Economics from the Top Down

new ideas in economics and the social sciences

Is Bitcoin More Energy Intensive Than Mainstream Finance?

Blair Fix

March 21, 2024

When it comes to Bitcoin, there's one thing that almost everyone agrees on: the network sucks up a tremendous amount of energy. But from there, disagreement is the rule.

For critics, Bitcoin's thirst for energy is self-evidently bad — the equivalent of pouring gasoline in a hole and setting it on fire. But for Bitcoin advocates, the network's energy gluttony is the necessary price of having a secure digital currency. When judging Bitcoin's energy demands, the advocates continue, keep in mind that mainstream finance is itself no model of efficiency.

Here, I think the advocates have a point.

If you want to argue that Bitcoin is an energy hog, you've got to do more than just point at its energy budget and say 'bad'. You've got to show that this budget is *worse* than mainstream finance.

On this comparison front, there seems to be a vacuum of good information. For their part, crypto promoters are happy to show that Bitcoin uses less energy than the global banking system. But this result is as unsurprising as it is meaningless. Compared to Bitcoin, global finance operates on a vastly larger scale. So *of course* it uses more energy.

To be meaningful, any comparison between Bitcoin and mainstream finance must account for the different scales of the two systems. So instead of looking at energy alone, we need to look at energy *intensity* — the energy per unit of circulating currency. That's what I'll do here. In this post, I compare the energy intensity of Bitcoin to the energy intensity of mainstream US finance.

Which system comes out on top? The results may surprise you.

Proof of energy wasted

Although many people know that the Bitcoin network uses lots of electricity, the reasons for this energy appetite remain widely misunderstood. So before we get to the energy data, it's worth pausing for a brief primer on how the Bitcoin network works.

For starters, the Bitcoin network is nothing but a database — a monetary ledger that records transactions of digital currency. For their part, banks have a similar ledger that tracks how their customers spend money. With banks, however, the database is private and under their exclusive command. Not so with Bitcoin. Think of the Bitcoin database like the banking equivalent of Wikipedia. Anyone can read the ledger, and anyone can (in principle) *write* to it.

Admittedly, this latter part sounds crazy. If anyone can write to the Bitcoin ledger, it means fraud should be pervasive. (Why write a legitimate transaction when you can write a fraudulent one that benefits you?) And that's precisely why write access to Bitcoin's database comes with a caveat. To write transactions to the Bitcoin ledger, you must demonstrate that you've paid a toll. The purpose of this toll is simple: it makes writing to the ledger so expensive that fraud doesn't payoff.

Now here's the interesting part. On the Bitcoin network, the toll is computational. To gain write access to the database, Bitcoin users must demonstrate that they've solved a computationally intensive puzzle. Importantly, the *only* purpose of this puzzle is to prove to the community that you've wasted significant amounts of energy — so much energy that fraud becomes impractical.

Now in crypto circles, this approach is know as 'proof-of-work'. To write a block of transactions to the blockchain (the ledger), you must prove that you've done the work needed to solve a taxing hash problem. But since the 'work' is done exclusively by electricity-guzzling machines, the system is more aptly described as 'proof-of-energy-wasted'. It is a system purposefully designed to waste electricity.

Keeping numbers scarce

Looking at Bitcoin's built-in waste, critics see enormous 'inefficiency'. But I think that's presumptuous. Built-in waste is not unique to cryptocurrency. It's part of all financial systems.

To see this waste, it helps to think about the nature of 'money'. In the most basic sense, money is just a mathematical idea. It's a set of accounting rules attached to a system of property rights. Now, since numbers cost nothing to conjure, there's no physical reason to waste energy on money 'creation'. Anyone can conjure money, anytime they want.

And that's precisely the problem. Numbers are infinitely plentiful. But *money* must be scarce. It is this (artificial) scarcity that converts numbers into 'currency'. Without it, monetary accounting quickly devolves into the children's game of number conjuring:

"I have a *thousand* dollars," says Alice.

"I have a *million* dollars," says Bob.

"I have a *billion* dollars," says Charlotte.

And so on, to infinity.

Adults may laugh at this childhood naivety, but the joke is on us. Numbers can be conjured at will, exactly as the children understand. But what the children don't understand are the (arbitrary) monetary rules that adults have

internalized. To make numbers behave like money, we create rules about how monetary values can be conjured. Break these rules and you haven't 'created' money. You've *forged* it.

It's with 'forgery' that energy enters the picture. You see, it requires energy to ensure that monetary numbers are *not* conjured freely.

Paper cash is a good example of this principle. In essence, cash is a number delivery mechanism — a way to give monetary numbers a physical form. Since it is the *numbers* (not the paper) that matter, the design of a cash bill could be utterly simple — nothing but a digit scrawled on a plain piece of paper. Yet despite this modest requirement, actual cash has an elaborate design. Why?

The purpose of cash's intricate design is to *waste* energy. By giving cash a complicated look, governments enforce monetary scarcity by making number conjuring expensive. If counterfeiters want to print money, they have to waste energy copying the government's design. Sure, a few counterfeiters will take the challenge. But for most people, the cost of mimicking government cash isn't worth the payoff.

And let's not forget the cost of getting *caught*. To maintain their monopoly over money creation, governments actively prosecute and punish 'illegitimate' number conjurers. Like Bitcoin's proof-of-work mechanism, this penal system is nothing but designed-in waste. Its purpose is to maintain monetary scarcity by upping the cost of fraud.[1]

Turning from paper cash to currencies based on precious metal, the built-in waste is even more severe. To conjure metal-based money, we're forced to rip rare elements from the Earth's bowels. With gold, that means wasting about 1.5 megajoules of energy to conjure a single US dollar.[2] It's the antithesis of efficiency. And that's the point. Gold is a universal currency precisely because it's scarcity provides a way to reign in number conjuring. If there *were* some highly efficient method for creating gold — say alchemy — it would ruin gold's monetary appeal.

[1] Fun fact: The US Secret Service — today, known mostly for protecting high-ranking politicians — was created in 1865 for the express purpose of fighting counterfeit US currency.

[2] According to Timothy Gutowski and colleagues, each kilogram of gold takes about 100,000 MJ to produce. At today's gold prices of roughly $67,000 per kilogram, we get a gold energy intensity of about 1.5 MJ per dollar.

With Bitcoin, the situation is similar. Bitcoin's creator, the pseudonymous 'Satoshi Nakamoto', realized that money is simply an accounting ledger that keeps numbers scarce by enforcing a set of rules. How are the rules enforce? By *wasting* energy.

Looking at the prospect of a digital currency, Satoshi decided that it made sense for the scarcity-inducing waste to be computational. Hence we get Bitcoin's use of 'proof-of-work' — a purposefully wasteful algorithm that is designed solely to enforce the rules of the monetary ledger.[3]

So *does* Bitcoin waste loads of energy? Absolutely. But so do all monetary systems. The important question, then, is whether Bitcoin's waste budget is *worse* than other forms of currency. And that remains an open question.

Bitcoin's energy appetite

Lifting the hood of the Bitcoin network, let's now look at its energy demands. Figure 1 shows one of the more rigorous estimates of Bitcoin's evolving energy budget.

The data comes from the Cambridge Bitcoin Electricity Consumption Index (CBECI), and works as follows. The CBECI first looks at the Bitcoin 'hash rate' — the rate that Bitcoin miners guess solutions to their proof-of-work puzzles. Next, the CBECI looks at the technology used for hashing and estimates its 'efficiency' — the hash output per unit of electricity input. Finally, the CBECI divides the hash rate by the hashing efficiency, giving an estimate for Bitcoin's electricity budget.

[3] A common misconception is that Bitcoin mining involves solving 'complex' math problems. But actually, it's more like finding a needle in a haystack. Bitcoin mining involves solving a 'hash' problem, the details of which are not important. What matters is that the only viable method for getting the solution is through trial and error.

On that front, the hash problem is similar to finding prime factors. If you want to reduce a number to its prime factors (i.e. $20 = 2 \times 2 \times 5$), there is only one known method: trial and error. You start with the smallest prime, 2, and see if it's a divisor of n. If it is, you take the resulting quotient and repeat the process. If 2 isn't a divisor, you move to the next prime and try again. Once the quotient is itself a prime number, you're finished.

If n is a very large number, finding its prime factors takes significant computer resources. But once the solution has been found, it's trivial to verify. You simply take the prime factors and confirm that they multiply to n.

With Bitcoin hashes, the same principle applies. The hash problem is intensive to solve but easy to verify. The result is that the network can easily reach a consensus that a miner has done the 'work' required to validate a block of transactions.

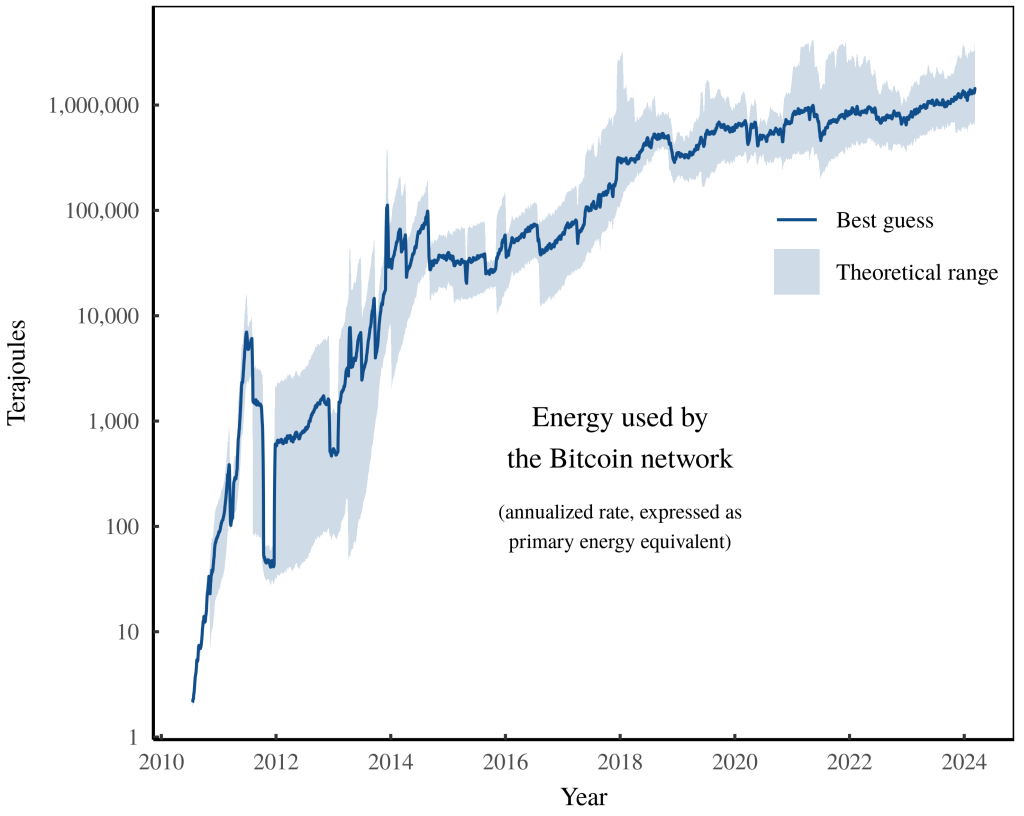

Figure 1: A growing glutton — the energy used by the Bitcoin network
Since its inception in 2010, the Bitcoin network's energy use has grown dramatically. Here, I've plotted energy estimates from the Cambridge Bitcoin Electricity Consumption Index. Note that I've expressed the energy use as an annualized rate in units of primary energy equivalent. Also note the log scale on the vertical axis. Sources and methods

---

In this calculation, the main unknown is the mix of hashing technology used by miners. The CBECI knows which technology is available (on the market), but not what's actually employed. Hence there's significant uncertainty in their energy estimate.

Fortunately, the growth of Bitcoin's energy budget has been so spectacular that the surrounding uncertainty is relegated to background noise. Figure 1 shows the pattern. Over the last fourteen years, Bitcoin's energy thirst has grown by a factor of a *million*. (The shaded region shows the uncertainty in this estimate.)

As of early 2024, Bitcoin's energy budget stands at roughly one million Terajoules. No doubt this number sounds large. However, energy units are notorious for being unintuitive. So before we continue, it's helpful to place Bitcoin's energy consumption on a more understandable scale.

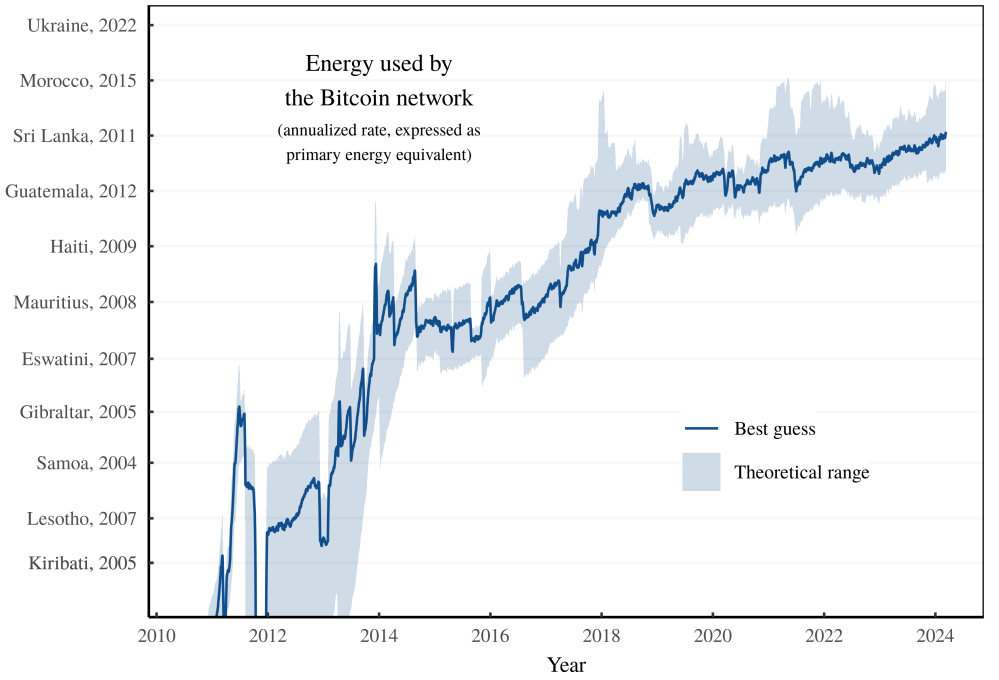

Figure 2: Bitcoin's energy thirst on a country scale

This chart plots the same data as Figure 1, but replaces the Terajoule scale with a country-equivalent scale. Note that the vertical axis uses a log scale. Sources and methods

---

For their part, journalists like to point out that Bitcoin uses more energy than 'entire countries'. It's an apt comparison. Figure 2 show's Bitcoins energy budget on the scale of various countries. When the Bitcoin network first got rolling, it used as much energy as the tiny island nation of Kiribati (population: 100,000). But today, Bitcoin uses as much energy as Sri Lanka (population: 20 million).

Endemic waste in mainstream finance

Now that we've estimated Bitcoin's energy appetite, it's time to do the same for its primary alternative — namely, *mainstream finance*. Here, things get more difficult.

The sticking point has to do with what system scientists call 'boundaries'. To measure the energy used by a system, you've got to first define the boundaries where the system begins and ends. The more expansive your boundaries, the more energy you'll end up counting.

Looking at the mainstream financial system, it's not clear how we should define our energy boundaries. A tempting option is to simply reuse our Bitcoin method and sum the electricity use by banking computers. But I think this approach is a bad idea, because it misunderstands the difference between the two systems.

When you walk into a Bitcoin mining operation, you see nothing but energy-burning computers. But when you walk into a traditional bank, you see much more than that. Sure there are computers. But there's also a brick-and-mortar office building. And most importantly, the bank is full of *people*. Collectively, the finance industry employees millions of people who are generally well paid. It's here that we find mainstream finance's primary form of waste.

Now that I've insulted everyone who works in finance, let me back up a bit. We're not accustomed to treating people's income as a form of 'waste'. So let me make the connection.

Think of Bitcoin as a technology for automating monetary transactions. Instead of having a bureaucracy that manages the monetary ledger, Bitcoin lets computers do the job. As we've seen, this automation leads to the profligate use of electricity — energy which most of us would agree is 'waste'. But if Bitcoin 'wastes' energy on *automating* transactions, it follows that mainstream finance 'wastes' energy on *non-automation*. It pays people to do a job that (conceivably) doesn't need to be done.

So which system is more wasteful. Is it Bitcoin, with its thirst for computation? Or is it mainstream finance, with its reliance on millions of well-paid people?

For his part, Bitcoin's creator thought that the answer was clear. In a 2009 email, Satoshi argued that Bitcoin would be an 'order of magnitude' more efficient than mainstream banking:

> If [Bitcoin] did grow to consume significant energy, I think it would still be less wasteful than the labour and resource intensive conventional banking activity it would replace. The cost would be an order of magnitude less than the billions in banking fees that pay for all those brick and mortar buildings, skyscrapers and junk mail credit card offers.

Was Satoshi correct?

The energy budget of US finance

To judge Satoshi's claims, we need to measure the energy budget of mainstream finance. Here's how I'll do it.

First, I'm going to focus on the US financial system. Second, I'll assume that the energy used by this system stems from the lifestyles of the people it employs. Third, I'll assume that people's energy consumption is a function of their income.

Starting with income, we know that US financial corporations receive about 6% of total American earnings. Assuming this income gets spent on energy, it follows that US finance sucks up about 6% the US energy budget. That equates to about 7 million Terajoules of energy per year. Unsurprisingly, that's far more energy than is consumed by the Bitcoin network. Figure 3 shows the comparison since 2010.

Disparate monetary magnitudes

If I was writing a Bitcoin puff piece, I'd stop here and proclaim Bitcoin's great 'efficiency'. But hopefully, you see why this proclamation is premature.

The problem is one of *scale*.

Mainstream US finance operates on a vastly larger scale than the Bitcoin network. So it's unfair to directly compare the energy budgets of the two systems. To make a fair comparison, we've got to put Bitcoin and mainstream finance on the same footing, which means accounting for their different scales.

How should we do that? Well, since we're talking about two different *monetary* systems, the obvious approach is to sum monetary value. In the case of the Bitcoin network, there are about 19.6 million bitcoins, each priced at roughly $68,000 USD. That pegs Bitcoins' market value at roughly $1.3 trillion USD.

Turning to US finance, the monetary calculation is more complicated, largely because there are many different types of financial instruments. For example, if we take Bitcoin to be 'just another asset', then it makes sense to compare its value to the sea of US corporate assets. Looking only at US public corporations, that sea is valued at roughly $50 trillion USD.

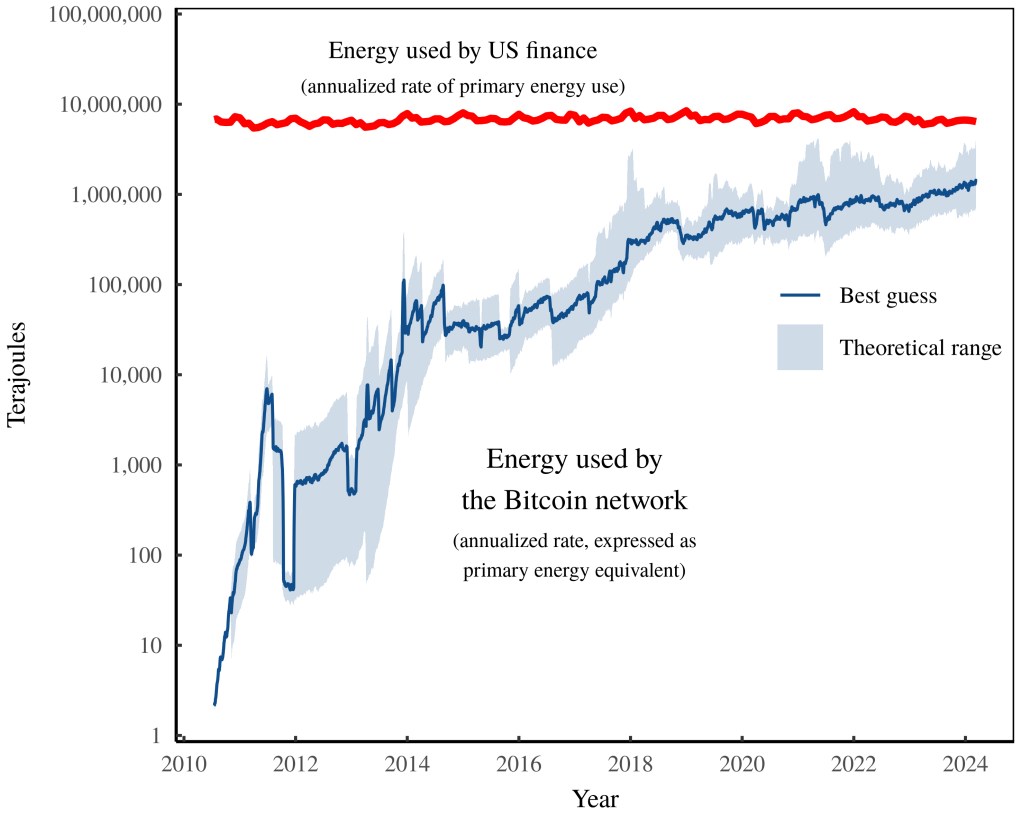

Figure 3: The energy appetite of US finance

While Bitcoin may be an energy glutton, so is US finance. This figure estimates the energy budget of US finance by assuming that finance's share of US income indicates its share of US energy consumption. The red curve shows the resulting estimate. As of late 2023, US finance consumed about 10 times more energy than the Bitcoin network. Note that the vertical axis uses a log scale. Sources and methods

Alternatively, we can treat Bitcoin as a 'cash asset'. In this case, it makes sense to compare its value to the stock of US cash, most commonly measured in terms of the 'M2' stock of money. In what follows, I'll take this latter approach. The idea (which many people will contest) is that Bitcoin aspires to be a universal currency.[4]

[4]Likely because of its ubiquity, 'money' is perhaps the most misunderstood of all social conventions. For that reason, there's a heated debate about whether bitcoin even counts as 'money'. I find this debate utterly boring.

I think Steve Roth gets it right when he defines money as a 'fixed-priced asset' — an asset whose price doesn't change because it is always pegged against itself. What's nice about this definition is that it's delightfully circular. And the same is true of 'money'. An asset becomes 'money' when it is so ubiquitous that it is compared to itself. It follows that 'money' is simply the most dominant form of asset — whatever that may be.

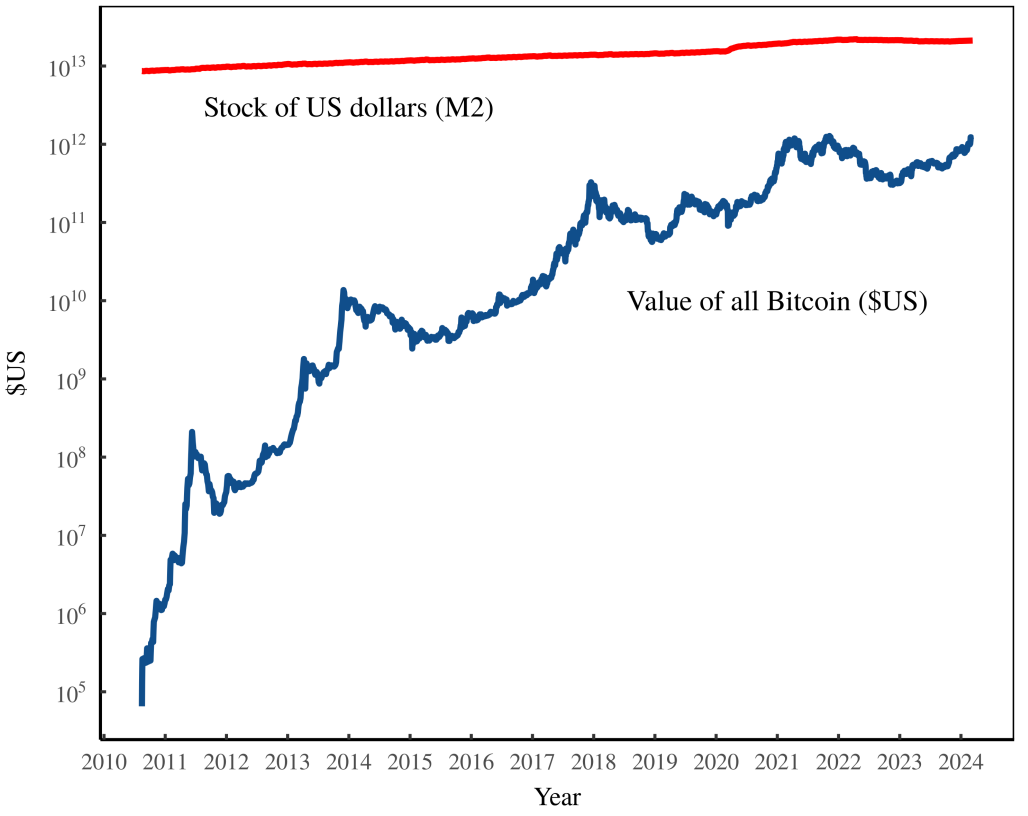

Figure 4: Disparate monetary magnitudes

Despite explosive growth over the last decade, the dollar-value stock of Bitcoin remains about an order of magnitude smaller than the M2 stock of US dollars. Note that the vertical axis uses a log scale. Sources and methods

---

Using the M2 stock of dollars to measure the scale of US finance, Figure 4 shows the degree to which the mainstream financial system dwarfs the Bitcoin network. In 2010, the chasm was enormous — roughly seven orders of magnitude. And even after a decade of explosive growth, the Bitcoin network remains valued at roughly 20 times less than the M2 stock of US dollars.

The energy intensity of Bitcoin relative to US finance

Now that we've measured both energy *and* monetary value, it's time to combine the two measurements. Our goal is to create a fair way to contrast Bitcoin's energy appetite with that of mainstream US finance. Our vehicle for this comparison will be the *energy intensity* of each system — the energy consumed per unit of circulating currency.[5]

To calculate Bitcoin's energy intensity, we take its energy budget and divide by its market value (measured in US dollars):

$$\text{Bitcoin energy intensity} = \frac{\text{Bitcoin energy use}}{\text{Bitcoin market value}}$$

Likewise, for US finance, we take the energy consumed by US finance (the energy required to support the lifestyles of everyone who works in finance) and divide by the M2 stock of US dollars. The result is the energy intensity of mainstream finance:

$$\text{US finance energy intensity} = \frac{\text{US finance energy use}}{\text{M2 money stock of USD}}$$

The caveat is that when viewed in isolation, these energy-intensity estimates are useless. That's because monetary value is only meaningful as a point of comparison. So the final step of our analysis will be to compare Bitcoin's energy intensity to that of US finance:

$$\text{energy intensity ratio} = \frac{\text{Bitcoin energy intensity}}{\text{US finance energy intensity}}$$

Plugging the data into our energy-intensity ratio gives the pattern shown in Figure 5. Immediately, we can dismiss Satoshi's claim that Bitcoin is an 'order of magnitude' more efficient than mainstream finance. If anything, the opposite is true. Since 2010, the Bitcoin network has, on average, been about 13 times more energy intensive than mainstream US finance.

[5] I'm anticipating that some people will interpret my energy intensity ratio as a measure of the energy needed to 'create' money. But that is *not* what it means. As I've taken pains to explain, money is just a number, and numbers are free. The energy put into financial systems is driven by the need to keep numbers scarce. Enforcing accounting rules is a costly business.

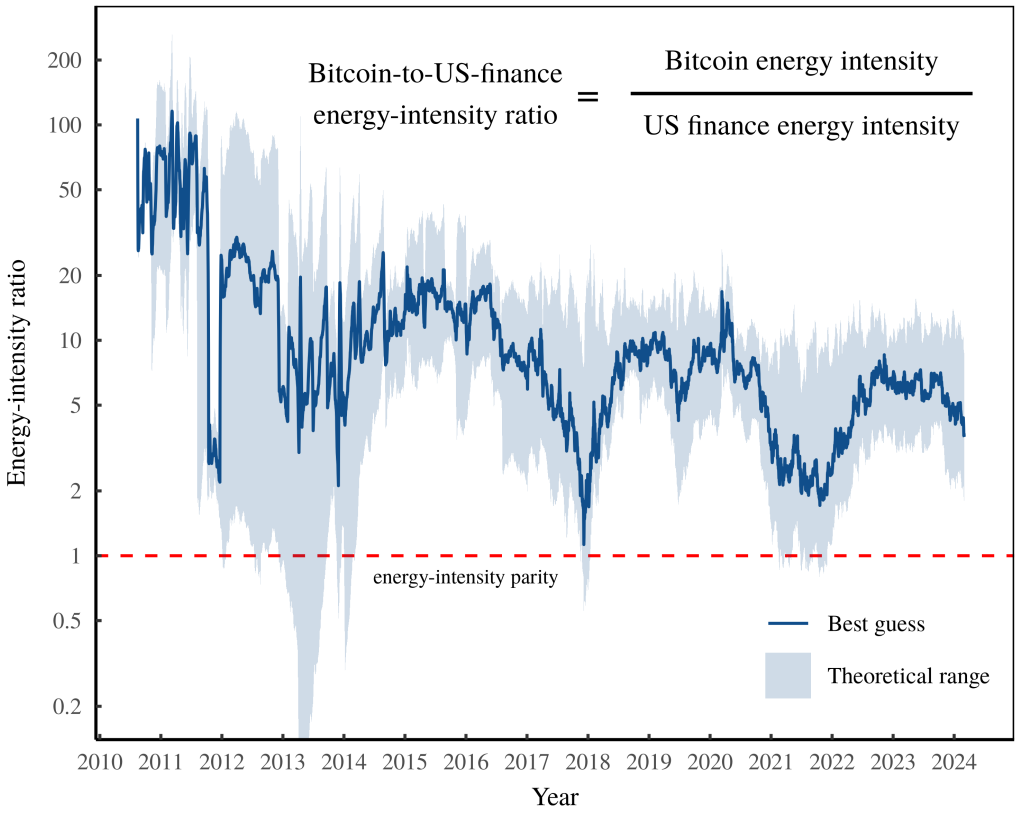

Figure 5: The energy intensity of Bitcoin relative to mainstream US finance

By accounting for monetary scale, this figure puts the energy budget of Bitcoin on equal footing with the energy budget of US finance. The blue curve shows the ratio between Bitcoin's energy intensity and US finance's energy intensity. I calculate Bitcoin's energy intensity by dividing Bitcoin's energy budget (Figure 1) by its market value (Figure 4). Similarly, I calculate the energy intensity of mainstream US finance by dividing its energy budget (Figure 3) by the US stock of M2 dollars (Figure 4). The shaded region indicates a plausible range for the energy-intensity ratio based on uncertainty in Bitcoin's energy use. The blue line indicates the best guess. Note that the vertical axis uses a log scale. Sources and methods

---

Looking closely at Figure 5, we see that Bitcoin's worst period of waste was early on. In 2010 — long before anyone complained that Bitcoin was wasting loads of energy — the network sucked up about *50 times* the energy of mainstream finance (dollar for dollar). To put that number in context,

if Bitcoin had been scaled up to replace the circulation of US dollars, the Bitcoin network would have use about 3 times more energy than the *entire US population*.[6] Outrageous.

Energy parity . . . and beyond?

In Figure 5, the main story is that compared to US finance, Bitcoin has historically been significantly more energy intensive. But looking closely at the evidence, there's a subplot that we shouldn't ignore.

Over the last decade, it seems that the Bitcoin network has steadily closed the energy gap with US finance. Instead of being 50 times more energy intensive (as it was in 2010), today, Bitcoin is about 4 times more energy intensive. That's a tenfold improvement. Intriguingly, if we project this improvement into the future, we find that Bitcoin may soon reach energy-intensity parity with US finance.

Figure 6 runs the numbers. A naive guess suggests that energy-intensity parity will arrive in the early 2030s. And if the trend continued, Bitcoin would then start to burn *less* energy (dollar for dollar) than US finance.[7] Will this parity actually happen? Only time will tell.

Proof-of-stake: a less wasteful method for network consensus

They say that Bitcoin is 'digital gold'. But unlike actual gold mining, there's no physical reason that Bitcoin 'miners' must burn energy 'harvesting' bitcoins. The coins themselves are conjured numbers, and the 'mining' process is simply a software algorithm. And algorithms can be changed.

[6] In 2010, US finance accrued about 6% of US income. Assuming that this income got burned on energy, it follows that US finance used about 6% of US energy. Now assume we replace all dollars with bitcoin. In 2010, the Bitcoin network was about 50 times more energy intensive than mainstream finance. It follows that the bitcoin replacement would increase finances' energy demands by fifty-fold, to a total of 300% of US total energy consumption.

[7] What's driving Bitcoin's decreasing energy intensity? Two things. First, the technology used for hashing has grown steadily more efficient. Second, the price of Bitcoin (in US dollars) has grown rapidly, which means that each Bitcoin transaction pushes around more dollar value.

This second pattern points to a feature of Bitcoin than many critics miss. It's build-in waste is tied to the transaction of *bitcoin*. But there is nothing that restricts what this transaction is worth in dollars. In other words, if a single bitcoin transaction pushes around a few dollars worth of value, then the exchange is horribly inefficient. But if the same transaction pushes around a billions dollars of value, it becomes highly efficient.

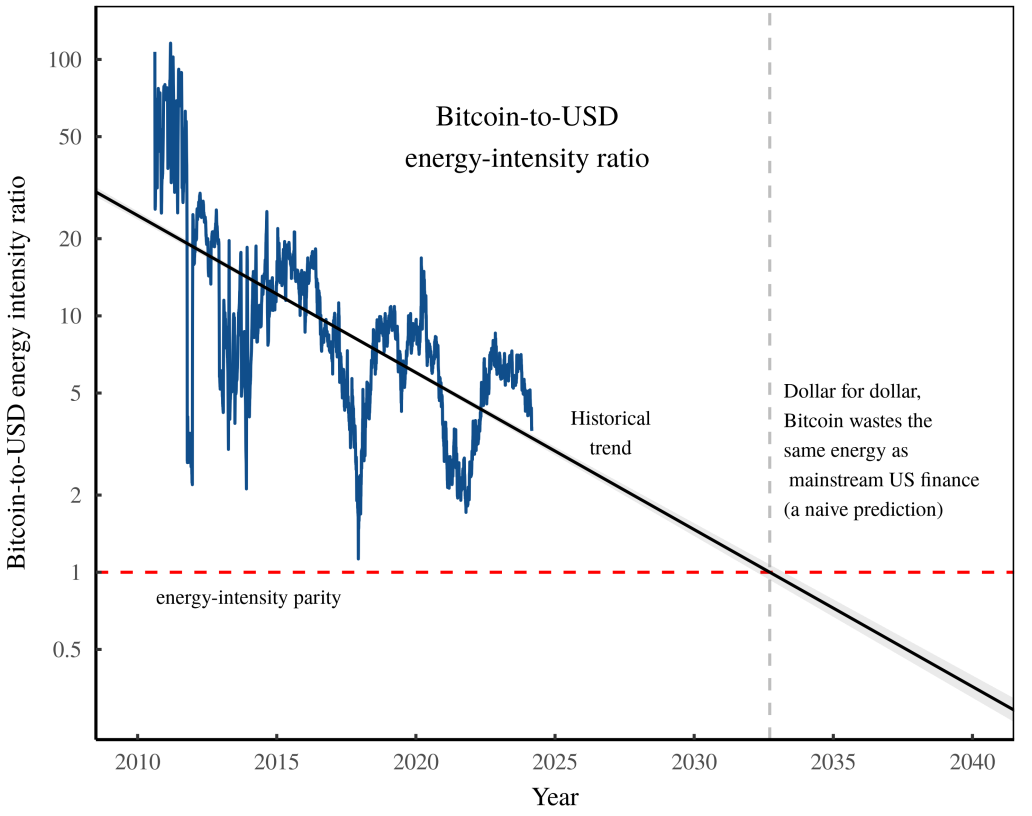

Figure 6: Will Bitcoin reach energy-intensity parity with mainstream US finance?

If we take historical data for the Bitcoin-to-USD energy-intensity ratio and fit it with a simple regression, we get the black line shown here. That line predicts that Bitcoin will reach energy-intensity parity with mainstream US finance sometime in 2032. Will this parity actually happen? We'll have to wait and see. Sources and methods

---

To recap, the function of Bitcoin 'mining' is to police the monetary ledger. Because Bitcoin has no governing institution, anyone is free to validate a transaction and write it to the 'blockchain'. But that freedom also means anyone can commit fraud. The purpose of 'mining' is to stop fraud by making it so expensive that it's impractical. To confirm a set of transactions, miners must demonstrate that they've wasted energy on a pointless computation. The reward for this 'proof-of-work' is a small amount of bitcoin.

As we've seen, the proof-of-work algorithm is no model of efficiency. It achieves consensus by wasting loads of energy. And that's got cryptocurrency designers looking for different consensus-generating algorithms.

A promising alternative is a design called 'proof-of-*stake*'. Here's how it works.

Instead of letting users compete to validate transactions, the proof-of-stake algorithm uses a lottery. When it's time to validate a 'block', a user is chosen at random from a pool of validators. The catch is that to get into this validator pool, you must put up a certain amount of currency as a 'stake'. Like Bitcoin's wasted computation, the purpose of this stake is to stop fraud. If a user 'validates' a fraudulent transaction, they risk losing their stake.

Because proof-of-stake (largely) does away with pointless calculations, it's a more energy efficient design. Or at least, that's the expectation.

The energy intensity of Ethereum

To measure the energy intensity of the proof-of-stake algorithm, we'll look at Ethereum, the second largest cryptocurrency.

Created in 2015, the Ethereum network ran for almost a decade on the proof-of-work algorithm. During that time, its energy intensity was similar to Bitcoin. Figure 7 shows the data. From late 2015 to mid 2022, Ethereum was on average about 4 times more energy intensive than mainstream US finance.

Then something dramatic happened. On September 15, 2022, Ethereum switched its codebase to the proof-of-stake algorithm. (In crypto circles, the event is known as 'The Merge'.) The result was a colossal drop in energy intensity. In Figure 7, the transition is easy to spot. Over the course of a day, Ethereum's energy intensity plummeted by four orders of magnitude. So in terms of reducing crypto's energy demands, the proof-of-stake algorithm seems like a no brainer.

Just the facts

Looking at the evidence in Figures 5 and 7, we can conclude two things about crypto.

First, coins like Bitcoin, which are based on the proof-of-*work* algorithm, are likely more energy intensive than mainstream finance. (But note that this intensity seems to be declining with time.) Second, coins like Ethereum, which are based on the proof-of-*stake* algorithm, are likely (far) less energy intensive than mainstream finance.

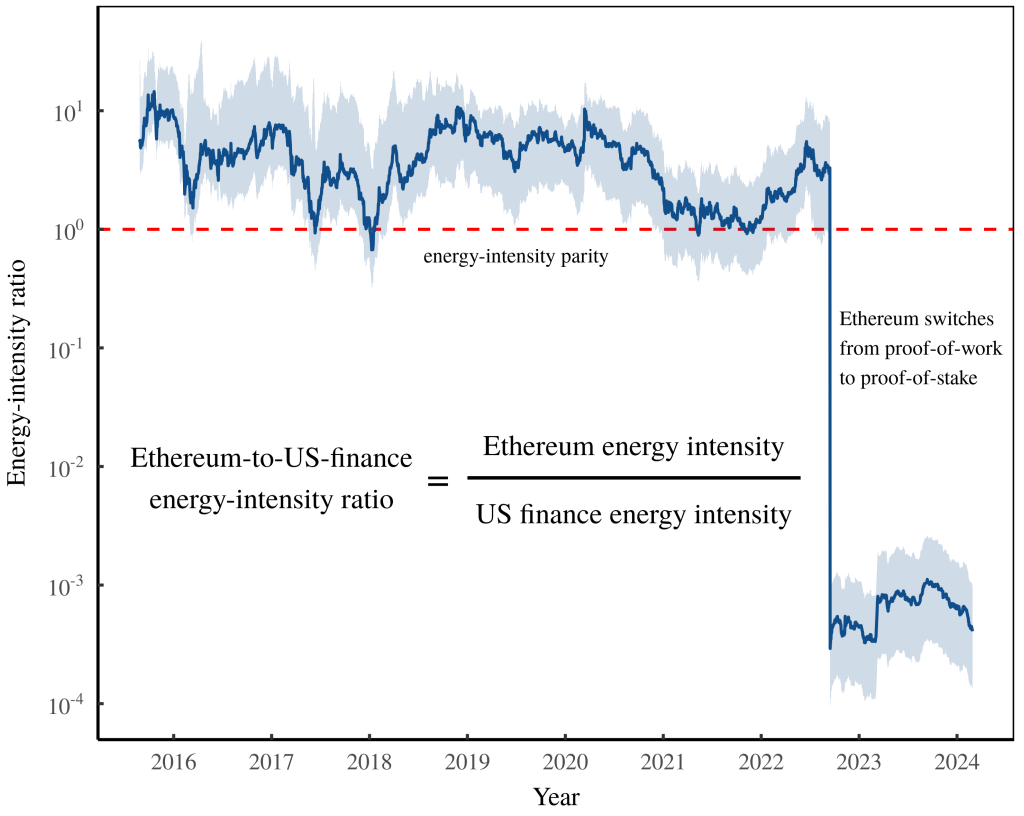

Figure 7: The energy intensity of Ethereum relative to mainstream US finance

Created in 2015, Ethereum ran for almost a decade using the proof-of-work algorithm. During that time, its energy intensity was similar to Bitcoin's — about four times more energy intensive than US finance. Then on September 15, 2022, Ethereum switched to the proof-of-stake approach. The result was a dramatic drop in energy intensity. Note that the vertical axis uses a log scale. Sources and methods

---

So that's what the data says. But somehow, I feel like this evidence will satisfy neither the crypto critics nor the crypto advocates. And that's why in the appendix, I add some obligatory speculation. But for now, let's conclude with just the facts. To date, it seems clear that Satoshi's claims about Bitcoin's superior 'efficiency' have *not* come to fruition.

Support this blog

Hi folks. I'm a crowdfunded scientist who shares all of his (painstaking) research for free. If you think my work has value, consider becoming a supporter.

Some obligatory speculation about the future of crypto

When it comes to crypto, the hate and love turns almost entirely on feelings about its *purpose*. And that's actually important, because purpose affects how we define 'efficiency'.

For example, the efficiency of a machine is typically measuring in terms of the work output per unit of energy input. But what happens when we make the machine do work that is *useless*? (Think of an excavator digging pointless holes and then filling them in.) In this case, *all* of the input energy gets wasted.

Returning to crypto, I'm expecting critics to argue that my energy-intensity estimates are silly for the same reason. Crypto, they'll observe, is the monetary equivalent of pointless hole digging. It's purpose isn't to facilitate commerce. Instead, it's a beast of socially-useless speculation.

While I'm sympathetic to this argument, I think the problem of crypto speculation tends to get overplayed. In particular, it ignores the fact that speculation plagues *all* forms of money.

When critics look a Bitcoin, they see an asset that is too volatile to be 'real' money. But a quick look at international money markets shows that 'real' (fiat) money can also be highly volatile. Figure 8 paints the picture.

Here, the blue curve shows the spread of exchange-rate volatility among the world's currencies (when pegged against the US dollar). When we put Ether and Bitcoin on this international scale, we find that they're on the high end of currency volatility. But they're certainly not off the chart. In other words, on the scale of actually existing money, there is nothing 'abnormal' about crypto volatility. Hence there is nothing 'abnormal' about crypto speculation.

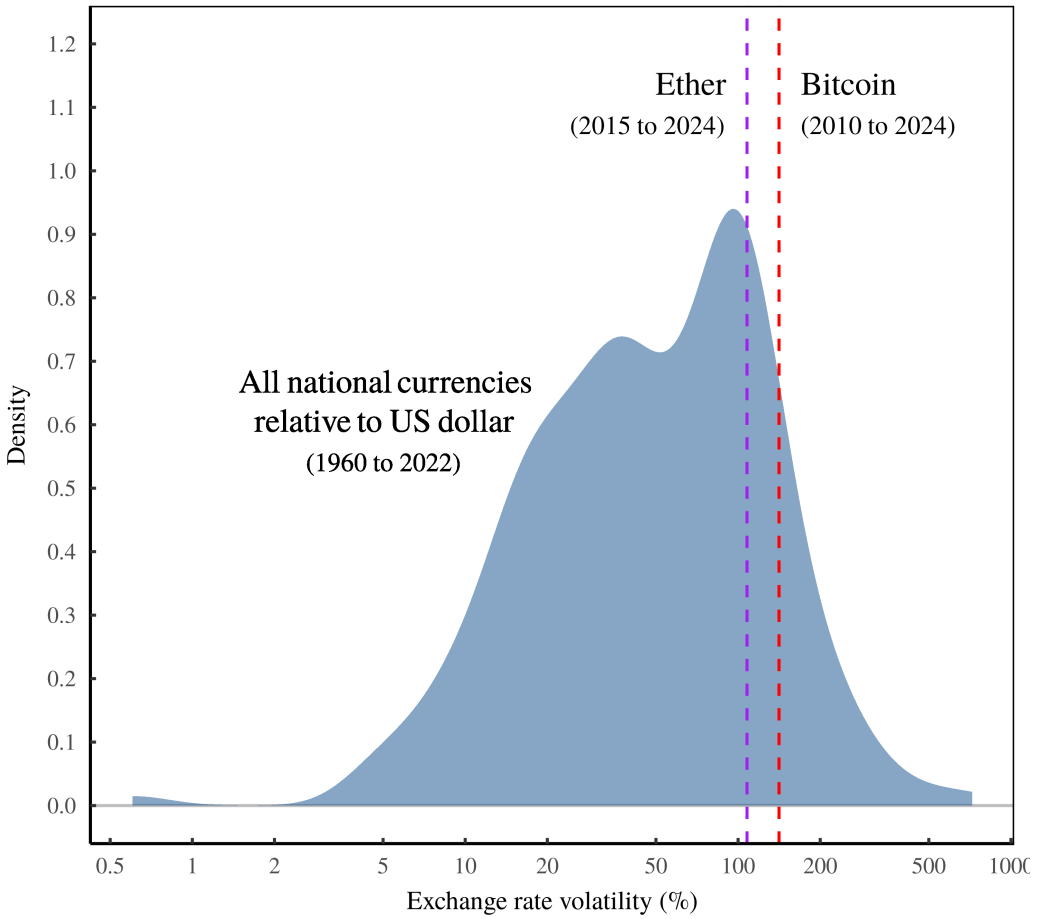

Figure 8: Cryptocurrency volatility in an international context

This figure measure the exchange-rate volatility of different currencies when pegged against the US dollar. (I've measure volatility by plugging the exchange rate annual time series into the coefficient of variation.) The blue curve shows the distribution of volatility among national currencies. The vertical lines show the historical volatility of Ether and Bitcoin. Note that the horizontal axis uses a log scale. Sources and methods

---

Still, the critics are right to pass judgment on crypto as a relatively volatile asset. But where I disagree with the critics is that this volatility makes crypto forever unsuitable for commerce. The reality is that the difference between a volatile 'asset' and stable form of 'money' is simple: it's a function of *hegemony*.

What makes a currency stable is its dominance. When most prices are denominated in a particular unit, that unit loses its speculative appeal. In other words, if Bitcoin became the world's dominant asset, it would behave exactly

like cash — stable and boring.[8] In short, crypto's 'usefulness' as a stable form of money depends on its ability to gain global dominance as a medium of exchange.

Hurdles to a crypto-dominated future

Thinking about a crypto-dominated future, there are many hurdles to it actually happening. Here's a short list.

Lack of scalability

Despite being built on stupendous computational power, crypto networks are typically quite slow at processing transactions. For example, the Bitcoin network maxes out at roughly 4 transactions per second.[9] And the Ethereum network can handle about 20 transactions per second. In contrast, global credit-card networks process about 10,000 transactions per second.[10] So as they currently stand, the Ethereum and Bitcoin networks can't scale to meet the needs of global commerce.

Interestingly, the cause of this high latency is part of the network design. The idea is that when choosing between security, decentralization, and scalability, you can only have two of the three. So networks like Bitcoin and Ethereum choose security and decentralization, but sacrifice scalability. Credit card networks, on the other hand, achieve scalability by choosing centralization and remarkably little security.

(In the age of online shopping, the security principle of credit cards is effectively "here is my secret number, please don't use it unless I ask you to".)

Of course, crypto advocates are aware that their networks need to be faster. To make that happen, one option is to build so-called 'layer 2' systems on top of cryptocurrency networks. For example, the Lightning network is a layer 2 system that runs on top of the Bitcoin network.

In conceptual terms, layer 2 systems work much like a credit account. For example, if Business A deals repeatedly with Business B, Business B will typically offer Business A a line of credit. The idea is that instead of using

[8] The irony here is that many crypto bros want Bitcoin to be both a speculative asset *and* the world's dominant currency. Sorry bros, but you can't have both.

[9] Since 2017, the number of Bitcoin transactions has hovered around 10 million per month. That equates to about 3.8 transactions per second

[10] According to cardrates.com, there were about 368.92 billion credit-card transactions in 2018. That equates to about 11,700 transactions per second.

cash to clear every transaction, Business B keeps track of the *net* value of Business A's purchases. Then every month, Business B sends a bill to settle the account.

In a similar vein, layer 2 systems allow crypto users to setup 'channels' in which transactions can occur off the blockchain. When users decide to close a channel, the net value of all transaction is then settled on the main ledger. By grouping many transactions under a single blockchain settlement, layer 2 systems can vastly increase the capacity of crypto networks. For example, the Lightning network claims to be capable of handling millions of transactions per second.

What remains to be seen is whether layer 2 systems will achieve widespread adoption. To date, of the roughly 19 million bitcoin in existence, only 5000 circulate in the Lightning network.

Government power

Setting aside the (current) technical shortcomings of crypto networks, I think the main hurdles to a crypto-dominated future are institutional. Let's start with government.

If crypto become the dominant form of money, it follows that governments would lose sovereign control of their national currencies. Now, we can debate whether this loss would be good or bad. But I think we can agree that it represents a significant loss of power — a loss that governments would be reticent to accept. So in my mind, the route to crypto dominance requires the demise of (or significant diminution of) the nation state.

Bank power

Other than governments, the institutions most invested in the existing financial system are undoubtedly banks. And that's because they have the power to create money by issuing credit.

In a crypto-dominated world, I find it unlikely that banks would simply relinquish this power. Instead, they'd likely start issuing crypto-based credit. But once this crypto credit started flowing, the credit itself would become the dominant currency.

The situation would be similar to the Bretton Woods system, in which bank notes were theoretically backed by gold reserves. But the 'backing' was completely notional. The gold itself didn't circulate and was almost never used as a medium of exchange. As Nixon realized, it was just as easy to cut the cord and admit that money was backed by nothing but social will.

In short, if banks retain the power to issue credit, I see nothing to gain from a crypto future, and no feasible path to actual crypto dominance.

Sources and methods

Cover image: the bitcoin-dollar-scale image is from the Wikimedia commons. The smokestack image is from Grigoriy via Pexels.

Bitcoin energy use

Estimates for Bitcoin energy use are from the Cambridge Bitcoin Electricity Consumption Index. The estimates are constructed by taking the hashing rate in the Bitcoin network (which is publicly available) and multiplying it by the hashing efficiency (i.e. hash per Watt) of available technology.

This hashing efficiency is the main unknown. To estimate it, the CBECI looks at the available Bitcoin mining technology (technology which changes over time). Here's the gist of their calculation.

If all miners used the *most efficient* technology on the market, we get a *lower bound* for the energy used by the Bitcoin network. If all miners used the *least efficient* technology that was still profitable (at an assumed electricity price of 5 cents per kWh), we get an *upper bound* for Bitcoin energy use. The *best guess* is somewhere in the middle of this range.

Note that the CBECI reports Bitcoin's *electricity use*. To compare this electricity use to US *primary energy* consumption, I convert it to a primary-energy equivalent. See the conversion notes here.

Bitcoin market value

Data for the number of Bitcoins in circulation is from blockchain.com.

Data for Bitcoin price comes from two sources:

- 2009-01-03 to 2014-09-14: blockchain.com.
- 2014-09-17 to present: downloaded using the R tidyquant package

Ethereum energy use

Estimates for Ethereum electricity use come from the Cambridge Bitcoin Electricity Consumption Index. Data for Ethereum's proof-of-work period live here. Data for its proof-of-stake period live here.

For the proof-of-work period, the CBECI uses the same estimation methods as for Bitcoin. (It multiplies the hash rate by the estimated hashing efficiency of existing technology.)

For the proof-of-work period, the CBECI counts Ethereum nodes, and then estimates the power draw of an average node. These power estimates come from the Crypto Carbon Ratings Institute's 2022 report 'The Merge'.

Note that the CBECI reports Ethereum electricity use. To compare this electricity use to US primary energy consumption, I convert it to a primary-energy equivalent. See the conversion notes here.

Ethereum market value

Data for Ethereum's total value (and the price of Ether) is from coingecko.com.

Exchange rates

Data for historical exchange rates (Figure 8) is from the World Bank, series PA.NUS.FCRF.

Energy used by US finance

Estimates for the energy used by US finance work as follows:

1. Calculate finance's share of US income. I do that by dividing the value added of US financial corporations (FRED series A454RC1Q027SBEA) by US nominal GDP (FRED series GDP).
2. Multiply finance's share of US income by US total energy consumption. Energy consumption is from the Energy Information Agency, series TETCBUS (total primary energy consumption)

Converting electricity to primary energy equivalent

Despite the growth of renewable energy sources, most electricity is still produced by burning fossil fuels (or what statistical agencies call 'primary energy sources'.)

Now, because thermo-electric power plants are not 100% efficient, more fossil-fuel energy goes into these plants than comes out in electricity. As a result, it's not fair to compare electricity consumption directly to fossil-fuel use — it's an apples-oranges comparison.

Turning to Bitcoin, its energy consumption is reported in terms of electricity use. But we want to compare this to the primary energy (read fossil fuels) used by US finance. To make the comparison, we need to convert electricity into a primary-energy equivalent.

I do that using US data from the Energy Information Agency. I take data for the total total primary energy consumed by the electric power sector (series TXEIBUS) and divide it by the net electricity generation of the electric power sector (series ELEGPUS). The result is the primary energy intensity of US electricity. I then multiply Bitcoin electricity use by this primary energy intensity. The result is Bitcoin energy use expressed as a primary energy equivalent.

Note: due to changing energy mixes, the primary energy intensity of US electricity is a moving target, as shown in Figure 9.

Further reading

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. http://satoshinakamoto.me/bitcoin.pdf

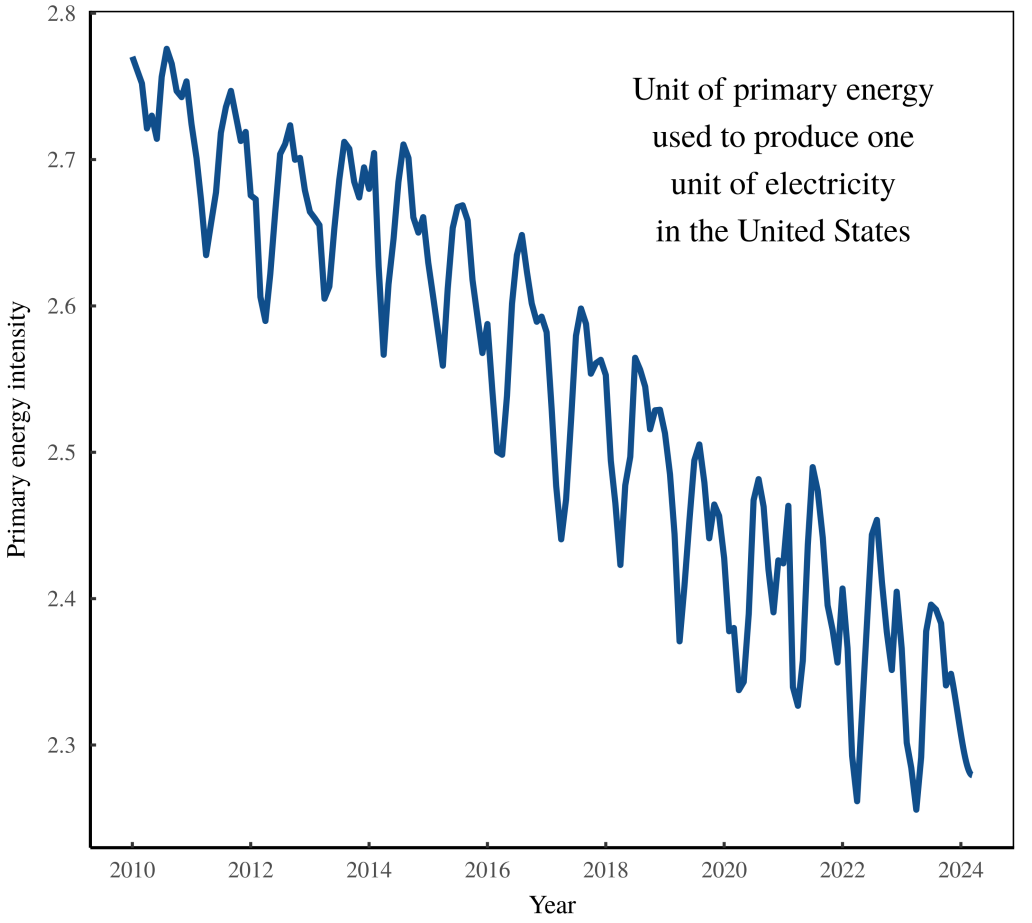

Figure 9: The primary energy intensity of US electricity

Because most electricity comes from fossil fuels, more 'primary energy' goes into the generation process than comes out as electricity. This figure shows the evolving primary energy intensity of US electricity.