Publications.

Schuster, E. (2021). Crypto cloud land. *Modern Law Review,* 84(5): 974–1004.

Shin, L. (2022). *Cryptopians: Idealism, Greed, Lies, and the Making of the First Big Cryptocurrency Craze*. Public Affairs.

Shinobi (2021). How centralized is Bitcoin mining really? *Bitcoin Magazine.* https://bitcoinmagazine.com/business/is-bitcoin-mining-centralized

Warmke, C. (2021). What is Bitcoin? *Inquiry,* 1–43.

Warmke, C. (2022). Electronic coins. *Cryptoeconomic Systems,* 2(1). https://cryptoeconomicsystems.pubpub.org/pub/warmke-electronic-coins