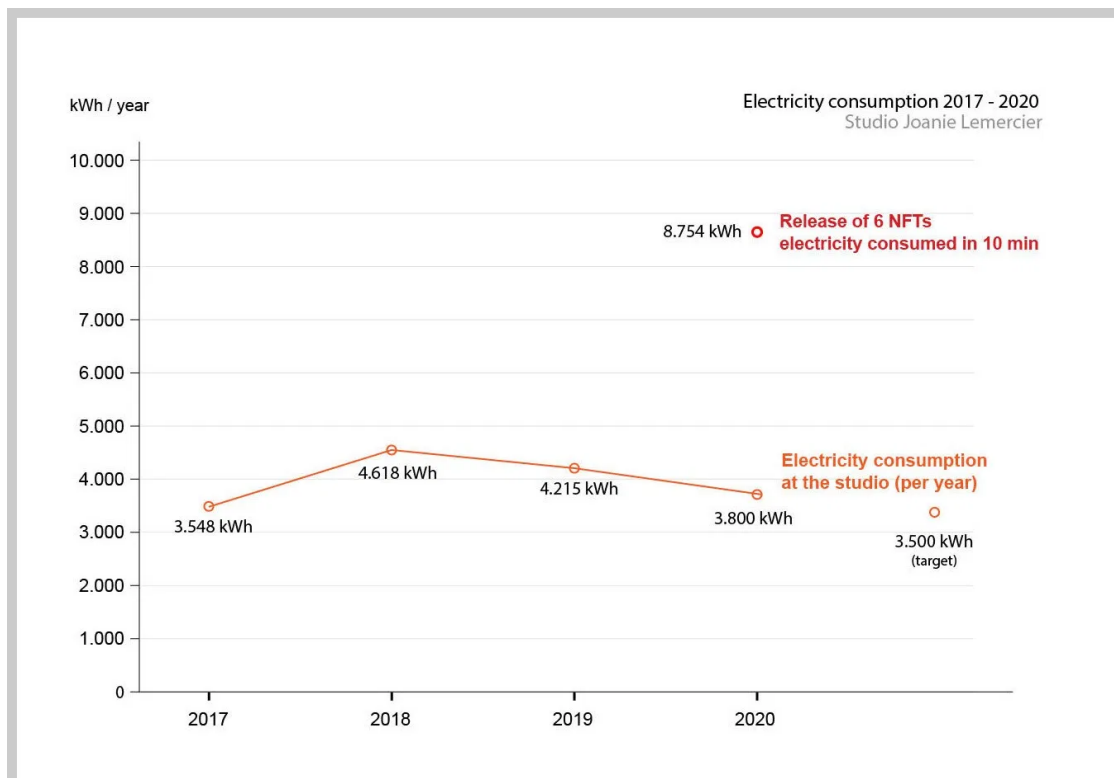


Satoshi Nakamoto and the Fate of our Planet

If you're interested in cryptocurrency, at some point you're going to come across Elon Musk, founder of Tesla and court jester of Twitter. He has strong opinions, he's not afraid to share them, and apparently he's also not afraid to **completely reverse them** due to ecological concerns over blockchain mining.

In the midst of the furor over one man's opinions, I also sense growing **anger** over the energy consumption of **non-fungible tokens (NFTs)**, which are blockchain-based certificates of ownership for digital art. One artist, Joanie LeMercier, calculated that the sale of six of his pieces consumed **more electricity in ten minutes** than his art studio had consumed in the previous two years.



Granted, determining blockchain's real ecological cost is not simple. Some argue that kilowatts per transaction is the [wrong equation](#). Others claim that roughly [three quarters](#) of the electricity used to mine blocks comes from renewable sources (though still others say it's [more like 40%](#), and most of the remaining power comes from **coal and natural gas**). Finally, proponents claim that cryptocurrency [drives adoption of renewables](#) and might be [a lot greener](#) than the global banking system.

But as blockchains become more popular and their tokens increase in value, more miners get in on the game, increasing the total electricity consumption. Even if you use the more favourable figures, with non-renewables accounting for only 25%, **25% of a lot will still be a lot**.

Public blockchains consume so much electricity because they have a lot of entropy to deal with. In thermodynamics, entropy is noise, waste, meaninglessness. The problem blockchain is trying to solve — dishonest agents trying to corrupt the global ledger — certainly fits that description.

Any time you have too much entropy, you're going to need to spend a lot of energy [moving it somewhere else](#). **My hot take: Bitcoin is basically converting dishonesty into CO₂**. It's [simple physics](#).

We get it. Bitcoin is burning the world. Ethereum is burning the world. NFTs are burning the world. There are more planet-friendly consensus designs out there, along with layer 2 protocols to ease the burden, and I appreciate these innovations. If the world is gonna use blockchains, it ought to figure out ways to make them greener.

But I think it ignores two important questions: Regardless of the consensus mechanism used, **is consensus even necessary?** And more importantly, **could we be doing better things with that electricity?**

Consensus: an irrelevant starting point?

Programmers love a 'single source of truth', a canonical representation of [system state](#) that everyone can rely on. That naturally led people to look for a way to get everyone to agree on the contents of one single, shared ledger of events.

This problem — reaching consensus among all honest agents in a low-trust system — is big. And the solutions are brilliant. As an engineer, I love them. But they all feel like answers to the wrong question.

What if we started with different questions?

Moving one step backwards, **do we really need consensus on everything?** The real world seems to do just fine without it, for the most part. And I'd like to move backwards even further and ask, **what are we actually trying to achieve?**

We just want to interact with each other on the internet without having to constantly worry about getting cheated. That's a simpler framing, and it opens the door to novel solutions. Evolution has been working on this problem for a long time. And it's come up with lots of great solutions (you could call them games) that all share three simple meta-rules (you could call this the meta-game of living systems).

1. Everyone knows and agrees to the rules of the specific game they're playing.
2. Each participant takes responsibility for following the rules.
3. If anyone sees anyone else breaking the rules, they take action against them and spread news of what they saw.

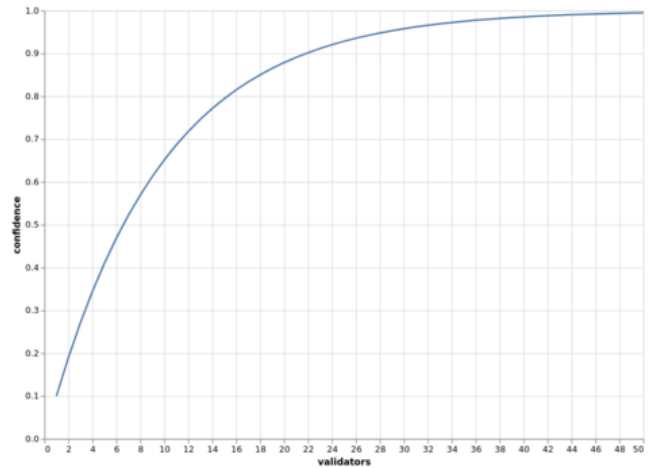
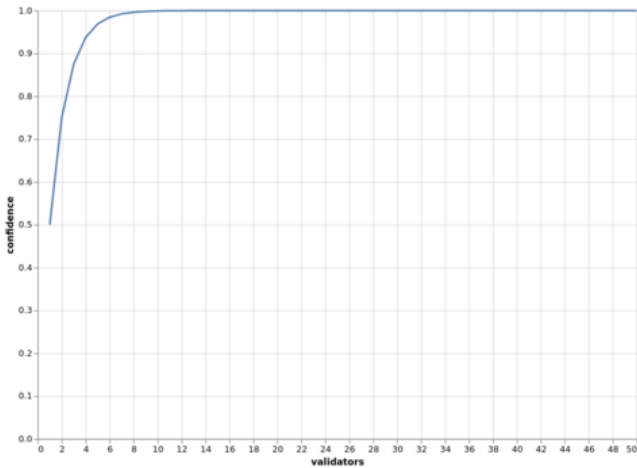
We see this meta-game popping up over and over again — in ecosystems, bee colonies, flocks of birds, and even human social structures (though we seem to pick really terrible games and break the rules a lot). **Considering the small energy input, it's a surprisingly robust defense against threats.**

The human immune system is a great example: the rules of the game are encoded in each cell's DNA, so each cell knows how to play nicely with the other cells. If any cell acts up — maybe it goes cancerous, maybe it's infected with a virus — special immune cells recognise it as a bad actor and trigger an immune response. The body protects itself without spending a lot of energy, simply by launching a small, targeted response against the rule-breaker.

That's how a Holochain application's network works. Each user has their own application cell, with a chunk of code (we even call it a [DNA](#)) that defines the rules of the game. They're responsible for the actions they take, which get written onto their own [personal ledger](#). Each action is witnessed by a small set of randomly chosen peers, who [store its data, check it](#) against their copy of the rules, and broadcast an alert if they see anything wrong.

With this arrangement, you can get 'good enough' security with a fraction of the effort that full consensus would require.

Holochain makes a bold claim: **Consensus is unnecessary for most of the things blockchain is interested in doing.**



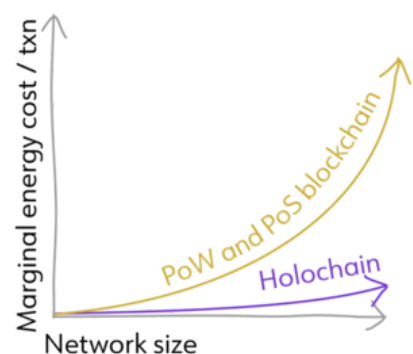
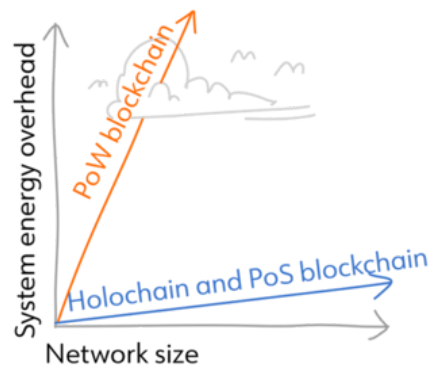
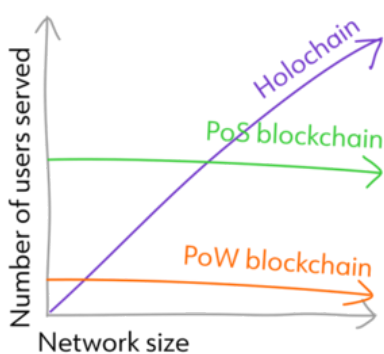
With such a lightweight approach to security, a Holochain network can scale almost infinitely. Even as the number of users go up, each user is still only responsible for witnessing a small portion of their peers' data.

Making sense of the energy costs

So what does this all mean for energy consumption? This is a hard question to answer, because blockchain's consensus and Holochain's peer witnessing are such different approaches. But I'll try my best.

In the graphs below, I attempt to show how three different systems – proof-of-work consensus, proof-of-stake consensus, and Holochain – perform compared to each other. To make things simple, I assume that every single user is perfectly average; they all want to make the same number of transactions per day. Don't think too hard about these graphs, though; they're 'napkin scribbles' that show the *character* of these systems' performance, not actual precise measurements.

Performance versus network size



The first graph shows how many average users each system can comfortably handle. Higher numbers are better. Blockchains don't get any faster as you add more machines; in fact they get slightly slower. The cloud industry would probably describe this as 'anti-scalability'. Holochain, on the other hand, keeps climbing roughly linearly in its ability to serve users, because each user takes care of their own business and helps validate a small portion of everyone else's. As with blockchain, performance drops slightly at larger network sizes, but it's more like 'doesn't climb quite as fast anymore'.

The other graphs show energy consumption, where lower numbers are better. The second shows the total system energy overhead, or 'cost to keep the thing running'. For all three systems, this grows linearly as the network grows. But for PoW blockchains, the mining overhead is massive — regardless of how much useful work is actually getting done.

Lastly, let's look at the marginal energy cost per transaction, or the energy it takes to commit data beyond the system overhead. All three systems get exponentially more expensive as the network grows, because each machine needs to talk to more peers in order to complete a transaction. But in Holochain that number grows much more slowly, because the number of witnesses you need to submit your transaction to is capped at 5, 10, 50, 100, whatever the network requires. (For the comp sci nerds, insertion time complexity for blockchain is $O(n^2)$ while Holochain is $O(n \log(n))$, where n is the number of nodes in the network.)

This means that **Holochain can serve more users with less energy**. Why does it perform so much better? Two really simple reasons (and please forgive me for repeating myself):

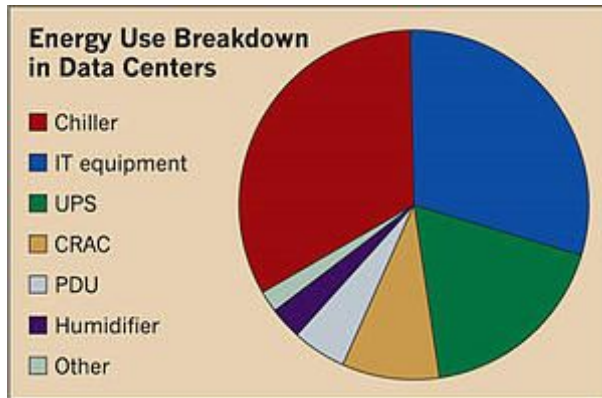
- **Consensus is expensive**, while **peer witnessing is cheap**.
- **Consensus forces everyone to behave like a [single-threaded program](#)**, while **agent-centric peer-to-peer is highly parallel**.

Closing loops and extending lifecycles

So Holochain appears to be faster and less energy-intensive than blockchain. But there are two other ecological advantages that are easy to miss.

Heat: waste or resource?

Blockchain miners and cloud servers usually live in a data centre somewhere. In this building, hundreds or thousands of machines spend all day thinking about math and logic. That generates a lot of heat — so much heat that [up to 50% of the electricity goes to cooling](#).



Permaculture designers say that waste is just a resource in the wrong place. All that heat could be put to good use — say, to heat my home in the winter. But there's no practical way to do that.

Because Holochain apps run on our own devices (or on someone else's device, if we're accessing them via the Holo hosting network), that heat is automatically spread out across the world and captured in our homes and offices. (Fun fact: Holo hosting first caught my attention because I saw the possibility of keeping my greenhouse lemons warm during the cold Canadian winters!)

It's about the hardware too

Every time I use a blockchain or cloud-hosted app, I'm leaning on faraway hardware and thousands of miles of network infrastructure. This seems wasteful when I have a supercomputer in my pocket and all I'm trying to do is talk to my dad on the other side of town. My precious devices take a lot of energy to make, with blood and toxic chemicals spilled along the way. Knowing this, I'd like to use them to their full capacity before I start making demands on other devices.

Once again, Holochain apps run on our own devices. And even with the Holo hosting network, where the apps are hosted elsewhere, the hosting software will eventually be available for desktops and laptops. This means we're getting more use out of the machines that already exist.

That all sounds pretty green to me.

From 'less bad' to 'more good'

It's probably pretty clear that I think Holochain could replace blockchain for a lot of the crypto applications we see today. As we've seen, a well-designed Holochain app can [deliver the same safety guarantees](#) as blockchain, with better performance, at zero cost, for a fraction of the resource consumption.

That excites me. I see a lot of creative things happening in crypto space, and I think Holochain could fill those niches in a way that's gentler on our planet.

And I'm also curious about what's next. As wonderful as these things are, can we do more? Can we go from 'gentler on our planet' to regenerating damaged ecosystems, sharing our common wealth more equitably, and preserving the dignity of our fellow humans? And does Holochain have unique features that can help us get there?

I invite you to explore these possibilities with me in an upcoming blog series about projects that are doing exactly that — starting with [RedGrid](#), who want to [help](#) the world become carbon neutral by 2030.

In the meantime, if you want to start prototyping your dApp on Holochain, head over to the [developer portal](#) and sign up for the upcoming (free) [DevCamp!](#)

(Side note on the cover photo: yes, I know that's probably not the Satoshi who created Bitcoin. But I had to put something there. Poor guy will never get any peace.)

ABOUT HOLO

Holo is a distributed peer-to-peer hosting platform for Holochain apps (hApps); a bridge to the new Internet.

Holo does to web hosting what Airbnb did to hotels—anyone can become a host by turning their computer into a source of revenue, getting paid in HoloFuel for hosting distributed applications. The Holo software runs in the background, allocating spare storage and processing power to serve hApps to the legacy web. Hosts choose what hApps to serve, set their own hosting prices, and manage their own priorities.

Holo