


# Cryptocurrency Might be a Path to Authoritarianism

---

 [theatlantic.com/technology/archive/2017/05/blockchain-of-command/528543/](https://theatlantic.com/technology/archive/2017/05/blockchain-of-command/528543/)

May 30,  
2017

□  
The door of La Maison Du Bitcoin in ParisBenoit Tessier / Reuters

All over town, the parking meters are disappearing. Drivers now pay at a central machine, or with an app. It's so convenient I sometimes forget to pay entirely—and then suffer the much higher price of a parking ticket. The last time that happened, I wondered: Why can't my car pay for its own parking automatically?

*Listen to the audio version of this article: Feature stories, read aloud: [download the Audm app for your iPhone](#).*

It's technically possible. Both my car and my smartphone know my location via GPS. My phone already couples to my car via Bluetooth. An app could prompt me to pay for parking upon arrival.

Or imagine this: My car, which is already mostly a computer, enters an agreement to lease time from a parking lot, which is managed by another computer. It "signs" this contract just by entering the lot and occupying a parking space. In exchange, the car transfers a small amount of Bitcoin, the currency of choice for computers, into the parking lot's wallet.

With computers handling the entire process, I'd never even be able to forget to pay for parking. The only way to fail would be for my car to run out of Bitcoin, in which case the parking lot has easy recourse: Because my car's ignition is managed by a computer, the parking lot could just shut my vehicle down.

Scenarios like this are possible when blockchain—the digital transaction record originally invented to validate Bitcoin transactions—gets used for purposes beyond payment. In certain circles, the technology has been hailed for its potential to usher in a new era of services that are less reliant on intermediaries like businesses and nation-states. But its boosters often overlook that the opposite is equally possible: Blockchain could further consolidate the centralized power of corporations and governments instead.

\* \* \*

In his book *Radical Technologies*, the urban designer Adam Greenfield calls cryptocurrency and blockchain the first technology that's "just fundamentally difficult for otherwise intelligent and highly capable people to understand." I was relieved when I read this, because I have been pretending to understand cryptocurrencies—digital money based in

code-breaking—for years. Bitcoin is hard to grasp because it's almost like a technology from an alien civilization. It's not just another platform or app. Making sense of it first requires deciphering the political assumptions that inspire it.

Bitcoin is an expression of extreme technological libertarianism. This school of thought goes by many names: anarcho-capitalism (or ancap for short), libertarian anarchy, market anarchism. Central to the philosophy is a distrust of states in favor of individuals. Its adherents believe society best facilitates individual will in a free-market economy driven by individual property owners—not governments or corporations—engaging in free trade of that private property.

Anarcho-capitalism is far more extreme than Silicon Valley's usual brand of technological individualism. For one, the tech sector's libertarianism is corporatist in its bent, and amenable to government, if in a strongly reduced capacity. And Silicon Valley takes a broader approach to the liberating capacity of technology: Facebook hopes to connect people, Google to make information more accessible, Uber to improve transit, and so on.

The ancap worldview only supports sovereign individuals engaging in free-market exchange. Neither states nor corporations are acceptable intermediaries. That leaves a sparsely set table. At it: individuals, the property they own, the contracts into which they enter to exchange that property, and a market to facilitate that exchange. All that's missing is a means to process exchanges in that market.

Ordinarily, money would be sufficient. But currency troubles market anarchists. The central banks that control the money supply are entities of the state. Financial payment networks like Visa are corporations, which aren't much better. That's where Bitcoin and other cryptocurrencies enter the picture. They attempt to provide a technological alternative to currency and banking that would avoid tainting the pure individualism of the ancap ideal.

This makes Bitcoin's design different from other technology-facilitated payment systems, like PayPal or Apple Pay. Those services just provide a more convenient computer interface to bank accounts and payment cards. For anarcho-capitalism to work in earnest, it would need to divorce transactions entirely from the traditional monetary system and the organizations that run it. Central banks and corporations could interfere with transactions. And yet, if individuals alone maintained currency records, money could be used fraudulently, or fabricated from thin air.

To solve these problems, Bitcoin is backed by mathematics instead of state governments. The Bitcoin "blockchain" is a shared, digital record of all the transactions (or "blocks") that have ever been exchanged. Every transaction contains a cryptographic record of the previous succession (the "chain") of exchanges. Each one can thus be mathematically verified to be valid. The community of Bitcoin users does the work of verification. To incentivize the onerous work of cryptographically verifying each transaction in the chain

that precedes it, the protocol awards a bounty—in Bitcoin of course—to the first user to validate a new transaction on the network. This is the process known as “mining”—a confusing and aspirational name for what amounts to computational accounting.

There’s a lot more detail that I am omitting. But the key to Bitcoin is that the network distributes copies of one common record of all Bitcoin transactions, against which individuals verify new exchanges. This record is the blockchain, which is sometimes also called the “distributed ledger”—a much more elucidating name. This is the missing element that’s supposed to allow the hypothetical anarcho-capitalist techno-utopia to flourish.

\* \* \*

At least, that’s the theory. In practice, Bitcoin and other cryptocurrencies don’t really meet the ancip ideal. Perhaps it’s an impossible goal; imagining the end of both nation-states and corporations is even harder than imagining the end of capitalism itself. Greenfield speculates in his book that Bitcoin was never meant to be a store of value, like state-backed currency, but only a medium for exchange “between parties who would presumably continue to hold the bulk of their assets in some other currency.”

Anarcho-capitalism might seem fringe and unfamiliar to most people, but at least it helps explain the rationale behind cryptocurrency and blockchain. Unfortunately, those topics become even more confusing when Bitcoin and its kin get used in ways incompatible with their original inspiration—which turns out to be most of the time.

As a medium for exchange, Bitcoin is relatively limited. Some retailers, many tech-oriented, accept the currency for purchases, but it remains best known as a means to buy black-market goods on darknet exchanges like [Silk Road](#). (The fact that such uses were illicit in the first place, the anarcho-capitalist would point out, is precisely the reason individual freedom-fighters should demand a decentralized market un beholden to governments.)

But Bitcoin’s success has accidentally undermined its viability. Each Bitcoin transaction adds more encrypted data to the blockchain, requiring increasingly more computer power to verify (and to earn the associated commission). More computing power means more energy cost to run and cool the machines, which requires more capital and physical infrastructure to support. Those rising costs inspire centralization. Adam Greenfield tells me that [two Chinese giants](#) can control over half of the global Bitcoin mining operations. If they collaborate, a majority-control of the blockchain could allow them to manipulate it. That’s precisely the risk a decentralized currency was meant to avoid.

More often, Bitcoin has been used as a financial instrument instead of a currency. From [tulips](#) to tech start-ups, market capitalism is flexible enough to turn anything into a tradable security or futures commodity. Bitcoin hype has made it appealing for speculators

certain to transfer their gains back into more stable state currencies, although its volatility makes it a difficult case either as a store of value or a medium of exchange.

The same hype driving cryptocurrency speculation has also attracted banks, governments, and corporations—exactly the authorities it was designed to circumvent. Financial services firms have taken an interest in cryptocurrency. Federal Reserve chair Janet Yellen has called for the Fed to leverage blockchain. Canada has been experimenting with a blockchain-backed version of its national currency, called CAD-Coin. Future cryptocurrencies operated by banks or governments might enjoy more productive use than Bitcoin.

But those futures also undermine cryptocurrency's ancap aspirations. Corporations and governments re-centralize control, for one. But also, they undermine the discretion and anonymity that accompanies free trade in the ancap fantasy. When the local or central bank manages the cryptocurrency platform, it also gets a record of every transaction that takes place in that economy. One doesn't need to be an anarchist to surmise potential downsides of that situation. Picture China mandating state cryptocurrency, tying the country's proposed social credit system to that ledger. Or imagine if the North Carolina State legislature decided to issue all food stamp vouchers in crypto form to better manage their future use.

\* \* \*

Even if Bitcoin's utility and value might decline, the distributed ledger offers potential uses beyond simple currency exchange. In theory, any internet-connected device could participate in verified, distributed transactions.

Greenfield offers a simple example: the German startup Slock.it, which "gives connected objects an identity, the ability to receive payments, enter into complex agreements and transact without intermediary." The simplest Slock.it device is a physical padlock that is connected to the internet. Networked locks are nothing new, thanks to the internet of things. But a blockchain-backed connected lock offers some additional capabilities. A distributed-ledger lock could enter into a "smart contract," an agreement whose terms are implemented directly in code. If attached to an AirBnB rental, such a lock could be programmed to automatically release when a smartphone belonging to a pre-paid renter approaches. Likewise, it could be programmed to cease to unlatch after that tenant's contract had terminated—or perhaps it could cut off the power or internet service if a sensor inside the property determined that its occupants were cavorting too loudly, or rifling through unauthorized cabinets.

Kik, a startup that makes a messaging app popular among teens, offers a more recent example of distributed-ledger tech in action. The company recently announced plans to introduce its own cryptocurrency, called Kin. Kik will automatically dole out Kin as rewards for developers who build apps on its platform, like stickers or chat bots. Kik's CEO, Ted

Livingston, presented the move as nothing short of emancipation from the oppression of ad-driven content platforms like Facebook and YouTube: “a cryptocurrency for an open future.”

Kin is built atop a platform called Ethereum, which is based on the same distributed ledger as Bitcoin. But Ethereum uses that technology to express a different aspect of the ancap model: contracts. For libertarians, contracts exist to facilitate market exchange, so smart contracts are always backed by currency (Ether, in Ethereum’s case). If Bitcoin is digital money for people, Ether is digital money for computers. It decides how to spend itself via software automation.

Why tout a private, distributed-ledger currency as an agent of liberation when it amounts to a complicated, software-backed, company-town store? One answer: It could give the workers a stake in the company store. In the world of cryptocurrency, this is known as an ICO or Initial Coin Offering. ICOs incentivize the use of an unproven platform, like Kik’s, by distributing an initial batch of cryptocurrency to early adopters. In theory, that value will increase if the platform becomes popular, creating a valuable base investment for its initial users.

In the extremist libertarian aspiration, smart contracts would allow anonymous actors to trade anything whatsoever in an untraceable way, via unregulatable markets. Instead, actual smart contracts, ICOs, and distributed ledger-backed devices mostly offer new ways to interface with the private technology industry. For example, in Brooklyn, a solar microgrid startup called Transactive sells clean energy to a community via Ethereum. And Toyota just announced a partnership with MIT to develop distributed ledger-based infrastructure for future autonomous vehicle services.

On that front, the anarcho-libertarians share something in common with the plain-vanilla technolibertarians: a belief in the wisdom and righteousness of a fully computational universe. My hypothetical smart-contract parking meter, Toyota’s future blockchain-backed rideshare system, Slock.it’s blockchain lock, Kik’s Kin, Transactive’s solar grid—all are just technology companies enjoying the capitalization and publicity spoils of the latest hot trend. They might become more than that, of course. But in order to do so, something terrifying has to happen first.

\* \* \*

Consider an off-the-cuff example of smart contracts from an Ethereum advocate:

An individual wants to purchase a home from another person. Traditionally there are multiple third parties involved in the exchange including lawyers and escrow agents which makes the process unnecessarily slow and expensive. With Ethereum, a piece of code could automatically transfer the home ownership to the buyer and the funds to the seller after a deal is agreed upon without needing a third party to execute on their behalf.

It sounds so easy. Who needs real-estate agents, closing attorneys, assessors, mortgage brokers, title insurers, municipal tax authorities, and all the rest? Just transfer some Ether after the computers shake hands.

But absent a global ancap revolution, those intermediaries are unlikely to disappear. Consider what would be required for distributed-ledger scenarios like this one become reality. Smart contracts require computational intermediation everywhere. Non-computational devices like parking lots and door locks and property deeds must become connected to computers. People would have to become willing to use machines that enter into decentralized contracts with other machines absent intermediary protection of government, law, banking, and other legacy infrastructures.

The problems with those old institutions are many. In a widely shared [tale](#) of voter suppression in the 2016 election, Eddie Lee Holloway Jr., a 58-year-old Wisconsin man, couldn't vote because the state's new voter-ID law demanded that he show proper identification. But an error on his birth certificate prevented him from getting a new ID. In a future run by the distributed ledger, a single copy of Holloway's identification would be securely stored on the blockchain, easily verifiable when needed. For the tech evangelist, it offers a rational solution that would solve social ills by means of impartial technology. (On that note, blockchain-based digital IDs have also been proposed for [refugees](#).)

It sure sounds good. But the scenario only works if the entire system of contemporary life becomes sufficiently interconnected to make it possible. All the departments of public health and the DMVs and the voter registration venues—not to mention the parking spaces and the automobiles and the power grids and all the rest—would have to cohere around a common understanding, so that the machines could execute smart contracts on their behalf. This would require a complete reinvention of public and private life.

A different reinvention is more likely. Instead of defanging governments and big corporations, the distributed ledger offers those domains enormous incentive to consolidate their power and influence. For people like Eddie Lee Holloway, Jr, who's African American, that might mean even greater exclusion, as the very institutions that locked him out of the voting booth might suppress his transformation into a digital-ledger citizen in the first place.

Or if not, other traumas might yet face citizens like Holloway in a society run by blockchain. A mandated DNA-test could accompany citizens' blockchainification, allowing their ethnic origins and medical predispositions to become attached to an identity record. Financial assets would also be connected, thanks to an underlying cryptocurrency account through which they make debits and credits. Not to mention all the personal insights already consolidated by services like Facebook.

Businesses might subscribe to this data. Thanks to distributed ledger, it could be used to prevent their automated doors from opening for people whom a smart-contract risk-assessment service rates below a threshold of desirability. Left outside, privately-contracted security robots might deploy ledger-backed ID scanners to sweep loiterers from private property. Once delivered and booked into jails, smart courts could automate sentences based on an automated assessment of future crime potential.

And that's just America. Imagine how a mature authoritarian state would fare under the rule of blockchain. Is this starting to feel like a Black Mirror episode yet? For Adam Greenfield, the anti-authoritarian left has profoundly misunderstood the corner into which such an ambitious aspiration paints society. "I believe distributed ledger enables the kind of central control they've never in their worst nightmares contemplated," he tells me. The irony would be tragic if it weren't also so frightening. The invitation to transform distributed-ledger systems into the ultimate tool of corporate and authoritarian control might be too great a temptation for human nature to forgo.

\* \* \*

If this sounds familiar, it's because contemporary culture has been here before. The existing, comparatively modest surveillance and control technologies in use by Google, Facebook, and their ilk—whose impact on governance we now know all too well—proliferated on the assumption that technology could make life better and more efficient. Nobody chose this life, exactly. People adopted technology in sufficient numbers to allow industry, and the culture that follows it, to conclude that the market had decided what was best.

Likewise, Bitcoin's triumph hinges mostly on the financial success of speculators who never had any intention of using it as currency, and who appear to have strip-mined it into oblivion in the process. Similarly, blockchain's future seems tied to the short-term vision of investors and entrepreneurs willing to speculate on a hypothetical, distributed utopia without hedging against the consolidated autocracy it seems equally likely to realize. "This is what happens," Greenfield says, "when very bright people outsmart themselves."

We want to hear what you think about this article. Submit a letter to the editor or write to [letters@theatlantic.com](mailto:letters@theatlantic.com).

Ian Bogost is a contributing editor at *The Atlantic* and the Ivan Allen College Distinguished Chair in Media Studies at the Georgia Institute of Technology. His latest book is *Play Anything*.

