

Cryptocurrency

- [No, your cryptocurrency cannot work](#)
- [Is my blockchain a blockchain?](#)
- [You don't need a blockchain.](#)

No, your cryptocurrency cannot work

This article was originally published at

<https://gist.github.com/joePie91/daa93b9686f554ac7097158383b97838>.

Whenever the topic of Bitcoin's energy usage comes up, there's always a flood of hastily-constructed comments by people claiming that *their* favourite cryptocurrency isn't like Bitcoin, that *their* favourite cryptocurrency is energy-efficient and scalable and whatnot.

They're wrong, and are quite possibly trying to scam you. Let's look at why.

What *is* a cryptocurrency anyway?

There are plenty of intricate and complex articles trying to convince you that cryptocurrencies are the future. They usually heavily use jargon and vague terms, make vague promises, and generally give you a sense that there must be *something* there, but you always come away from them more confused than you were before.

That's not because you're not smart enough; that's because such articles are *intentionally* written to be confusing and complex, to create the impression of cryptocurrency being some revolutionary technology that you *must* invest in, while trying to obscure that it's all just smoke and mirrors and there's really not much to it.

So we're not going to do any of that. Let's look at what cryptocurrency *really is*, the fundamental concept, in simple terms.

A cryptocurrency, put simply, is a currency that is not controlled by an appointed organization like a central bank. Instead, it's a system that's built out of *technical rules*, code that can independently decide whether someone holds a certain amount of currency and whether a given transaction is valid. The rules are defined upfront and difficult for anybody to change afterwards, because some amount of 'consensus' (agreement) between the systems of different users is needed for that. You can think of it kind of like an automated voting process.

Basically, **a cryptocurrency is a currency that is built as software**, and that software runs on many people's computers. On paper, this means that "nobody controls it", because everybody has to play by the predefined rules of the system. In practice, it's unfortunately not that simple, and

cryptocurrencies end up being heavily centralized, as we'll get to later.

So why does Bitcoin need so much energy?

The idea of a currency that can be entirely controlled by independent software *sounds* really cool, but there are some problems. For example, how do you prevent one person from convincing the software that they are actually a *million* different people, and misusing that to influence that consensus process? If you have a majority vote system, then you want to make really sure that everybody can only cast one vote, otherwise it would be really easy to tamper with the outcome.

Cryptocurrencies try to solve this using a 'proof scheme', and Bitcoin specifically uses what's called "proof of work". The idea is that there is a finite amount of computing power in the world, computing power is expensive, and so you can prevent someone from tampering with the 'vote' by requiring them to do some difficult computations. After all, computations can be automatically and independently checked, and so nobody can pretend to have more computing power than they really do. So that's the problem solved, right?

The underlying trick here is to make a 'vote' require the usage of something scarce, something relatively expensive, something that you can't just infinitely wish into existence, like you could do with digital identities. It makes it costly *in the real world* to participate in the network. That's the core concept behind a proof scheme, and it is *crucial* for the functioning of a cryptocurrency - without a proof scheme requiring a scarce resource of some sort, the network cannot protect itself and would be easy to tamper with, making it useless as a currency.

To incentivize people to actually *do* this kind of computation - keep in mind, it's expensive! - cryptocurrencies are set up to *reward* those who do it, by essentially giving them first dibs on any newly minted currency. This is all fully automated based on that predefined set of rules, there are no manual decisions from some organization involved here.

Unfortunately, we're talking about *currencies*, and where there are currencies, there is money to be made. And many greedy people have jumped at the chance of doing so with Bitcoin. That's why there are entire datacenters filled with "Bitcoin miners" - computers that are built for just a single purpose, doing those computations, to get a claim on that newly minted currency.

And *that* is why Bitcoin uses so much energy. As long as the newly minted coins are worth *slightly* more than the cost of the computations, it's economically viable for these large mining organizations to keep building more and more 'miners' and consuming more and more energy to stake their claim. This is also why energy usage will always go up alongside the exchange rate; the more a Bitcoin is 'worth', the more energy miners are willing to put into obtaining one.

And that's a fundamental problem, one that simply cannot be solved, because it is so crucial to how Bitcoin works. **Bitcoin will forever continue consuming more energy** as the exchange rate rises, which is currently happening due to speculative bubbles, but which would happen if it

gained serious real-world adoption as well. If everybody started using Bitcoin, it would essentially eat the world. There's no way around this.

Even renewable energy can't solve this; renewable energy still requires polluting manufacturing processes, it is often difficult to scale, and it is often more expensive than fossil fuels. So in practice, "mining Bitcoins on renewable energy" - insofar that happens *at all* - means that all the renewable energy you are now using could not be distributed to factories or households, and they have to continue running on non-renewable energy instead, so you're just shuffling chairs! And because of the endless growth of Bitcoin's energy consumption, it is pretty much guaranteed that those renewable energy resources won't even be *enough* in the end.

So there's this proof-of-stake thing, right?

You'll often see 'proof of stake' mentioned as an alternative proof scheme in response to this. So what is that, anyway?

The exact implementations vary and can get very complex, but every proof-of-stake scheme is basically some variation of "instead of the scarce resource being energy, it's *the currency itself*". In other words: the more of the currency that you own, the more votes you have, the more control you have over how the network (and therefore the currency) works as a whole.

You can probably begin to see the problem here already: if the currency is controlled by those who have most of it, how is this any different from government-issued currency, if it's the wealthy controlling the financial system either way? And you'd be completely right. There *isn't* really a difference.

But what you might not realize, is that this applies for proof-of-work cryptocurrencies *too*. The frequent claim is that Bitcoin is decentralized and controlled by nobody, but that isn't really true. Because who can afford to invest the most in specialized mining hardware? Exactly, the wealthy. And in practice, almost the entire network is controlled by a small handful of large mining companies and 'mining pools'. Not very decentralized at all.

The same is true for basically every other proof scheme, such as Chia's "proof of space and time", where the scarce resource is just "free storage space". Wealthy people can afford to buy more empty harddrives and SSDs and gain an edge. Look at *any* cryptocurrency with *any* proof scheme and you will find the same problem, because it is a fundamental one - if power in your system is handed out based on ownership of a scarce resource of *some* sort, the wealthy will *always* have an edge, because they can afford to buy whatever it is.

In other words: it doesn't actually matter what the specific scarce resource is, and **it doesn't matter what the proof scheme is!** Power will always centralize in the hands of the wealthy, either those who already were wealthy, or those who have recently gotten wealthy with cryptocurrency through dubious means.

The only redeeming feature of proof-of-stake (and many other proof schemes) over proof-of-work is that it *does* indeed address the energy consumption problem - but that's little comfort when none of these options actually *work* in a practical sense anyway. This is ultimately a socioeconomic problem, not a technical one, and so you can't solve it with technology.

And that brings us to the next point...

Yes, cryptocurrencies are effectively pyramid schemes

While Bitcoin was not *originally* designed to be a pyramid scheme, it is very much one now. Nearly every other cryptocurrency was designed to be one from the start.

The trick lies in encouraging people to buy a cryptocurrency. Whoever is telling you that *their* favourite cryptocurrency is the real deal, the solution to all problems, probably is holding quite a bit of that currency, and is waiting for it to appreciate in value so that they can 'cash out' and turn a profit. The way to make that value appreciation happen, is by trying to convince people **like you** to 'invest' or 'get in' on it. If you buy the cryptocurrency, that will drive up the price. If a *lot* of people buy the cryptocurrency, that will drive up the price *a lot*.

The more hype you can create for a cryptocurrency, the more profit potential there is in it, because more people will 'buy in' and drive up the price before you cash out. This is why there are flashy websites for cryptocurrencies promising the world and revolutionary technology, this is why people on Twitter follow you around incessantly spamming your replies with their favourite cryptocurrency, this is why people take out billboards to advertise the currency. It's a pump-and-dump stock.

This is also the reason why proponents of cryptocurrencies are always so mysterious about how it works, invoking jargon and telling you how much complicated work 'the team' has done on it. The goal is to make you believe that 'there must be something to it' for long enough that you will buy in and they can sell off. By the time you figure out it was all just smoke and mirrors, they're long gone with their profits.

And then the only choice to recoup your investment is for *you* to hype it up and try to replicate the rise in value. Like a pyramid scheme.

The bottom line

Cryptocurrency as we know it today, simply cannot work. It promises to decentralize power, but proof schemes *necessarily* give an edge to the wealthy. Meanwhile there's every incentive for people to hype up worthless cryptocurrencies to make a quick buck, all the while disrupting supply chains (GPUs, CPUs, hard drives, ...), and boiling the earth through energy usage that far exceeds that of *all of Google*.

Maybe some day, a legitimate cryptocurrency *without* Bitcoin's flaws will come to exist. If it does, it will be some boring research paper out of an academic lab in three decades, not a flashy startup promising easy money or revolutionary new tech today. There are no useful cryptocurrencies today, and there will not be any at any time in the near future. The tech just doesn't work.

Is my blockchain a blockchain?

This article was originally published at

<https://gist.github.com/joepie91/e49d2bdc9dfec4adc9da8a8434fd029b>.

Your blockchain must have *all* of the following properties:

- It's a merkle tree, or a construct with equivalent properties.
- There is no single point of trust or authority; nodes are operated by different parties.
- Multiple 'forks' of the blockchain may exist - that is, nodes may disagree on what the full sequence of blocks looks like.
- In the case of such a fork, there must exist a deterministic consensus algorithm of some sort to decide what the "real" blockchain looks like (ie. which fork is "correct").
- The consensus algorithm must be executable with *only* the information contained in the blockchain (or its forks), and no external input (eg. no decisionmaking from a centralized 'trust node').

If your blockchain is missing *any* of the above properties, **it is not a blockchain, it is just a ledger.**

You don't need a blockchain.

This article was originally published at

<https://gist.github.com/joepie91/a90e21e3d06e1ad924a1bfdf3c16902>.

If you're reading this, you probably suggested to somebody that a particular technical problem could be solved with a blockchain.

Blockchains aren't a desirable thing; they're defined by having [trustless consensus](#), which necessarily has to involve some form of [costly signaling](#) to work; that's what prevents attacks like [sybil attacks](#).

In other words: blockchains *must* be expensive to operate, to work effectively. This makes it a last-resort solution, when you truly have no other options available for solving your problem; in almost every case you want a cheaper and less complex solution than a blockchain.

In particular, **if your usecase is commercial, then you do not need or want trustless consensus**. This especially includes usecases like supply chain tracking, ticketing, and so on. The whole *point* of a company is to centralize control; that's what allows a company to operate efficiently. Trustless consensus is the exact opposite of that.

Of course, you may still have a problem of trust, so let's look at some common solutions to common trust problems; solutions that are a better option than a blockchain.

- **If you just need to provide authenticity for a piece of data:** A cryptographic signature. There's plenty of options for this. Learn more about basic cryptographic concepts [here](#).
- **If you need an immutable chain of data:** Something simple that uses a [merkle tree](#). A well-known example of this application is [Git](#), especially in combination with [signed commits](#).
- **If that immutable chain of data needs to be added to by multiple parties (eg. companies) that mutually distrust each other:** A cryptographically signed, append-only, replicated log. [Chronicle](#) can do this, and a well-known public deployment of this type of technology is [Certificate Transparency](#). There are probably other options. These are *not* blockchains.
- **If you need to verify that nobody has tampered with physical goods:** This is currently impossible, with or without a blockchain. Nobody has yet figured out a reliable way to feed information about the real-world into a digital system, without allowing the

person entering it (or handling the sensors that do so) to tamper with that data.

Some people may try to sell you one of the above things as a "blockchain". It's not, and they're lying to you. A blockchain is defined by its trustless consensus; all of the above schemes have existed for way longer than blockchains have, and solve much simpler problems. The above systems also don't provide full decentralization - and that is a *feature*, because decentralization is expensive.

If somebody talks to you about a "permissioned blockchain" or a "private blockchain", they are also feeding you bullshit. Those things do not actually exist, and they are just buzzwords to make older concepts sound like a blockchain, when they're really not. It's most likely just a replicated append-only log.

There's quite a few derivatives of blockchains, like "tangles" and whatnot. They are all functionally the same as a blockchain, and they suffer from the same tradeoffs. If you do not need a blockchain, then you *also* do not need any of the blockchain derivatives.

In conclusion: blockchains were an interesting solution to an extremely specific problem, and certainly valuable from a research standpoint. But you probably don't have that extremely specific problem, so you don't need and shouldn't want a blockchain. It'll just cost you crazy amounts of money, and you'll end up with something that either doesn't work, or something that has conceptually existed for 20 years and that you could've just grabbed off GitHub yourself.

Additions

I'm going to add some common claims here over time, and address them.

"But it's useful as a platform to build upon!"

One of the most important properties of a platform is that it must be *cost-efficient*, or at least as cost-efficient as the requirements allow. When you build on an unnecessarily expensive foundation, you can never build anything competitive - whether commercial or otherwise.

Like all decentralized systems, blockchains fail this test for usecases that do not benefit from being decentralized, because decentralized systems are *inherently* more expensive than centralized systems; the lack of a trusted party means that work needs to be duplicated for both availability and verification purposes. It is a flat-out impossibility to do *less* work in an optimal decentralized system than in an equivalent optimal centralized system.

Unlike most decentralized systems, blockchains add an extra cost factor: costly signaling, as described above. For a blockchain to be *resiliently decentralized*, it *must* introduce some sort of significant participation cost. For proof-of-work, that cost is in the energy and hardware required, but any tangible participation cost will work. Forms of proof-of-stake are *not* resiliently decentralized; the cost factor can be bypassed by malicious adversaries in a number of ways,

meaning that PoS-based systems aren't reliably decentralized.

In other words: due to blockchains being inherently expensive to operate, they only make sense as a platform for things *that actually need trustless consensus* - and that list pretty much ends at 'digital currency'. For everything else, it is an unnecessary expense and therefore a poor platform choice.