Chapter Four

THERE'S A BLOCKCHAIN FOR THAT

The last few chapters amply demonstrated that fintech is not going to deliver when it comes to solving problems of financial inclusion and economic precarity. But maybe those are just particularly thorny problems, and maybe it's unfair to judge Silicon Valley's efforts against such complex obstacles. If you've gotten this far in the book you know that Silicon Valley is not shy about offering techno-solutions to some of our most wicked problems, but for now let's give Silicon Valley the benefit of the doubt and engage with the tech industry's more "bread and butter" promises to make things more efficient, more competitive, and more secure. To do that, though, we have to figure out what counts as "efficient" and "competitive" and "secure."

Just like beauty, efficiency, competition, and security are all in the eye of the beholder. For example, one person's "efficiency" may be another person's "dismantling critical government infrastructure." And yet technological solutions designed to make things more efficient, more competitive, or more secure are often presented by Silicon Valley as neutral and universally desirable. That veneer of neutrality and universality

can be dangerous if it disguises the fact that Silicon Valley is solving (or creating and then solving) problems in ways that are antithetical to our values. To illustrate those dangers, we'll use a particular technological solution: the blockchain. A blockchain is a clunky type of database, and it really is the perfect example to demonstrate the hollowness of techno-solutionism: it promises to do everything but really isn't very good at doing much of anything (anything other than helping some unscrupulous folks make money, that is).

Once upon a time

In that sense, blockchain is an Emperor's New Clothes technology. Everyone sort of knows the story of the Emperor's New Clothes, but many modern versions of the tale end with a small child saying "the emperor has no clothes" and then everyone concedes right away that the child is right. It's reassuring to think that we're all capable of such quick introspection and redemption, that we'll all quickly grasp when we've been duped by swindlers claiming that only stupid and unworthy folks can't see the clothes. In the original Hans Christian Andersen version, though, the Emperor and his courtiers never admit he's naked – they're in too deep. So he walks more proudly than ever in his undressed state, as those who swindled him ride off into the sunset.

The fact that blockchain is still sometimes described as a paradigm shifting innovation – more than fifteen years after its launch with so little to show for itself – suggests that people are either still too afraid of looking like they don't understand, still too deferential to Silicon Valley's supposed technological expertise, or still too busy doing other things, to voice any

skepticism about blockchain-based solutions. For most people, I suspect the latter is the case. Because blockchain isn't very useful, most people haven't interacted with this supposedly revolutionary technology in their everyday lives. As a result, they haven't even had a chance to see its limitations in the wild, and all they have to go by is the hype.

At Hogwarts School of Witchcraft and Wizardry, there is a room known as "The Room of Requirement." It appears, magically equipped with whatever is needed, to those who thrice walk past its hidden entrance while concentrating on whatever it is they require. Blockchain technology is often marketed as a Room of Requirement, as the killer app for whatever ails you – but an inconvenience lies in the fact that (unlike Harry Potter) blockchains are not actually magic. Blockchain applications are extremely constrained by the technology's real-world limitations, according to more than 1500 independent computer scientists, software engineers, and other technologists who signed on to a letter to US Congressional leaders in 2022. Here's the money quote:

> *By its very design, blockchain technology is poorly suited for just about every purpose currently touted as a present or potential source of public benefit.*

And yet, because of the hype surrounding the technology, there has been so much blockchain experimentation starting with the premise of "where can I stick my blockchain?," instead of starting with a problem and then finding the best solution to it. Trying to jam blockchain's square peg into a round hole has often proved costly, though (and that comparison is probably unfair to square pegs everywhere, which do have uses outside of round holes).

In 2016, for example, the Australian Stock Exchange announced with great fanfare that it was partnering with the firm Digital Asset Holdings to replace its existing clearing and settlement system with blockchain technology. The ASX ultimately ended up with egg on its face, though, abandoning the project in 2022 after spending years and the equivalent of about USD$164 million on it. Why wasn't it a good solution for the ASX? Well, the scaling and complexity challenges associated with blockchain technology were reportedly a big part of it.

> Fun fact: the CEO of Digital Asset Holdings at the time the ASX signed up was none other than Blythe Masters, the woman credited with inventing the credit default swap, a.k.a. the derivative contract that was at the epicenter of the 2008 financial crisis.

Also in 2022, IBM and the shipping giant Maersk abandoned their collaboration on a blockchain-enabled global supply chain platform known as TradeLens because of insufficient industry buy-in. Reporting suggests that some of the greatest obstacles to adoption were the costs associated with the blockchain-based platform, and concerns from competitors that Maersk would be able to control and exploit the platform.

Sadly, though, a technology won't always fall out of favor just because we have ample evidence of how much it sucks. Like the Emperor and his courtiers, Silicon Valley hype men may simply double down on trying to sell people on it. I vividly remember talking to a Bloomberg journalist a few years back about the overwhelming limitations of blockchain technology, implying that it was probably doomed as a result. Their succinct

and cutting reply? "But a technology doesn't have to be good to succeed, does it?" Blockchain has benefitted from one hell of a VC-funded public relations and lobbying campaign to make it look useful and justify favorable legislative reform – and the beauty of a technology that doesn't do much of anything is that it's very easy to project one's wildest dreams upon it.

Take the book *Read Write Own*, written by Andreessen Horowitz partner Chris Dixon. This paean to blockchain technology argues that it is the key to dislodging big tech companies like Meta from their monopoly positions (excuse me if I'm a little suspicious of whether Andreessen Horowitz *really* wants to help dislodge Meta, given that founding partner Marc Andreessen remains a member of Meta's board of directors, but I digress…). Dixon is quick to dismiss any legal or regulatory measures for restraining the market power of the tech giants, and instead leans into the power of "a new software movement…that can reimagine the internet."

His book is long on dreams for a blockchain-based internet referred to as "Web3," but it is short on concrete details on how to achieve those dreams. The very brief Part Four, which is titled "The Here and Now," has little to say about actual successful blockchain applications (notwithstanding that there had already been about fifteen years of blockchain experimentation by the time *Read Write Own* was published). Having dispensed quickly with prosaic reality, Dixon moves on to discussing "What's Next," where he dreams about how blockchain technology could be used to remake markets for art, for financial services, for social media – and as the necessary foundation for our old friend the Metaverse (but wait – I thought

the whole point of blockchain was to displace Big Tech like Meta. Silly me, I must have misunderstood…).

Blockchainsploitation

Dixon's tome of blockchain evangelism became a New York Times bestseller, although the New York Times helpfully added a "dagger symbol" to *Read Write Own*'s ranking to show it was supported by bulk orders (subsequent reporting found that many bulk orders were placed by Andreessen Horowitz and several companies that it funded). Money can buy bad technology a *lot* of marketing hype. But while it's kind of fun to skewer *Read Write Own* – crypto critic Molly White wrote a takedown of Dixon's book with such relish that her review has been likened to a New York Times food critic reviewing Guy Fieri's Flavortown restaurant – a lot of real blockchain experimentation has happened out of the public eye, on marginalized communities, with devastating results for those communities and little else to show for itself.

It's no laughing matter, for example, that a corporation backed by venture capitalists including Peter Thiel and Marc Andreessen bought up land in Honduras following a military coup to establish a libertarian start-up city called Prospera where blockchain technology would undergird everything from land registries to recruiting people for unregulated gene therapy trials. Simple databases would have done at least as good a job at maintaining these records, but they wouldn't further the founders' ideological desire to "exit legacy systems" (in Chapter 7, we'll dig deeper into this disturbing blockchain-based "Network State" movement). In 2021, Honduras' newly elected President Xiomara Castro worked with the legislature to repeal the laws that

allowed Prospera to operate outside the realm of Honduran sovereignty and the Honduran Supreme Court ultimately declared such zones illegal, but the Prospera Corporation and its billionaire founders responded by suing Honduras for almost USD$11 billion. The entire country's GDP was only USD$31.43 billion that year, and so the suit (as yet unresolved) could prove ruinous for an already struggling nation.

It's also no laughing matter that the Andreessen Horowitz-backed "play to earn" game Axie Infinity was pitched as a way of empowering people by introducing them to a blockchain-powered Web3/Metaverse that would, as Zeke Faux quotes Axie's founder, let "people interact with the global economy, actually exiting their prisons, where they are born." In the game, players would battle their Axies (cartoon blobs that have been described as Pokemon knockoffs) and the winner would receive crypto assets known as "smooth love potion" that could be used to breed new Axies, or be cashed out. However, instead of financially empowering the many Filipinos and other residents of the Global South who flocked to the game, Axie Infinity turned out to be very sweatshop-like and Ponzi-ish. As it became harder to attract new users, the value of Smooth Love Potion fell from a high of 44 cents in the summer of 2021 to less than one cent in 2022, devastating those who had quit their jobs to play Axie full-time, or who had incurred debts denominated in real money to buy Smooth Love Potion.

A little closer to home, it's no laughing matter that bitcoin ATMs have sprung up alongside payday lending and check cashing operations in lower-income US neighborhoods. Although they're often marketed with the typical "democratizing finance" BS, these ATMs accept cash and turn it into crypto but

rarely work the other way. Not only do users face challenges cashing out any crypto gains, the machines also charge exorbitant fees (often hidden in the USD-bitcoin exchange rate). Scammers have also been capitalizing on these bitcoin ATMs as a way to separate marks from their cash.

Perhaps the most egregious blockchain-based project I've heard of, though, is WorldCoin. Founded by a trio that includes Sam Altman (yes, that Sam Altman, the CEO of ChatGPT developer OpenAI) and backed by Andreessen Horowitz (yes, I know I'm starting to sound like a broken record but it's not my fault that Andreessen Horowitz funds all this stuff), WorldCoin's website at one point described itself as:

> *designed to become the world's largest privacy-preserving human identity and financial network, giving ownership to everyone. Worldcoin aims to provide universal access to the global economy no matter your country or background, establishing a place for all of us to benefit in the age of AI.*

That's a pretty standard serving of technobabble world salad with a side order of "making the world a better place." What the project *actually* entails is using a dystopian-sounding device known as "The Orb" (one report described The Orb as resembling a "decapitated robot head") to collect biometric data by scanning retinas. In exchange for their biometric data, people receive the crypto asset WorldCoin. WorldCoin can't be used for much of anything right now, but the vision is that ownership of WorldCoin will one day onboard holders into the new, blockchain-based version of the internet that will be known as Web3. If you're asking why WorldCoin thinks retinal scans will be important for

developing Web3, well, Sam Altman has a pretty dystopian vision for you.

Remember that WorldCoin is a side hustle for Sam Altman – his day job is CEO of OpenAI, and so he is highly invested in selling the vision that AI will render many jobs obsolete through efficiency gains. Without jobs, people will need other ways of obtaining money, and Altman envisages a world where people can monetize the attention they devote to online content. If you've ever seen the Pixar movie Wall-E, that seems to be the world that Altman is going for. People rendered mentally and physically flabby by lack of activity float around with screens permanently glued to their faces, intermediating every single conversation. Every activity (from golf to learning the alphabet) is conducted virtually, as humanity slowly wastes away in space without any dignity or purpose – until Wall-E inspires a turn of events that kickstarts humans into coming back to earth to clean things up.

Wall-E was intended as a cautionary tale, but it sometimes seems like our overly optimistic friends in Silicon Valley miss the subtext and react to dystopian fictions with the response "cooooooool - what if we actually did that?!" If the truly depressing attention-based economy that Altman envisions were to come to fruition, then there would need to be some way of ensuring that people aren't double-dipping by creating multiple accounts to watch multiple types of content at the same time. But because of the pseudonymity associated with the blockchain, figuring out who a person is in a blockchain-based Web3 would be challenging. Enter WorldCoin's proposed "proof of personhood," trained on real humans' biometric data, which they consider a necessary authentication method for Web3. And

something that necessary would certainly become valuable, wouldn't it, especially if it was the only (centralized, some might say) accepted identity authentication mechanism? Worldcoin's venture capital investors (including crypto exchange Coinbase's venture arm as well as Andreessen Horowitz) certainly seem to think so.

WorldCoin is kind of Metaverse-ish, in the sense that its founders are trying to will the problem of AI-forced worker obsolescence into existence so that this blockchain-based project can solve it. And yet, in the name of solving a problem that Silicon Valley intends to cause but probably won't succeed in causing, Worldcoin is inflicting very real present harms through its experiments with a solution that is too superficial to address the dislocations that a massive reduction in employment opportunities would entail. Even if the AI criti-hype came true and the robots actually did take all our jobs, we would deserve better than Wall-E-world.

We don't always have the best vocabulary for articulating the harms we humans suffer from being reduced to a pile of data and then having that data used against us, but it seems pretty obvious that WorldCoin raises some privacy concerns. WorldCoin says it's going to use the biometric scans it collects as training data for an AI tool that will recognize irises, but there is nothing to prevent WorldCoin from selling those scans or using them for other purposes. Although WorldCoin promises it won't sell, those promises don't seem all that reassuring, given that the business has not been entirely forthcoming about how it uses, stores, and disposes of the data it collects (and there have been reports it has collected many more types of data than iris scans). Even without all the specifics, it is relatively easy to grasp that

it's probably a bad idea for people to give up their unique biometric data for a pile of magic beans (like most crypto, the price of these WorldCoin magic beans is highly volatile: priced at over $11 in March 2024, one WorldCoin was worth less than $1 a year later. Also like most crypto, there are reports of users permanently losing their WorldCoin through hacks and other technological snafus).

Unfortunately, millions of people have already been scanned – often poor individuals living in the Global South (and they are also typically scanned *by* poor individuals living in the Global South, who have been recruited as orb operators in a process that looks a lot like a multilevel marketing scheme). As reporters Elaine Guo and Adi Renaldi put it, "it's just cheaper and easier to run this kind of data collection operation in places where people have little money and few legal protections" – just as it's easier and cheaper to run off-label medical testing in Honduras. While some countries are already concerned enough about potential privacy violations that they've either curtailed or investigated WorldCoin's business (operations have been investigated or shut down in more than ten countries), operations keep popping up in new countries as local authorities are sold on WorldCoin's vision. And at the end of April 2025, the United States earned the dubious distinction of joining "those places where people have few legal protections:" WorldCoin (now rebranded "World" because, sure, whatever) rolled out in San Francisco.

Decentralization theater

Even after reading all of those purported blockchain use cases, you're probably still struggling to figure out how this

clunky database actually works, so let me explain. A word of warning before we start, though: I'll occasionally need to get a little bit in the weeds. This is not always the best strategy for expressing skepticism. Engaging with technological technicalities is often counterproductive, because if you're worried about the impact of a particular technology, talking about how the technology *works* is typically less important than, and can distract from, talking about how the technology is *used*.

It's also true that technologists often disagree among themselves on these technological technicalities, and so there may not even be an expert consensus about how a particular technology works. And yet industry folks will sometimes seize on the small errors they perceive in your description of a technology to discredit your bigger picture concerns entirely, missing the forest for what they consider to be a slightly misidentified tree. Sometimes it's just better to stay above the fray and not wade into the technological technicalities. But if you're trying to thoroughly debunk the utility of a particular technology, like I am here, you have to engage with those technicalities to some extent. So here goes.

Blockchain technology is often described in highly complex terms that lend it mystique, but we will call the blockchain what it really is: a spreadsheet or database which you can add information to, but not delete information from. We've had databases for quite some time, and lots of them are hosted by multiple computers in multiple locations in the same way that blockchains are. Certain functions on blockchains can be automated using computer programs known as "smart contracts," but functions on other databases can also be automated.

The main thing that sets blockchains apart from other databases is that instead of having trusted authorities who are charged with adding and removing entries, a blockchain theoretically allows any computer or "node" hosting a copy of the database to add entries to that database so long as some kind of validation mechanism is satisfied that those new entries should be added (entries can't be removed without taking drastic steps to remake the database in a process known as "forking," which is not great if you need to undo a mistaken or fraudulent transaction). The purported absence of any trusted authority charged with updating the database is often referred to as "decentralization," and decentralization is blockchain's main claim to fame.

Promises that blockchains will make things more efficient, more competitive, and more secure all flow from the assumption that by allowing for decentralization, the technology eliminates the need for intermediaries. If there were truly no intermediaries, then there would be no middlemen to slow down transaction processing or collect fees along the way – that should be more efficient. And if transactions were truly performed peer-to-peer, then we could avoid reliance on intermediaries like big tech platforms or financial institutions – that should whittle down their market power, making markets more competitive. And dispensing with intermediaries should presumably eliminate the security risks that can arise from relying on ill-intentioned intermediaries who might censor our activity or steal our money, or serve as a single point of failure.

But all of these aspirations are based on fundamental confusion regarding the "decentralization" that blockchains offer. A system needs to offer more than just the *opportunity* for

decentralized control to actually *be* decentralized. Blockchains, and many of the things built on them, are technologically decentralized systems in the sense that there are lots of nodes involved, but if one person can control lots of those nodes, or some nodes are more important than others practically speaking, then control of the system will become centralized and all that effort that went into technological decentralization will be for naught.

You might have thought this would be obvious. For centuries, we've had the "technology" for decentralized organizations in the form of corporations that issue lots of shares, but the fact that I can buy a single share in a corporation doesn't give me the right to have any meaningful say in how that corporation runs its business. My voice will be drowned out by the controlling shareholders (and my impotence is becoming even more assured as tech companies lead the way in embracing dual-class share structures that allow their founders to exert outsize control even after they've sold off lots of their shares). And yet we're supposed to believe that a blockchain-based system will allow users, simply by operating a single node in that system, to wrest control away from those who have invested more time and money in it? This is magical thinking, and blockchains aren't magic. As technology publishing guru Tim O'Reilly observed, "history teaches us that there will always be new avenues for power to become centralized." He then noted that "blockchain turned out to be the most rapid recentralization of a decentralized technology that I've seen in my lifetime."

In Chapter 2, we met some of the individuals and companies that users of the purportedly-decentralized bitcoin blockchain have to trust, like the handful of core software

programmers who maintain that blockchain, and publicly-traded bitcoin mining companies. We also met some intermediaries that most bitcoin users choose to trust, like exchanges for converting their bitcoins into dollars or other crypto assets. We also talked about how most bitcoin users are at the mercy of the large whales (i.e. people holding more than 1,000 bitcoins) who are in a position to manipulate the price of bitcoin by trading back and forth with themselves or one another (at the peak of the market in 2021, bitcoin whales were reported to own about 53% of all bitcoins).

These kinds of centralized power aren't unique to bitcoin; they're common throughout the crypto markets. Another popular blockchain is the Ethereum blockchain, where transaction validators "stake" their ETH coins in order to be able to add transactions to the blockchain and get paid for their trouble. If you want to be a validator, you need to own at least 32 ETH coins – as of February 2024 (when 32 ETH coins would have been worth about $108,000) the crypto exchange Coinbase reportedly controlled 15% of all Ethereum validators. So, not really the democratized peer-to-peer system we were promised.

Ethereum users also depend on the Ethereum Foundation to maintain the blockchain's code. The Foundation's website (which, by the way, is resplendent with extremely trippy pastel illustrations), has a photo and contact details for Vitalik Buterin, the co-founder and most well-known face of Ethereum, but the website is at pains to assure readers that neither Buterin nor the Foundation is actually in charge, saying things like:

> *the EF is hard to categorize. We are not a tech company, or a "normal" non-profit. Just as Ethereum requires new*

> *concepts and technologies, it has spawned new kinds of organizations. We are at the frontier of a new kind of organization: one that supports a blockchain and its ecosystem without controlling it.*
>
> And:
>
> *Through grants, research, and other initiatives, the Ethereum Foundation nurtures the vitality of the ecosystem and supports benevolent actors, working so that Ethereum remains a true public good: Directed by none, useful for all.*
>
> And:
>
> *Were the Foundation to claim a central role in the Ethereum ecosystem, it would be at odds with the core values enshrined in the protocol code – at odds with the vision of Ethereum's future called serenity.*

Methinks the Foundation doth protest too much, especially because when the chips were down in 2016 and the very first blockchain-based organization built on the Ethereum blockchain was hacked, Vitalik Buterin was a driving force behind the fork in the blockchain's code that effectively allowed the hack to be undone and kept undone. Seems like a pretty "central" and "directed" move to me – and these kind of moves will inevitably be needed when the future turns out to be less than serene.

As with bitcoin, most users rely on exchanges to buy ETH, and some of these exchanges (like Coinbase) are very open about being centralized intermediaries. Other exchanges, like

Uniswap, claim to be decentralized, controlled by the holders of "distributed governance tokens." But researchers have found that as of 2022, less than 10% of Uniswap token holders bothered voting (whereas the shareholder participation rate in US public companies is more like 70%). And even if all of those token holders did vote (voting is done by delegating tokens to a delegate), ownership of Uniswap tokens is so concentrated that the same researchers found that only 11 delegates need to agree on any change for it to go through. Also, Uniswap backs a lobbying arm, in the form of the DeFi Education Fund. Nothing screams decentralization like a Washington DC lobbying shop…

Part of the explanation for why control tends to become centralized is that full participation in a decentralized system requires a user to do a lot of upfront work to figure out exactly how the system functions, and then to keep engaging after they've figured it out. Most people are too busy or lazy for that. Part of it is that it's very unwieldy for lots of people to have an equal say in how the system should run – as they say, a camel is a horse designed by a committee. And even if everyone involved can agree at the beginning, things will inevitably happen that require changes to how the system operates – and it's likely to be impractical to involve everyone in developing and signing off on those changes, especially if it's an emergency and quick action is required (like when your first blockchain-based organization gets hacked, ahem, Vitalik Buterin).

Having a hierarchy of control streamlines things in the face of uncertainty, and makes life easier for people who don't want to invest heavily in learning the intricate workings of something. And when there are opportunities to make money from hierarchy and streamlining, the evolution of centralized

intermediaries seems inevitable – someone will always rush to fill a profitable power vacuum. This is, of course, how our current internet became intermediated by Big Tech platforms like Google (now Alphabet) and Facebook (now Meta): they made the internet easy to use for those who didn't understand how internet protocols actually worked, and became some of the largest companies in the world as a result. These tendencies towards centralization of profit and power have implications for the (in)ability of the blockchain, and the things built upon it, to make things more efficient, more competitive, and more secure.

Efficiency

A techno-solutionist mindset encourages us to look at problems and view them as things that are easily solvable with technologies. We tend to think of technology as being particularly good at making things more efficient, and so it's not surprising that Silicon Valley encourages us to frame so many complex problems as simple inefficiencies that technology can streamline (for example, as we saw last chapter, financial inclusion problems are often over-simplistically attributed to banks' clunky user interfaces and to the cost of back-office processing by slow and squishy human beings). But techno-solutionism isn't the only thing encouraging us to view efficiency as the be all and end all. As sociologist Elizabeth Popp Berman has chronicled in her book *Thinking Like an Economist*, the rise of "efficiency" as a policy goal – which dethroned previous generations of policy goals framed around things like rights and equality – has also been driven by the prominence of economists and economic thinking among the policymakers charged with fixing our most stubborn social problems.

Popp Berman notes that while it wasn't always this way, we've by now been conditioned to think that "more efficient" is always an improvement without thinking too hard about what "efficiency" actually means. That word, however, means different things to, and even among, economists, technologists, and other kinds of experts. Different people will also view the tradeoffs involved in generating different kinds of efficiencies differently depending on their individual position and values. As soon as we start going down the rabbit hole of trying to define "efficiency," the notion that it is a single coherent concept, or in any way a neutral concept, falls apart pretty quickly.

Does efficiency just mean "eliminating wastefulness" in the colloquial sense? If so, wastefulness from whose perspective? If we're talking purely about technology, are we speaking specifically about eliminating frictions so that we can more efficiently use computing power or data? But might eliminating frictions sometimes limit our ability to interject human values into how technological solutions work? Some economic measures of efficiency are focused on promoting utilitarian increases in overall welfare, where making some people worse off is fine so long as that is offset by others reaping big benefits. But will we be ok with this kind of distributional inequality in every situation? Complexity scientists tend to think of efficiency as one of several attributes of a complex system – an attribute that can make that system more fragile overall. Which begs questions about which kinds of tradeoffs are appropriate between efficiency and redundancy to keep the systems we need going, and who benefits from particular choices about those tradeoffs.

I could go on, but what I want to establish here is that what is considered efficient in a particular context will always depend

on that context and need to be measured against other goals. Solving for "efficiency" as a universally shared value – as so many techno-solutions purport to do – can therefore hide a multitude of sins. Let's return to the blockchain to illustrate this. Blockchains are supposed to be efficient in the colloquial "eliminating wastefulness" sense, because they purportedly eliminate the need for intermediaries, including the need for those intermediaries to spend time reconciling different sets of books and records. But, in their quest to eliminate intermediaries, blockchains are intentionally *in*efficient in the computational sense: all of the validation mechanisms that blockchains use are designed to consume more computing power than would be needed by a system presided over by a centralized authority.

> For those who really want to get into the technical weeds, I'm talking here about a type of blockchain that is referred to as "permissionless." The bitcoin and Ethereum blockchains are both examples of permissionless blockchains. There are, however, other types of blockchains that don't have these kinds of problems because they rely on trusted nodes to validate transactions.

Because any participant in this kind of blockchain-based system could be a bad actor, wasteful validation mechanisms are unavoidable. Without artificially injecting inefficiency and expense into transaction processing, it would be far too easy for a bad actor to add problematic transactions to the database. But this in-built inefficiency makes it challenging for blockchains to scale up and process lots of transactions in an expedient manner (remember that the bitcoin blockchain can only process an

average of seven transactions per second whereas Visa can process about 24,000).

Still, for those using blockchain-based technologies, these kinds of inefficiencies may be worth it (or at least worth working around) if other kinds of efficiencies (perhaps law-avoiding efficiencies?) can be wrung from the technology. This is especially likely if some of the costs can be pushed off onto others. The environmental costs of bitcoin mining, for example, are borne by all of us. Global efforts to combat climate change are being undercut by bitcoin mining businesses devoting a small nation's worth of energy to the intentionally inefficient activity of guessing a random number. But those impacts are not distributed evenly: the profits for mining companies outweigh their interest in our environment and so mining is worth it for them; many of us who will eventually be impacted by climate change don't even realize that bitcoin mining imposes such steep environmental costs. Today, mining costs are felt most keenly by the communities located near the mining companies' warehouses, who often see their power bills skyrocket and are tormented by noise that has been compared to having a jet engine in your backyard that never leaves.

The vast majority of bitcoin mining was done in China, until the Chinese government kicked the mining companies out in 2021. Bitcoin mining business then took root in the United States in what the New York Times has described as "a boon for the fossil fuel industry." Riot Platforms, the largest bitcoin mining company in the United States, did not take kindly to the New York Times' reporting on this issue, issuing a fiery rejoinder that included the following appeal to decentralization:

> *The NYT appears to have singled out this industry because the NYT has tied itself to political interests opposed to decentralization of authority. Choosing who can and cannot use energy based on political considerations is a dangerous path inconsistent with the values of a free society.*

And yet in that same statement, Riot Platforms acknowledges that it is a for-profit company whose stock trades on the NASDAQ and whose "vision is to be the world's leading Bitcoin-driven infrastructure platform." So very, very decentralized...

We've seen that the Ethereum blockchain relies on a different kind of validation mechanism known as "proof-of-stake." It's much better for the environment than bitcoin-style proof-of-work mining, but still inefficient in its own way. Even Ethereum's co-founder Vitalik Buterin has acknowledged that there's a "blockchain trilemma" where attempts at technological decentralization entail trade-offs for scalability and security. And yet, because of a dearth of skepticism, blockchains continue to be touted as efficient solutions – even to the point of being touted as solutions to technological sticking points that don't exist.

I once spoke on a panel with an economist who was extremely excited about blockchain's capabilities for settling transactions instantaneously. I pointed out that settling transactions in that way eliminates the possibility of netting those transactions (this is kind of wonky but basically, instead of settling up each transaction one-by-one, netting involves batching a whole bunch of transactions and essentially offsetting or cancelling them out to reduce the total number of payments and transfers needed to settle up). Once I stepped off the stage, a man

I'd never met before made a beeline for me. It turned out he was a senior executive at a derivatives exchange. He said something along the lines of "I can't believe someone finally said it! We've had the technology for that kind of instantaneous settlement for years" (and he wasn't talking about a blockchain). "We just don't use it because no one wants to get rid of the efficiencies of netting!"

Some big financial players are on board, though. In 2024, the asset management giant BlackRock decided to host its investment fund Buidl on the Ethereum blockchain (and I regret to inform you that Buidl is not a typo. The fund is pronounced "Build," but the spelling is a shout out to "hodl" which originally *was* a typo for "hold" but now is used intentionally as crypto slang. We really do live in the stupidest timeline). Anyway, a BlackRock representative reportedly told a conference that BlackRock had decided to use the Ethereum blockchain because other financial institutions were "coalescing" around Ethereum "so as not to fragment liquidity."

With most kinds of market infrastructure, that kind of statement would make sense. There is an economic concept known as "network externalities" that essentially means that some things become more valuable the more people use them. Take a social media platform, for example. If no one else is posting on the platform, then you wouldn't want to use it. Conversely, the more users it attracts, the more will come. But blockchains are not most kinds of market infrastructure – their scaling problems mean that the more people use them, the slower and more expensive they get. So how does BlackRock plan to get around the Ethereum blockchain's limitations, and more importantly, what's the point of using it in the first place?

Well, for BlackRock and other institutional firms like the crypto exchange Coinbase who are building on the Ethereum blockchain, it seems like the plan is to bypass Ethereum's clunky transaction processing by using their own private databases to record and settle (and yes, net out) their customers' transactions, and only use the blockchain to settle up among themselves. Coinbase already informed the Securities and Exchange Commission that it makes debits and credits to its customers' accounts ""off-chain," meaning the transaction is recorded on Coinbase's internal ledgers, not on any blockchain."

If this approach takes root, these centralized intermediaries will simply be recreating the traditional financial system except that the underlying layer for settling transactions between financial institutions will be the Ethereum blockchain instead of the balance sheets of central banks like the Federal Reserve. But ask yourself, if you were starting from scratch to create a new financial system, why on earth would you choose a concededly inefficient blockchain to replace the existening settlement infrastructure? If a crypto exchange like Coinbase doesn't think that the blockchain works for its own internal record-keeping purposes, then that seems like a pretty strong indictment of the technology to me. I told you in Chapter 2 that I'm not a fan of gambling, but if I had to wager, I would say that the reason the parties involved want to use the blockchain as the settlement layer is that they spy some efficiencies that can be wrung from carrying on business away from the watchful eye of financial authorities.

Despite its shortcomings, the complexity of blockchain technology does help justify what I consider to be its main use

case: avoiding laws that apply to everyone else. After all, using an inefficient technology that doesn't scale very well might still seem very efficient to you if it allows you to justify things that would otherwise be illegal. Blockchain-based industries have complained about laws ranging from economic sanctions, to tax laws, to consumer and investor protection regulations, to requirements to report suspicious transactions that might be part of a money laundering scheme. The industry as good as says "those laws can't apply to us because those laws were designed to target intermediaries, and the blockchain eliminates intermediaries!" Of course, if you scratch even a little beneath the surface you can find people in charge of operating blockchains and the things built on them. But unfortunately, claiming "decentralization" as a get out of jail free card has been quite effective with some audiences.

Competition

Call me old fashioned, but I don't think we should be cheering for businesses to profit by avoiding laws that were designed to protect the rest of us. I also don't think it's desirable for those law-dodging efficiencies to provide the basis of a business' competitive edge. We saw in Chapters 2 and 3 that many fintech business models – including the blockchain-based crypto industry – trade on their ability to skirt rules that incumbent financial institutions have to play by. While we tend to assume that Silicon Valley startups disrupt existing businesses with their technological superiority, if their edge lies instead in exploiting legal loopholes to get a leg up over less sexy incumbents, then the disruptor is not really making the market more competitive.

At least, that's the way I see it. But not everyone will see it the same way. Like "efficiency," the term "competition" can serve as a kind of Rorschach test for our values, and a Rorschach test with a fascinating history at that. If we go back about a century, competition policy in the United States had multiple goals ranging from improving equity to limiting concentrations of corporate power in order to prevent the subversion of our democracy. But an intellectual takeover of the antitrust field in the 1960s and 70s by those who viewed our friend "efficiency" as the only appropriate goal of antitrust policy ensured that bigger concerns about concentrated market power fell by the wayside. "Efficiency" in this context was translated into a narrow "consumer welfare standard" that led to mergers and other business activities being judged (in the Supreme Court, the Department of Justice, and the Federal Trade Commission) only by their impact on the prices that consumers pay for goods and services.

The most notable figure in this intellectual takeover was Robert Bork, who served at various times as a law professor, U.S. Solicitor General, and a Court of Appeals judge. In 1973, Bork infamously followed President Nixon's order to fire Watergate Special Prosecutor Archibald Cox after Nixon's Attorney General and Deputy Attorney General refused to do so (a turn of events known as the Saturday Night Massacre, which led to President Nixon's impeachment – it was a simpler time). In 1987, Bork was nominated by President Ronald Reagan to be a Supreme Court Justice, but he was blocked by Senators who were concerned about views Bork had expressed opposing civil rights legislation and Supreme Court decisions on gender equality. Before all that, though, Bork was best known for arguing that concentrated market power wasn't a problem if it created

"efficient" economies of scale that reduced the prices consumers paid.

The result of this Borkian intellectual takeover was that competition law in the United States lay pretty inert for decades, even as tech platforms like Google and Amazon built up extraordinary market power (measured not just in terms of the money they make and their ability to snuff out fledgling competitors but also in terms of the data they collect about us and their ability to dictate the information we receive). Then, in 2021, President Biden appointed Lina Khan as Chair of the Federal Trade Commission, Tim Wu as special assistant to the President for competition and technology policy, and Jonathan Kanter as Assistant Attorney General for the Department of Justice's Antitrust Division. They advocated for a much more muscular use of antitrust laws, viewing those laws as a tool for curbing concentrated market power that impacted information flows, slowed economic growth, and contributed to growing economic inequality. It seems safe to say that their efforts during the Biden Administration royally pissed off many in Silicon Valley, with key figures like venture capitalists Marc Andreessen and Ben Horowitz switching their allegiances to the Republican party in the 2024 election cycle.

And you can see why Silicon Valley was so mad, even as (or rather, especially because) many of us stood to benefit from Khan's, Wu's, and Kanter's efforts. If "competition" is interpreted in a way that embraces concerns about different kinds of market power and different ways of abusing that market power, legal authorities can intervene even if prices are low (or non-existent, as they are with many tech services where you're not paying so you are the product). For example, a Federal Trade

Commission report published during Khan's tenure focused on whether tech platforms' aggressive collection and exploitation of user data undermine competition. These kinds of interpretive shifts were a kind of return to the more robust views of "competition" that prevailed before the intellectual sea change of the 1960s and 70s.

Khan's, Wu's, and Kanter's approaches to addressing market power are precisely what Andreessen Horowitz partner Chris Dixon is rejecting in his book *Read Write Own*. Dixon at least pays lip service to the idea that the domination of the internet by a few giant tech platforms is a problem, but he doesn't want any political or legal solutions to that problem. No sirree, he wants a techno-solution in the form of a blockchain-based Web3. But let's be real: if the goal of blockchain-based experimentation were true decentralization, then no intermediary would profit – and without the possibility of a return, no venture capital firm would be willing to fund Web3 ventures. We've already discussed how the blockchain ecosystem is rife with intermediaries, but if you need further proof of how hollow decentralization rhetoric is, Andreessen Horowitz has ploughed more than $7 billion into Web3 ventures. It's safe to assume that it's going to want a return on that investment.

On the web, the biggest returns come from operating a platform that serves as critical infrastructure for some internet-based activity (be it online shopping, searches, or social media). These platforms act as gatekeepers who can take "here a little slice, there a little cut, three percent for sleeping with the window shut," as Les Misérables's Master of the House would say (sing, actually. And if I just got that song stuck in your head à la George Costanza in Seinfeld, I'm sorry not sorry). The slice might be of

data, the cut might be of cash from advertisers, and the shut may be blocking competitors from accessing the platform's infrastructure, but they all add up to market power and resulting profit for platforms like Amazon, Google, and Meta.

If Web3 were to come to fruition, it's theoretically possible that new businesses could emerge to take some market share away from the existing tech giants. But without any legal constraints and with some creative use of "off-chain" databases, we would probably just see the emergence of a new monopolist platform that collects and monetizes our data and charges a small fee for every online human interaction. And it's just as possible that an existing tech giant would end up providing that platform (I suspect that's what Meta was going for with its visions for the Metaverse). In short, if the goal of blockchain were to give power back to the people without any political or regulatory intervention, basic economic realities will ensure that it fails – Silicon Valley is banking on it.

Security

There is another "competition" argument that is often made in favor of new technologies, and that is the "international competitiveness" argument. There is a palpable panic that "if we don't embrace this technology fast, we'll get left behind! The jobs will move overseas! Aaaaaahh!!!" There's a particular fear that failing to embrace blockchain technology in the United States will undermine the international dominance of the US dollar, but as Martin Chorzempa explained to us in Chapter 3, that dominance comes from political and economic factors, not from the dollar's technological plumbing. And that dominance is increasingly being frittered away through reckless trade policy and challenges

to the Federal Reserve's independence at the same time as our national competitiveness in so many scientific and technological fields is being frittered away by terminating government research funding. So excuse me if I don't have a lot of patience these days for those who argue that Silicon Valley needs to be given free rein to ensure that the U.S. doesn't fall behind. Furthermore, I would humbly submit that we might not care to be the world leader in a technology that exposes our citizens to harm and/or compromises our national security interests.

Ever since bitcoin's early days, it has been used to facilitate illegal activities – ranging from ransomware attacks to human trafficking to terrorist activities. More recently, the stablecoin Tether joined the party: as the Financial Times put it, "the eye-popping constellation of gangsters and sanctions evaders using Tether includes cocaine cartels, North Korean hackers, Iranian and Russian spies, and fentanyl smugglers." The reason why these blockchain-based payments are so appealing to bad actors is that, when coupled with software tools like mixers and tumblers, they make it very easy to obscure the path of payments, avoiding sanctions and anti-money laundering laws.

Blockchains and the crypto assets that live on them are also eminently hackable, and there's no easy way to undo bad actors' transactions – a reality that has been exploited by North Korea, which is reported to be funding half of its nuclear program through crypto theft and other cyberattacks. It never ceases to amaze me that Congresspeople who typically claim to be very concerned about crime and national security are so willing to look the other way when it comes to crypto. China hawks, for example, are somehow cool with the fact that bitcoin mining operations throughout the United States have reported links to the

Chinese government. As for Russia's use of crypto to evade sanctions imposed by the United States after the Ukrainian invasion – well, that's somehow not a deal breaker.

The most charitable reading of all this is to assume that different people value different types of security differently (a less charitable reading would be that Congresspeople are in the pockets of the crypto industry, but we'll talk about that in a few weeks' time). Getting back to our charitable reading, perhaps some people are so ideologically opposed to the idea of governments regulating finance that they're primed to accept the blockchain alternative – even if it comes with a side order of human trafficking, North Korean nuclear capabilities, and increased threats of kidnapping and dismemberment. That's the argument that David Golumbia made in his 2016 book *The Politics of Bitcoin: Software as Right-Wing Extremism*: that bitcoin only makes sense for those who see governmental power as an inherent problem to be avoided at all costs.

But those who bemoan government overreach may not appreciate how vulnerable blockchains actually are to governmental authorities, as well as to non-governmental bad actors. We know that a whole lot of inefficiency and expense are involved in the validation mechanisms used to protect blockchains from bad actors, but unfortunately, even with all of that, blockchain operations remain vulnerable to intervention by both authorities and intermediaries. To start with the most fundamental vulnerabilities, blockchains won't work if access to electricity and the internet is curtailed. Now, you might think that I'm unfairly singling out blockchains here. After all, most of modern life would be upturned without electricity or the internet. But I do think it's important to mention these vulnerabilities,

because some blockchain devotees envision a post-apocalyptic world where we can somehow all still transact using bitcoin. I'm not sure how that's supposed to work if there's no working electrical grid to plug computers into.

I also mention the internet here because it is a pain point that governments could use to shut down a blockchain. Authoritarian governments around the world regularly restrict their citizens' internet access, and countries like China and Nigeria have already ordered telecommunications companies to restrict access to crypto exchanges. It may be possible for blockchain users to deploy workarounds like VPNs that pretend the computer is logging on from a different country, but authoritarian governments are also cracking down on VPNs, and VPNs certainly won't be of any help if the internet is turned off entirely. While turning off the internet would be a drastic step for any government to take, it's not unthinkable: India is reported to have intentionally shut down internet access 771 times between 2016-2023, sometimes in response to protests.

In dark moments, I have sometimes joked that a blockchain can only protect against Diet Authoritarianism – more aggressive authoritarianism will overwhelm it (the wisdom of treating blockchains as emergency lifelines for dissidents also needs to be assessed in light of the reality that authoritarian countries like Russia and North Korea rely on blockchains to strengthen themselves so that they can stamp out dissidents). While there have certainly been examples of political dissidents who managed to receive crypto payments in moments of need, blockchains are targets that remain vulnerable to attack by home governments, hostile nation states, and garden variety hackers.

Even with the lights and the internet on, blockchains have lots of security vulnerabilities.

In 2022, the cybersecurity firm Trail of Bits was engaged by the Department of Defense's research agency DARPA to investigate just how decentralized blockchains actually were from a security perspective. The short answer? Not very. With regards to the bitcoin blockchain, they found that "the vast majority of nodes do not meaningfully contribute to the health of the network" and that "the core developers and maintainers of blockchain software are a centralized point of trust in the system, susceptible to targeted attack." They concluded that, at that time, four pools of bitcoin miners working in concert could have disrupted the bitcoin blockchain if they wanted to – or they could have been hacked. Transaction validation on the Ethereum blockchain is also concentrated in a few hands: a 2024 report from the Federal Reserve Bank of New York found that "even though there are 156,150 block proposers, five large staking pools capture more than 50% of all the proposer revenue and blocks proposed." As with the bitcoin blockchain, this small group of staking pools could disrupt the Ethereum blockchain – because they wanted to, due to pressure from hostile governments, or under attack by hackers.

The security of blockchains is also threatened by neglect and boneheaded mistakes. As we saw with the faulty CrowdStrike update distributed in July 2024 (which crashed computer systems relied upon by businesses ranging from airlines to hospitals and caused more than $5 billion in direct losses), monumental f-ups can have widespread and damaging effects even without bad actors getting involved. A blockchain is software, and software is not "set and forget:" as it interacts with

other software, it can decay as well as develop security vulnerabilities. Big tech platforms and traditional financial institutions employ armies of engineers to maintain their software; when it comes to important financial services infrastructure, there are internationally accepted regulations that require providers to have policies and procedures in place regarding maintenance, cybersecurity, and recovery from major disruptions. When it comes to blockchains, though, no one is in charge of or accountable for performing these kinds of functions – and there's no guarantee that the foundations and other *ad hoc* maintainers that fill the breach will always have the best interests of blockchain users at heart.

I testified before Congress on this issue in June of 2024, and as has often been my experience in these hearings, my fellow witnesses were all drawn from the blockchain industry (or law firms representing the blockchain industry). After the hearing, an industry witness pulled me aside to tell me that he was a technologist and I was not (true enough), and to tell me that I was getting things wrong and should stay in my lane. He was particularly bothered by the concerns I expressed about blockchain's YOLO approach to maintenance and cybersecurity. He told me that my comments were misleading, and so I asked him who BlackRock relied upon to get comfortable that the Ethereum blockchain would keep functioning. He made it pretty clear that he thought this was an idiotic question, and responded something along the lines of "I don't need to worry about that. There are thousands of nodes hosting the Ethereum blockchain."

His absolute certainty and his PhD credentials made me second guess myself at first (I'm not saying it's easy to be a skeptic – we're all human). So I did what seemed to be the

sensible thing and immediately rushed home to reread some research on the topic by a computer science PhD who *didn't* work for the crypto industry. As Cornell professor James Grimmelmann (together with his co-author Jason Windawi) put it, "the need to modify and upgrade blockchain protocols and software to bring them into line with the intended design never goes away" – so someone *does* need to worry about these things. And "[e]veryone involved in a blockchain ecosystem benefits from the existence of a rock-solid protocol and high-quality software, but everyone is also better off free riding on someone else's work to develop them" – so it's *not* realistic to think that all those thousands of nodes are devoting their efforts to maintaining the Ethereum blockchain. Grimmelman and Windawi also observe that there can be challenges in coordinating the nodes who *do* want to participate – which perhaps explains why the Ethereum blockchain largely depends on the Ethereum Foundation to maintain the software for the Ethereum blockchain, despite the Foundation's protestations that it's not in charge (implicit in those protestations is a claim that the Foundation shouldn't be regulated as a financial market infrastructure provider…). I'm sure those protestations will be invoked extra loudly if the shit ever does hit the proverbial fan and there's a major operational outage on Ethereum that leaves BlackRock customers in a pickle.

A blockchain-based financial crisis?

You really have to fear your government – and at the same time believe that it won't get worse than Diet Authoritarian – to knowingly take on blockchain's security risks. But some techno-libertarians do have that Goldilocks level of fear, and they want to preserve their freedom to use blockchain technology, warts and

all. More times than I can count, I've been told "if you don't like blockchain, don't use it, and leave me alone." The problem with framing blockchain usage as a purely personal choice, though, is that it misses the risks and harms the technology generates for those who have never touched it.

We've already talked about the victims of crimes facilitated using blockchains and the environmental costs of bitcoin mining. But my area of specialty is financial crises, and I'm particularly worried that blockchain-based finance is setting us up for another one of those.

When the crypto bubble burst in 2022, the harm was mercifully contained. Don't get me wrong: there were tragic consequences for individual investors. But people who had never invested in crypto? Most of them didn't notice anything amiss, unless they were reading headlines about Sam Bankman-Fried's FTX fraud (I discussed these events with my students as they transpired, and one student expressed confusion about who Sandbag McFreed was – I was both envious of her ability to live her life without worrying about this stuff, and grateful that she didn't really need to worry). Given the way things are going, though, we won't be so lucky next time.

The crypto markets are becoming increasingly intertwined with the rest of our financial system. This process started when a regulatory agency called the Commodity Futures Trading Commission allowed bitcoin-based products to be traded on traditional commodity exchanges back in 2018. But the disintegration of barriers between crypto and the rest of our financial system has accelerated significantly during the second

Trump administration – notably, banks and 401(k) plans have been given the green light to increase their exposures to crypto.

The push for "tokenization" is another important part of this integration project. "Tokenization" really just means recording the ownership of real-world assets on a database in a way that allows for transactions to be automated using a kind of computer program known as a "smart contract." Tokenization doesn't have to happen on a blockchain, and because of the technology's fragilities, it frankly shouldn't – something I stressed in my 2024 Congressional testimony, which I closed with the warning:

> *much tokenization experimentation uses public permissionless blockchains, and seems designed to facilitate interconnections between crypto and traditional finance…Regulators around the world have sounded the alarm that greater integration of crypto and traditional finance could undermine the stability of our financial system. Tokenization should not be used to facilitate this integration.*

All my fears about integration are coming true right now, unfortunately. The current drive for tokenization seems to be less about improving finance's technological plumbing and more about avoiding the securities laws and "feed[ing] into the perpetual motion machine that is crypto trading," as one Financial Times article put it.

While there's been a lot of hype about tokenizing things like houses and art, blockchains aren't magic, and just recording ownership of a house or artwork on a blockchain doesn't

necessarily confer any legal rights – it certainly doesn't prevent these assets from changing hands offline. Instead, we've seen the most focus on tokenizing stocks and other financial assets that already owe their existence to recordings on a database somewhere. We've already discussed BlackRock's March 2024 launch of its tokenized Buidl fund, which allows people to invest in traditional financial assets using the Ethereum blockchain, but in 2025 – with regulators no longer looking too closely at securities law violations – the tokenization floodgates have opened up.

One of the most high profile launches in 2025 came from the trading app Robinhood, which announced tokenized versions of stocks that ultimately settle on the Ethereum blockchain with the goal of making crypto "the backbone of the global financial system." In a little Silicon Valley-on-Silicon Valley crime, Robinhood even offered tokenized versions of OpenAI's stock to the public, prompting OpenAI to tweet "These "OpenAI tokens" are not OpenAI equity. We did not partner with Robinhood, were not involved in this, and do not endorse it. Any transfer of OpenAI equity requires our approval—we did not approve any transfer. Please be careful."

> Robinhood's tokenization launch was also accompanied by a deeply cringy video, with CEO Vlad Tenev trying to style himself as Cary Grant in Hitchcock's *To Catch a Thief*. He speeds through the French Riviera in a convertible in order to deliver his "crypto keynote" in a chateau. In terms of sheer symbolism, it looks like Robinhood has gone straight from "stealing from the rich" to "let them eat cake."

So what does all this integration of crypto and traditional finance portend? As we discussed in Chapter 1, our financial system already has a lot of fragilities that result from its complexity, inflexibility, and ubiquitous leverage. Exacerbating those fragilities only makes it more likely that the rest of our economy will be shattered by another financial crisis, and integrating blockchain-based finance with the rest of the financial system is absolutely a recipe for exacerbating those fragilities. While Satoshi Nakomoto's Bitcoin White Paper pitched blockchain-based finance as a superior alternative to the traditional financial system, the reality is that the blockchain-based version has evolved in a way that replicates and exacerbates everything that is wrong with traditional finance.

We already know that, despite the hype, blockchain-based systems are rife with intermediaries, and that those intermediaries often escape the moderating influence of financial regulation. As a result, those intermediaries are able to borrow and lend money to fund investments at levels that wouldn't be permitted for regulated banks and brokers, making a blockchain-based financial system more prone to booms and busts. This leverage won't be completely unlimited: there will presumably come a point at which even an unregulated intermediary will decide that enough is enough and stop extending credit to an overextended borrower. But as we learned from our experience with AIG in 2008, lots of leverage can be created before that point is reached – leverage is very profitable until things go bad, and many of the costs of overextending leverage are borne by people other than the parties involved. In the bust phase, when intermediaries abruptly stop being so charitable with leverage, that's when we start seeing defaults, bankruptcies, and fire sales of assets. These can ripple outside of the financial system into harm for workers

(if problems in the financial system cause an economic recession) and taxpayers (if bailouts are involved).

The amount of leverage in the financial system can be juiced not just by allowing increased borrowing against existing financial assets, but also by creating new assets to borrow against. Securities regulations create some hurdles that need to be cleared before certain kinds of financial assets can be created, and those hurdles limit the ability to create assets out of thin air. But if those rules aren't enforced in the realm of blockchain-based finance, then creating more assets will know no bounds – just program an asset, hey presto, no real-world productive capacity required, and then use it as collateral for a loan (after all, that's what FTX did. Remind me again how that turned out…). And the prices of these kinds of assets – with no real-world productivity, no cash flows backing them – are highly susceptible to manipulation and volatility, which will make the bust phase more unpredictable and severe. And if people do start dumping blockchain-based assets in fire sales, everyone will know immediately because the blockchain is publicly visible. This level of transparency will only add to the panic (at least, that's what happened during the run on the Terra stablecoin in 2022).

As we just saw, there are ambitions to turn other real-world assets like artworks into financial assets by tokenizing them – it's not clear if that it will work out, but if it does, that'll mean yet more assets to borrow against. We also saw in that discussion of tokenization that assets on a blockchain can be pre-programmed to execute transactions without the intervention of any human being. In good times, this makes things more efficient – but the code will execute just as quickly in bad situations, even if everyone would be better off if it didn't.

> This is a bit wonky but if you want an example, when critical parts of the financial system have taken on too much leverage, flexibility may be needed during a bust to excuse the largest institutions from obligations to respond to margin calls or repay loans. I know this sounds like rewarding bad behavior and it kind of is, but without this kind of flexibility, we can end up with the kinds of defaults, bankruptcies, and fire sales at large institutions that drag down the whole financial system and the broader economy with it.

In traditional finance, obligations are written up in long legal documents, but they are not self-enforcing. This means that the parties (or regulators, or courts) can waive or forgive those obligations in low-probability but high-stakes situations – the kinds of situations Nassim Nicholas Taleb has popularized as "black swans." The problem is that some techno-solutionists have such faith in computer software to address all possible eventualities that they don't see the need for this kind of flexibility or forgiveness. In a truly cringeworthy holiday video made by the venture firm First Round Capital (which you can watch on YouTube if you're a glutton for punishment), startup founders sing the carpool karaoke lyrics "Cause I know software will eat black swans." Blockchain-based finance is more brittle as a result of this kind of hubris.

Valuing any complex financial asset is difficult enough at the best of times, and it gets much more challenging when people are panicking. Blockchain-based assets ratchet up the difficulty of valuation even more, because assessing them requires an audit of the assets' pre-programmed code to understand how they're

going to perform during black swans (as well as to see if there are any software vulnerabilities that can be exploited by hackers amidst the mayhem). There may also be uncertainties about who actually owns blockchain-based assets, which can further complicate valuation and add to the general panic. Despite claims that blockchains makes everything transparent, we know that lots of blockchain intermediaries manage assets on their own books and off the blockchain – Robinhood, for example, currently uses the Arbitrum database to process tokenization transactions, and plans to launch its own "Layer 2" database in the future. Transactions are ultimately settled on the Ethereum blockchain, but if there is a possibility of discrepancies between blockchain and off-chain records when it comes to asset ownership, buyers will want further discounts on those assets to compensate them for the uncertainty.

When things are spiraling out of control like this, sometimes the best medicine is a pause. Lots of traditional financial markets close at the end of the day and on weekends, which provides a natural opportunity for a break (and if things are really bad, for emergency government intervention). But one of blockchain-based finance's claims to greater efficiency is that operations continue 24/7. We may end up missing the pauses once they're gone.

The supply chain breakdowns in 2020 should have clued us into an important characteristic of complex systems: one tradeoff for efficiency is fragility, and we need to start asking "when is something efficient enough? When will making it more efficient introduce fragilities that will be counterproductive in the long run?" What I really want to emphasize here is that the efficiency gains that blockchain-based finance *can* manage –

through automating transactions, always-on markets, and unlimited asset proliferation – may not be in the best interests of society at large. These kinds of efficiencies make our financial system more fragile and therefore make our economy less secure. This may not be the same kind of security that techno-libertarians value, but it's valuable to most of us. It's particularly valuable to communities who are already more economically vulnerable: the harms of financial crises aren't distributed evenly, and those communities tend to suffer more in their aftermath.

Unfortunately, simply refusing to invest in crypto won't protect an individual from a crypto-inspired financial crisis. A coordinated policy response is needed, but many legislators and regulators are ignoring the dangers that blockchain-based finance poses for the broader economy – in part because they are unable or unwilling to see through blockchain's superficial promises to innovate us into some kind of universally beneficial ideal of efficiency, competition, and security.

Turtles

I started this chapter by talking about The Emperor's New Clothes, and I'll end it with another fable. There's an apocryphal story about an old lady who interrupts a presentation about the Earth's place in the universe in order to say that the Earth is actually supported on the back of a giant turtle. When she's asked what supports that turtle, she replies "another turtle," and so on, until she ultimately says "it's turtles all the way down." When it comes to efficiency, competition, and security, it's not turtles but values all the way down. A technology like a blockchain can never solve for efficiency, competition, or security in any kind of

neutral or universal way, because different people value different types of efficiency, competition, and security.

The versions of efficiency, competition, and security that technological solutions *do* solve for are typically the versions that will most benefit those developing or funding those solutions. This is a key reason why we should be skeptical about the technologies that Silicon Valley delivers. Although win-wins are possible, it is by no means guaranteed or even the norm that Silicon Valley technologies will be a net positive for society. And yet, we so rarely dig that deep. It's not just the blockchain – in so many spheres, we simply accept technological solutions without question. Right now, this is a huge problem as governments fall over themselves to be hospitable to generative AI, assuming that the technology has great promise and potential for humankind. Spoiler alert – the generative AI juice may not be worth the squeeze, at least not when it comes to finance. That's where we're heading next…